IAJ

InterAgency Journal

A Quarterly Journal on National Security

from the Arthur D. Simons Center for Interagency Cooperation

About The Simons Center

The Arthur D. Simons Center for Interagency Cooperation is a major program of the Command and General Staff College Foundation, Inc. The Simons Center is committed to the development of military leaders with interagency operational skills and an interagency body of knowledge that facilitates broader and more effective cooperation and policy implementation. The Simons Center celebrates its 10th anniversary in 2020.

About the CGSC Foundation

The Command and General Staff College Foundation, Inc., celebrates its 15th anniversary in 2020. The Foundation was established on December 28, 2005 as a tax-exempt, non-profit educational foundation that provides resources and support to the U.S. Army Command and General Staff College in the development of tomorrow's military leaders. The CGSC Foundation helps to advance the profession of military art and science by promoting the welfare and enhancing the prestigious educational programs of the CGSC. The CGSC Foundation supports the College's many areas of focus by providing financial and research support for major programs such as the Simons Center, symposia, conferences, and lectures, as well as funding and organizing community outreach activities that help connect the American public to their Army. All Simons Center works are published by the "CGSC Foundation Press."

The CGSC Foundation is an equal opportunity provider.

FEATURES

From the Editor-in-Chief

Welcome to this first edition of the *InterAgency Journal* for 2020. This year marks a milestone anniversary for the Simons Center and the work we do in the interagency environment. We celebrate our 10th anniversary on April 21. Ten years of seeking a better understanding of the many organizational, cultural, and material factors that promote or impede interagency cooperation. Ten years of championing the investigation of issues impacting interagency coordination. Ten years since Mr. Ross Perot had the vision and provided the funds to begin our work to improve interagency cooperation. We celebrate that vision and continue the execution of the mission.

I invite you to watch us, and join the effort, throughout the year as the Simons Center will be expanding its efforts to enhance interagency cooperation. We will be looking to expand our reach and impact by fostering more opportunities for dialogue, by increasing our publications, and by working to establish a recognized education process and credentialing standard for competency and experience in interagency leadership and operations.

This edition of the *IAJ* continues our tradition of offering readings on a variety of topics. The nine articles featured take you through the importance of effective and efficient leadership, why for the Border Patrol decentralized leadership is needed, collaboration in WMD efforts, our inadequacies in bioterrorism response, the importance of moral leadership in detention operations, what we should do in the Nile Valley, the need for partnerships and cooperation in the Artificial Intelligence arena, a case study in strategic irregular warfare, and the importance of Multi Domain Operations in great power competition.

Thank you for reading this issue of the *InterAgency Journal*. Your feedback is always welcome as we strive to improve the discourse across the interagency community. I invite you to visit our website and to submit articles and book reviews for publication consideration. Best wishes for a productive and peaceful 2020. – **RMC**

The Productive Organization:

Survival of the Fittest

by Ted Thomas, Kevin Gentzler, and Billy Miller

> *If I had asked people what they wanted, they would have said faster horses.*
>
> —Attributed to Henry Ford[1]

> *It is not the strongest species that survive, nor the most intelligent, but the ones most responsive to change.*
>
> —Attributed to Charles Darwin[2]

Organizations come and go. Sears, at one time, was the largest retailer and employer in the United States. Sears dominated the retail industry for decades. In 1991 Sears lost the title as the largest U.S. retailer but still seemed unconcerned about the future.[3] During its more than 100 year reign as the leader of the retail industry in the United States, Sears massive economies of scale dwarfed its competition enabling it to withstand any challengers. But, after the growth of Wal-Mart, and now Amazon and others, went unacknowledged as a threat by the leaders of Sears a new future was upon the doorstep.[4] By 2017 the company needed to raise $1.5 billion just to stay in business even after shuttering stores and selling off decades old Sears brands such as

Ted Thomas, Ph.D., Lieutenant Colonel, retired, is formerly the Director of the Department of Command and Leadership in the U.S. Army Command and General Staff College at Fort Leavenworth, Kansas. Thomas graduated from the United States Military Academy and served in various command and staff positions before retiring from the military. He received a master's from the University of Illinois, and a Ph.D. from Missouri University of Science and Technology.

Dr. Kevin Gentzler is an assistant professor in the Department of Command and Leadership at the U.S. Army Command and General Staff College. Gentzler holds a Doctorate of Management in Organizational Leadership from University of Phoenix and a Master of Organizational Leadership from Regent University.

Mr. Billy Miller is an assistant professor in the Department of Command and Leadership at the U.S. Army Command and General Staff College. He is also a leadership instructor in the Leadership Instruction Division. Miller holds a Masters in Human Resources Development from Webster University.

Craftsmen tools.[5] Between 2010 and 2019 Sears lost $1 billion annually.[6, 7]

Eddie Lampert, the billionaire hedge fund manager became majority owner of Kmart, combined Kmart with Sears in 2005 to create the largest retail merger of its time. His goal was to better compete with Walmart and Home Depot and keep Sears competitive within the changing retail industry. Part of Lampert's change plan was to turn Sears and Kmart into a tech company to compete with upstarts and other rapidly growing companies. Instead of turning the business around, he secluded himself from the rank and file, took briefings over video teleconferences, would not invest in the company's core brands, and developed a vision and direction that neither customers nor employees believed in. In only a few short years Sears, a 100+ year old icon of America and long time industry leader, came to a breaking point. Sears leaders failed to efficiently and effectively respond to challengers, changes in the marketplace and correct an errant and failing strategy. These missteps eventually pushed the company to bankruptcy and the complete downfall of the one-time king of retail.[8]

> **To last, to thrive, and succeed organizations must be both efficient and effective.**

To last, to thrive, and succeed organizations must be both efficient and effective. An emphasis on one or the other without balance eventually leads to failure. We propose a model to help leaders develop organizations that stay effective and efficient, while recognizing threats from other institutions within the business environment. All organizations, whether business, government, or military, must see and respond to threats through learning processes while concurrently affecting timely and accurate change. We define both efficiency and effectiveness, present a model relating the two,

and discuss the need to establish a culture of learning to change at a level sufficient to stay ahead of the competition or defeat an adversary.

Efficiency and Effectiveness

Efficiency focuses on doing things better, faster, and cheaper. It is measured in time, effort, money, and resources. As Peter Drucker, the founder of modern management, once said, efficiency is "concerned with doing things right"[9, 10] by looking inward at the organization to improve its costs, processes, programs, and routines. Efficient organizations concern themselves with incremental changes to improve what the organization is already doing. However, even the most efficient organization will not survive if the leaders are doing the wrong things. Dr. Stephen Covey uses an analogy of a ladder to describe organizational efficiency. If the people in the organization are climbing the wrong ladder or the ladder is leaning against the wrong wall, they can maximize their speed in getting up the ladder while being very busy and very efficient, but the journey only ends at the wrong place faster.[11]

Effectiveness focuses on the long term strategy.[12] Most people measure effectiveness by the end results. Drucker made an important distinction when he said, effectiveness is concerned with "doing the right things," instead of doing things right.[13] From our perspective, an external focus on threats and opportunities is the primary idea of effectiveness. Leaders anticipate the future to influence the direction of the organization. Effectiveness is concerned with having the ladder leaning against the right wall.

However, even the most effective organization fails if its opponents copy the effective organization's ideas and do it more efficiently. In July of 2018, journalist Shane Harris reported on attempts by Chinese and Russian companies to steal proprietary information and use it to improve their countries' production capacities and capabilities. In effect,
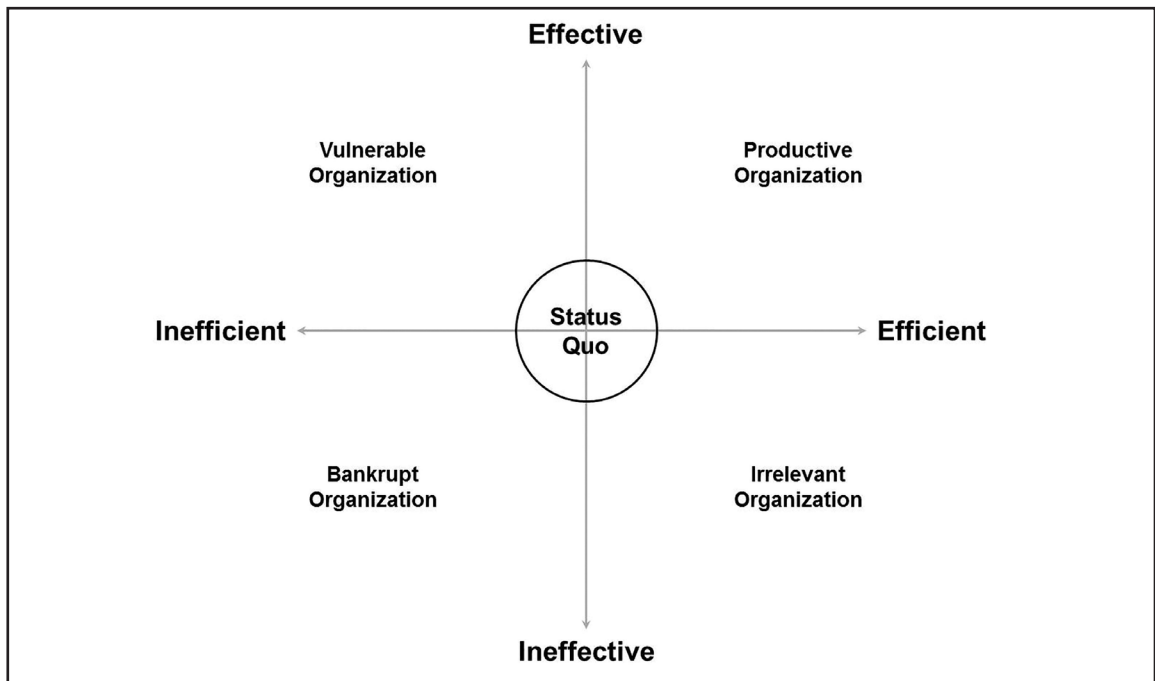
Figure 1. The Importance of Efficiency and Effectiveness in Organizational Culture

these countries became more efficient and effective by reducing or eliminating research and development time and costs, and by adopting newer and better technology. Both countries used this stolen information to boost their economies and grab market shares from the U.S. and other countries. Iran also targets U.S. firms to steal information on missile and space programs, seeking sensitive military technology to help them create their own weapons.[14]

We contend that survival of an organization depends on understanding the relationship between efficiency and effectiveness. Graphing efficiency and effectiveness on an x-y axis creates a four quadrant figure. The efficiency axis includes programs, processes, stability, and management. The effective axis concerns vision, disruption, people, and leadership. Efficiency is more oriented toward quantifiable, measurable, and predictable items, the "science of management." Effectiveness is directed towards the assessment of organizational matters that are qualitative in nature, the "art of leadership."

Efficiency and effectiveness reflect ideas in Craig Christensen's book, *The Innovator's Dilemma*. The question for organizational leaders is whether to take a short-term or long-term perspective. In the short-term, improving existing products and maintaining current income streams keeps customers happy and makes the organization efficient. Taking a long-term perspective increases the risk of losing customers and money by pursuing disruptive technologies that appeal to a different market or a smaller niche market. These disruptive technologies potentially improve effectiveness and take over the existing market.[15] Becoming more efficient seems the safer route, but it can lead to failure.

The graph shown in Figure 1 reviews a number of organizational case studies. The studies identified commonalities between organizations concerning efficiency from a managerial perspective and effectiveness from a leadership perspective. They determined what happens to an organization if both elements are, or are not, part of the organizational culture.

The graph places efficiency and effectiveness on opposing axes and describes the presence of each element in the organization as either high or low. The upper right quadrant indicates an organization that is efficient and effective. Found in this area of the chart is the *productive organization*. To survive in a changing and volatile environment, productive organizations must be both efficient and effective. To thrive in a competitive environment, leaders must

> **...an organization that is effective but inefficient...[is] a *vulnerable organization*.**

focus their efforts on improving current products and processes, seeking better quality, reducing costs, gaining a larger market share through pricing strategies, or timely delivery to customers. Organizational leaders operating in a business context need to anticipate market changes. Government and military leaders must anticipate changes in the political or operational environment. Both groups must take chances on new, disruptive technologies and methods to improve effectiveness within the respective spheres of influence or operations. Even the best leaders and companies are not always highly successful, but do have enough success to stay productive and competitive. Companies determine their destiny by how they respond to market changes and threats. Organizations that don't respond or respond incorrectly to these changes allow others to determine their fate.

Google, Amazon, and Apple are examples of productive companies. Each had failures in product launches, but their successes far outweigh their disasters. As Jeff Bezos, the founder and chief executive officer of Amazon said, "You need to be making big, noticeable failures. The great thing is that, when you take this approach, a small number of winners pay for dozens, hundreds of failures, and so every single

important thing we've done has taken a lot of risk, risk-taking, perseverance, guts, and some have worked out. Most of them have not."[16] Amazon, as a company, is a master at making the small changes to make things cheaper, better, and faster; more importantly, they constantly look for disruptive marketing approaches to force other companies to adapt or fail.

The upper left quadrant describes an organization that is effective but inefficient, which creates a *vulnerable organization*. If an organization does not take advantage of new technology, or a competitor steals the idea and improves efficiency in production and marketing, the original company loses to its competitors. Based on still employing outdated paradigms, the original innovator, though ahead of its peers in development, is vulnerable to outside threats and market changes. The organization may have the correct concept and leads at the turn, but loses the race because of a failure to see the future clearly and runs into a hazard instead of staying on course. By inventing the digital camera and failing to see the importance of the concept in future applications Kodak empitomoizes the vulnerable organization.

Kodak pioneered many fields with numerous different patents. They introduced the first camera over a century ago, but the digital camera, which its engineers invented in 1975, put Kodak out of business because of the failure of leaders to recognize the potential of digital photography and adequately market the product. The leaders failed to pursue digital photography because it threatened Kodak's dominance of the lucrative film business. Digital cameras threatened Kodak's primary income stream of selling film and other products. Pursuing digital technology required a change in paradigms and reduced profits in the transition years. "Like many other companies on the East Coast, Kodak has been phenomenal in research and patents and not so good commercializing things…"[17] Kodak effectively innovated but did not effectively

market their innovations. Kodak's leaders did not want to disrupt their existing business model. Instead, they allowed other companies to disrupt the industry and ultimately forced Kodak to lose dominance.

The lower right quadrant—efficient but ineffective—illustrates an "irrelevant" organization. This is an organization that technology passed by. An irrelevant organization continues working on building a better typewriter, floppy disk, or DVD when the technology moved to laptop PCs and cloud-based solutions. When an organization's leadership has no vision, the organization becomes complacent and focuses on keeping its current customer base happy by making existing technology better, faster, and cheaper. These organizations become are irrelevant as new, disruptive, and/or emerging technologies and innovative products upend the status quo and put them out of business.

Blockbuster is a prime example of a company dedicated to an income stream that dried up and left them bankrupt. Reed Hastings, the founder of Netflix, originally went to the CEO of Blockbuster to develop a partnership. Blockbuster dominated the marketplace with thousands of retail locations and millions of customers. They could not see a need to try something different, especially when that something threatened their current sources of revenue. Six years before filing bankruptcy, the CEO of Blockbuster realized Netflix was a threat to his business and tried to change the model to reflect more of what Netflix was doing. Blockbuster dropped late fees, a major source of income, and invested in digital platforms to reach customers, imitating Netflix. This caused a lag in profits and led to the firing of the Blockbuster CEO. The new Blockbuster CEO went back to an efficiency model to increase profitability. Five years later, Blockbuster declared bankruptcy. "The irony is that Blockbuster failed because its leadership had built a well-oiled operational machine. It was a very tight network that could execute with extreme efficiency, but poorly suited to let in new information."[18] Blockbuster was one of many companies with very efficient operations, but no vision of the future. Without a vision, Blockbuster became irrelevant when other companies disrupted their business.

The last quadrant reflects the inefficient and ineffective organization, this is the *bankrupt organization or* one which will soon fail. Many organizations lie on the dust heap of history because of poor leadership, poor management, and a culture resistant to change. As competitors move forward, the "inefficient and ineffective organization" remains complacent, stuck in their paradigms of past success, unable to visualize progress.

> ...efficient but ineffective — illustrates an "irrelevant" organization.

Sears is an example of a company with poor leadership, poor management, and a culture resistant to change. When Sears merged with Kmart in 2005, they had 3,500 stores, and 14 years later they are now below 900. In six years, they lost $10 billion. Their CEO, "thought he could turn around both companies simply by cutting costs and selling the real estate where underperforming stores were located."[19] He focused on efficiency by merging the two troubled retailers to cut costs and redundancies. Sears cut costs by ignoring infrastructure and ending up having stores with leaking roofs, cracked floors, and empty floor space where products should be. The CEO's vision was to turn Sears into a fast-growing tech company, similar to Apple or Microsoft. The employees did not believe in the CEO's vision and neither did their vendors, who canceled orders while their customer base turned elsewhere to shop.[20] Sears failed to become more efficient or more effective, and filed for bankruptcy in October 2018.
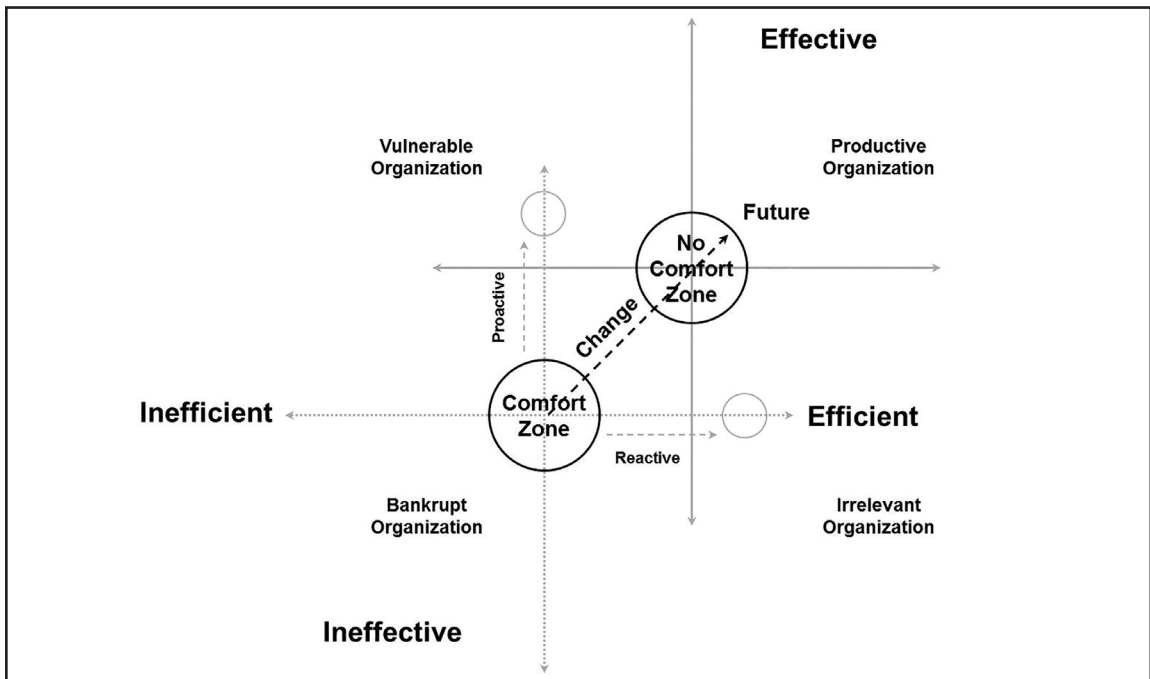
Figure 2. Moving Outside the Comfort Zone to Affect Positive Change

If the intersection of the lines in Figure 2 represents the current state of the organization, then over time, that intersection must move up and to the right as the environment becomes more efficient and effective. Conversely, organizations that do not change with the times and are comfortable with the status quo drift into one of the other quadrants. If they fail to change, they remain in their comfort zone where the income stream is secure. There is no growth and the organization goes out of business. If they change in one dimension only, such as in becoming more efficient or more effective, but not both, then the organization becomes vulnerable or irrelevant, and eventually drifts into bankruptcy. An organization focusing on effectiveness may have great vision and leadership, but will be overcome by others who are more efficient. Organizations that focus on efficiency without a good organizational vision and the associated direction become obsolete and irrelevant as they continue to improve old, outmoded ways of doing things. The end state for both is closed locations and out-of-work employees.

Change

What keeps organizations from becoming more effective and efficient? Resistance to change is a leading cause and occurs when a leader challenges the comfort of the group. Complacency, fear, worry that change causes more work or possibly makes their job obsolete are all common concerns. People usually prefer the security of the status quo rather than the unknowns of change which require them to move from their comfort zones and increase personal risk.

Leadership involves changing behaviors.[21] Often, the members of the organization cannot see a need for change, have no belief in the proposed change, or do not buy-in to the change and may subtly try to subvert the change. People are comfortable performing familiar tasks. Moving people from their comfort zone creates unknowns, risks, and elicits fear. There is an unwritten assumption of what worked in the past will continue to work in the future. Developing

an effective, efficient organization takes a strong, visionary leader to overcome natural resistance to change.

Resistance to change is natural and pervasive in organizations. Overcoming this resistance requires enough dissatisfaction with the status quo to make the struggles and effort associated with change worthwhile. Successfully changing an organization requires a vision of what the change will bring and a plan to accomplish it. Without these elements, the leader may attempt to simply force the change. Without member commitment, it may only last long enough for the members of the organization to subvert the change initiative and cause it to fail. Another factor that influences the acceptance of change is complacency.

The Beer's Model gives a partial explanation of how to make lasting change happen. While this model is written as a formula, C (change) = D (dissatisfaction) x M (vision) x P (plan) > R (resistance), it is not mathematical. There are no change units or vision units to multiply, but it does relate critical components needed for change to occur. The model's formula suggests that for change to occur there must be enough dissatisfaction with the status quo, accompanied by a vision or desirable future state, and a plan to achieve the change to overcome the natural resistance to change that exists in any organization.[22]

Michael Beer is not the only author to recognize the difficulty of overcoming the seeming overwhelming inertia of the status quo and complacency. John Kotter dedicated a chapter in his book *Leading Change*,[23] and later an entire book, *A Sense of Urgency*, to overcoming the resistance to change. Individual change is difficult, but organizational change is a monumental challenge. Due to the difficulty of organizational change, leaders must take an active role in the process. Leaders must reduce resistance to change and engender commitment from the organization's members to overcome complacency.[24] Authors Ron Heifetz and Marty Linsky said leadership is disappointing people at a rate they can handle.[25] In other words, leadership overcomes complacency to create change in a manner and a rate that followers accept.

Learning Organization

Becoming a learning organization is one antidote to ineffectiveness. Learning organizations (LO) exist to solve an existing problem, contend with competitors, improve the product delivered by the organization, or meet a newly identified need.[26, 27] An effective LO culture requires both leaders and followers to take part in the learning. Leaders in an LO encourage members to take time to reflect on events or experiences and make meaning from that reflection.[28] Reflection is central to one's ability to learn and grow in skills and abilities. Members of an LO must see their leaders as willing to adapt to and adopt the new knowledge created, resulting in wide acceptance of change.[29] Leaders must also contribute to the development of an LO culture through communicating a shared vision or understanding the necessity of becoming an LO.[30]

In a true LO, learning occurs at three levels: individual, team, and total organization.[31] Individual members of organizations must turn their personal or tacit knowledge, into useful information that is important to improving or developing his or her own expertise or abilities. Teams should learn collectively through meaningful work and share new knowledge between teams. Finally, the entire organization must collect information and distribute it effectively to develop shared understanding. Individuals and teams use shared understanding to develop new methods or processes, which improve both efficiency and effectiveness and lead to improved productivity in the field or market of that organization.

An LO is led by an individual or group of

leaders who accept the importance of learning to stay relevant.[32] These leaders develop a culture that values learning or incorporates the importance of learning into the beliefs and the underlying assumptions of the organization. When culture is infused with the importance of learning by individuals, teams, and the entire organization, a supportive climate materializes and freedom to change becomes the custom. This customary climate in the LO is conducive to a free exchange of ideas, to candor and dialogue.[33] Individual members working in this environment take tacit knowledge and make it explicit knowledge for their team or teams. The team, armed with new knowledge, shares it across the entire organization, or with other teams that may benefit from the knowledge, ultimately helping to achieve the organizational vision and make desired improvements.

If the leaders are complacent about learning, it is likely the members are complacent too.

LO processes benefit the organization by enabling continuous improvement and change within necessary areas, increasing relevancy in the market, or rapid responses to competitor changes. For the organization to truly benefit from the LO processes, the leaders must develop a systems approach to the input, transfer, and retrieval of information that enables and encourages using established learning processes which become an extension of the organizational culture.[34] If the system is not easy to use and readily available or does not meet the expected level of value of the individual, then organizational members avoid or neglect the system, which reduces the effectiveness of learning and results in decreased efficiencies across the organization.

One aspect of success in change efforts is unlearning. For more efficient and effective organizations, members and teams must unlearn

the things that prevent improvement or decrease flexibility and stand in the way of adaptation to changing environments and competition. Often, new ways of doing things and changing market conditions necessitate learning new methods and procedures to continue the ongoing work. Sometimes old beliefs and values are no longer accurate or necessary and must be unlearned or replaced. At other times the operational environment changes with such quickness and depth, the underlying assumptions become invalid. When this occurs simply changing methods or processes is ineffective. New underlying assumptions must be developed based on the changed environment. In situations such as these, learning requires new ways of thinking about the problems. Existing mental models or paradigms no longer represent reality and when used result in poor decisions and judgment reducing the organization's ability to efficiently and effectively respond to the situation. Unless the organization establishes a climate and culture that allows for change, innovation, and adaptation, they fall behind the competition and become bankrupt or irrelevant.

Complacency is a confounding factor in organizational life. If the leaders are complacent about learning, it is likely the members are complacent too. Complacency of leaders results in mismanagement or missed opportunities.[35] Complacency among the members at the lower organizational levels results in reduced efficiencies in production or outdated methods and processes. Even worse, complacency contributes to decreased safety, injuries, and death. Complacency is a key identifier of an organizational climate or culture that is not supportive of learning.[36] Complacency has no place in a learning organization or in a productive one. It is the leader's job to eliminate complacency, even when it is uncomfortable for the leader and the member. There has to be a level of discomfort to encourage people to grow and organizations to change. It is said there is no

growth in the comfort zone and no comfort in the growth zone. LO processes and concepts contribute to developing a growth zone that is an area of comfort if led correctly.

Conclusion

Leaders focused on both doing the right things (effectiveness) and doing things right (efficiency) are necessary to survive in today's volatile and turbulent market. Only agile and adaptive companies who change quicker than their competitors and adversaries have the resiliency to survive. Leaders need to recognize the seeds of their organization's destruction lies in success, due to the resulting complacency and concentration on efficiency. Successful companies are vulnerable to new upstarts with a vision that disrupts and changes the industry. In our increasingly automated world, the intersection of efficiency and effectiveness is shifting up and to the right quicker and quicker. Efficiency to adapt and effectiveness to innovate are both key to an organization's survival in today's world. *IAJ*

Notes

1   "My Customers Would Have Asked for a Faster Horse," *Quote Investigator*, https://quoteinvestigator.com/2011/07/28/ford-faster-horse, accessed 9 October 2018.

2   "It Is Not the Stronges of the Species that Survives but the Most Adaptable," *Quote Investigator*, https://quoteinvestigator.com/2014/05/04/adapt, accessed 10 October 2018.

3   Geoff Colvin, "Why Sears Failed," *Fortune*, http://fortune.com/2016/12/09/why-sears-failed, accessed September 14, 2018.

4   Haley Peterson, "Inside Sears' death spiral: How an iconic American brand has been driven to the edge of bankruptcy," *Business Insider*, 8 January 2017, https://www.businessinsider.com/sears-failing-stores-closing-edward-lampert-bankruptcy-chances-2017-1, accessed 3 October 2018.

5   Ibid.

6   Geoff Colvin, "Why Sears Failed," *Fortune*, http://fortune.com/2016/12/09/why-sears-failed, accessed September 14, 2018.

7   Haley Peterson, "Inside Sears' death spiral: How an iconic American brand has been driven to the edge of bankruptcy," *Business Insider*, 8 January 2017, https://www.businessinsider.com/sears-failing-stores-closing-edward-lampert-bankruptcy-chances-2017-1, accessed 3 October 2018.

8   Ibid.

9   Steve Denning, "The Best Of Peter Drucker". Forbes, accessed 18 October 2018.

10   Peter F. Drucker, *People and Performance: the Best of Peter Drucker on Management*, New York: Harper & Row, 1977, p. 33.

11   Stephen R. Covey, *The 7 Habits of Highly Effective People*, New York: Simon & Schuster, 1989, p. 98.

12   Sean Surbhi, "Difference Between Efficiency and Effectiveness," *Key Differences*, 23 May 2015, https://keydifferences.com/difference-between-efficiency-and-effectiveness.html, accessed 12 September 2018.

13   Drucker, *People and Performance: the Best of Peter Drucker on Management*, p. 33.

14   Shane Harris, "Chinese theft continues in cyberspace as new threats emerge, U.S. intelligence officials warn," *The Washington Post*, 26 July 2018, https://www.washingtonpost.com/world/national-security/chinese-theft-continues-in-cyberspace-as-new-threats-emerge-us-intelligence-officials-warn/2018/07/26/7af698ae-90cc-11e8-9b0d-749fb254bc3d_story.html?noredirect=on&utm_term=.94df3c1fdb0f, accessed 10 September 2018.

15   Clayton Christensen and Michael E. Raynor, *The Innovator's Solution: Creating and Sustaining Successful Growth*, Boston, MA: Harvard Business School Press, 2003, p. 43-45.

16   Eric Whiteside, "7 Worst Products Amazon Ever Had," *Investopedia*, 4 September 2018, https://www.investopedia.com/articles/company-insights/092016/7-worst-products-amazon-ever-had-amzn.asp, accessed 26 September 2018.

17   Dawn McCarty and Beth Jinks, "Kodak Files for Bankruptcy as Digital Era Spells End to Film," *Bloomberg*, 19 January 2012, http://cc.bingj.com/cache.aspx?q=eastman+kodak+bankruptcy+2012&d=4897922389838877&mkt=en-US&setlang=en-US&w=wQY6jZu_fOuzUW0va_nXo97fNywV8_0b, accessed 2 October 2018.

18   Greg Satell, "A Look Back At Why Blockbuster Really Failed And Why It Didn't Have To," *Forbes*, 5 September 2014, https://www.forbes.com/sites/gregsatell/2014/09/05/a-look-back-at-why-blockbuster-really-failed-and-why-it-didnt-have-to/#323c4fb41d64, accessed 2 October 2018.

19   Chris Isidore, "Here's what's killing Sears," *CNN Money*, 12 February 2018, https://money.cnn.com/2018/02/12/news/companies/sears-downfall/index.html, accessed 3 October 2018.

20   Hayley Peterson, "Inside Sears' death spiral: How an iconic American brand has been driven to the edge of bankruptcy," *Business Insider*, 8 January 2017, https://www.businessinsider.com/sears-failing-stores-closing-edward-lampert-bankruptcy-chances-2017-1, accessed 3 October 2018.

21   Alan Deutschman, "Change or Die," *Fast Company*, 1 May 2005, https://www.fastcompany.com/52717/change-or-die, accessed 20 February 2019.

22   Michael Beer, "Leading Change." Harvard Business School Background Note 488-037, January 1988, Revised January 20017.

23   John P. Kotter, *Leading Change*, Boston: Harvard Business School Press, 2012, p. 17-53.

24   John P. Kotter, *A Sense of Urgency,* Boston: Harvard Business School Press, p. 20-46.

25   Martin Linsky and Ronald Heifetz, *Leadership on the Line: Staying Alive through the Dangers of Leading*, Boston: Harvard Business School Press, 2002, p. 12.

26   Karen F. Marsick and Victoria J.Watkins, "The Learning Organization: An Integrative Vision for HRD.," *Human Resource Development Quarterly* 5, no. 4, 1994: p. 353–60, doi:10.1002/hrdq.3920050406

27   Peter M. Senge, *The Fifth Discipline: The Art and Practice of the Learning Organization*, 1st ed. New York: Doubleday/Currency, 1990, p. 3-16.

28   David A. Garvin, "Building a Learning Organization," *Harvard Business Review* 71, no. 4, 1993: p.78–91.

29   Edgar H. Schein, *Organizational Culture and Leadership*, San Francisco: Jossey-Bass, 2010, p.374-383.

30   Senge, *The Fifth Discipline: The Art and Practice of the Learning Organization*, p. 205-232.

31   Karen Marsick and Victoria J.Watkins, "The Learning Organization: An Integrative Vision for HRD." Human Resource Development Quarterly 5, no 4, August 2006: p. 353-360.

32   Senge, *The Fifth Discipline: The Art and Practice of the Learning Organization*, p. 3-14.

33   Anthony J DiBella and Edwin C Nevis, *How Organizations Learn,* San Francisco: Jossey-Bass, 1998; p.70-71. and Schein, *Organizational Culture and Leadership*, p. 365-371.

34   DiBella and Nevis, *How Organizations Learn*, p. 19-38 and p. 124-127.

35   Barbara Whitaker Shimko et al., "Debunking the " Lean and Mean " Myth and Celebrating the Rise of Learning Organizations" *Emerald Insights* 7, no. 2, 2000: p. 99–109, doi:10.1102/09696470010316251

36   James Barlow and Ashok Jashapara, "Organisational Learning and Inter-Firm 'Partnering' in the UK Construction Industry," *The Learning Organization* 5, no. 2, 1998: p. 86–98, doi:http://dx.doi.org/10.1108/09696479810212051.

Celebrating
10 Years of Service

The largest and most extensive of the CGSC Foundation's programs, the Simons Center is committed to the development of interagency leaders and an interagency body of knowledge. Over the past 10 years, the Simons Center has produced several publication and lecture series, including the *InterAgency Journal* and InterAgency Brown-Bag Lecture Series.

The CGSC Foundation is rightfully proud of all the Simons Center's accomplishments and contributions to improving interagency cooperation and education of leaders for the nation. We encourage you to join us in celebrating 10 years of service, and we urge you to stay tuned as we announce exciting new initiatives throughout 2020. May our next 10 years be the best yet!

From left, Foundation CEO Bob Ulin, Fort Leavenworth Commander/CGSC Commandant Lt. Gen. Robert L. Caslen, Jr., Foundation Chairman Lt. Gen. (Ret.) Robert Arter, Ross Perot, Foundation President Hyrum Smith, and the Chief Operating Officer of the Simons Center, Maj. Gen. (Ret.) Ray Barrett, cut the ribbon for the opening of the Col. Arthur D. Simons Center for the Study of Interagency Cooperation, April 21, 2010.

April 21, 2010	2010	2011	2012	2013
Grand opening of the Simons Center for Interagency Cooperation. Ross Perot performed the ribbon cutting.	First edition of the *InterAgency Journal* published in October.	Simons Center establishes student internship program. Interagency bibliography begins to take shape.	Simons Center hosts Greater Kansas City Cybersecurity Seminar. First special editions of the *InterAgency Journal* published.	Foreign Policy Advisor Conference hosted at American Academy of Diplomacy. Simons Center Scholars Program launched.

300 + Manuscripts published

More than 120 penned by CGSC students, graduates, and faculty

32 editions of the
InterAgency Journal

14 *InterAgency Essays*

18 *InterAgency Papers*

5 *Special Reports*

2 Books

Including 7 special editions of the IAJ

IAJ
InterAgency Journal
A Quarterly Journal on National Security
from the Arthur D. Simons Center for Interagency Cooperation

The CGSC Foundation Press

The U.S. Army Command and General Staff School
and the Arthur D. Simons Center present the

InterAgency
Brown-Bag
Lecture Series

Nearly 40 lectures...
and counting!

---

14 Interns and Scholars

More than

1,200

annotated
bibliography entries

2015	2016	2017	2018	April 21, 2020
Simons Center hosts CEO Cyber Security Roundtable.	InterAgency Brown-Bag Lecture Series and DACOR Visiting Professor of Diplomacy Program added to the Simons Center's Distinguished Speaker Series.	WWI Centennial Series and Vietnam War Lecture Series added to the Distinguished Speakers Series.	Simons Center debuts new design for *InterAgency Journal*.	Simons Center celebrates 10 years as the largest and one of the longest running CGSC Foundation programs in support of CGSC.

Mission Command:

Small Teams in the U.S. Border Patrol

by Robert W. Edwards

The U.S. Border Patrol divides personnel into shifts using line units, or patrol groups. Line units are the norm throughout the U.S. Border Patrol, dividing a 24-hour rotation into shifts filled by agents at each station within the 20 sectors in the U.S. Border Patrol. Most stations use small teams, like all-terrain vehicle units and horse patrol units. However, the idea of creating autonomous clusters of small teams on patrol groups or line units as an employment construct has not been executed.

Line units are cumbersome, divided into groups or teams in an ad hoc nature not specifically aligned to an area or expertise, whereas personnel employed in small teams would be the most responsive in the field, functioning autonomously. On small teams, agents report to one or two supervisors, and those supervisors work hand-in-hand with agents, augmenting the team. On a patrol group, supervisors have oversight of greater field tasks and office assignments. They delegate agents and technology assets to traffic in the field, devise schedules, and approve office work products completed by subordinate agents. Small teams may also require less technology, as they are proactive in response to specifically mobile technology in the field. Versus line units or patrol groups that respond reactively to infrequently mobile and static technology. Unlike patrol groups—which are assigned arbitrarily on weekly or monthly schedules—small teams work in the same area day after day, gaining familiarity with traffic or other structural patterns of activity, and fostering subject matter expertise. Line unit agents never gain this familiarity with their assigned areas.

Small Teams: Mission Command

Tactically and operationally, small teams would improve the U.S. Border Patrol's situational awareness along the border. Throughout the area of responsibility of any sector, and likewise

Robert Edwards attended the U.S. Army Command and General Staff College in 2016-2017, and received the Homeland Security Studies Award. Edwards also holds a Master of Public Administration degree from Texas A&M International University. Since 1995, Edwards has worked on several small teams with the U.S. Border Patrol.

Figure 1. Border Patrol Command Structure

station, in the U.S. Border Patrol, small teams would positively affect response rates and management as the primary method of personnel employment. Small teams would and do optimize the work output of the station's agents, more so than the current method of line units, or shifts. Small teams are characteristically more adaptive, rapidly mobile, and members work "autonomously."[1] The implementation of small teams is currently in use at the Tucson Station and elsewhere throughout the Border Patrol, but only as a force multiplier to enhance line units. To improve morale, effectiveness, efficiency, and reduce attrition, division of personnel into teams makes sense. Tucson Border Patrol Station, the largest in the Border Patrol as of 2014,[2] is an example of small teams employment, requiring a division of agents consisting of approximately 50 teams, with 10-12 Border Patrol Agents, and one to two Supervisory Border Patrol Agents. Managerial oversight remains with the Watch Commanders. Nested within each member of the small team construct is the "command intent"[3] of the station, provided by the Watch Commander.

Small teams at the Tucson Border Patrol Station are in short supply, due to the line unit factor, as not to deplete line units of agents and Supervisory Border Patrol Agents. Small teams, such as horse patrol units and the Tucson Station Mountain Team, are mission specific and rapidly mobile, as they work to respond to specific areas that are less feasible to access swiftly by line unit agents. Maximizing the efforts and skill sets of agents in the field with rapid response to risk managed[4] operations requires an agile

work force. Small teams are not cumbersome, with aligned purpose to the mission. They are swift to respond, without Supervisory Border Patrol Agent oversight or direction, thus providing autonomous initiative without slowed authorization from a Watch Commander.

A further proposal to align the small teams with leadership at the agent level entails selection of a Senior Patrol Agent. The Supervisory Border Patrol Agents from the Tucson Border Patrol Station select the Senior Patrol Agents, without consideration of seniority, based solely on merit. The Senior Patrol Agents fill Team Leader positions and peer the agents in the field. Further, Senior Patrol Agents mentor the agents and Supervisory Border Patrol Agents with tactical expertise.[5]

Line Units: Command and Control

Numerous individual agents make up line units. Watch Commanders at the second line supervisory level and Supervisory Border Patrol Agents at the first line level conduct oversight of the line units. The number of agents, Watch Commanders and Supervisory Border Patrol Agents vary in ratio depending upon the number of agents on a patrol group, or line unit. See Figure 1 for the Border Patrol command structure working left (higher rank) to right (lower rank).

The Command and Control[6] aspect of the line unit relates to the "designated commander"[7] role of the Watch Commander, with direct oversight of the Supervisory Border Patrol Agents in the field, providing authorization for specific operational response tasks. Further,

Supervisory Border Patrol Agents report to the Watch Commander through a Tactical Operations Center, which possesses tactical control of risk management resources, like Air and Marine Operations assets, again through the auspices of the Watch Commander. Agents assigned to a line unit work in positions that change daily, weekly, and in some instances monthly if assigned to an ad hoc team or group assignment. Assignment to an ad hoc team or group is rare—for example, the sudden creation of such units to meet a surge in illegal alien entries into the U.S.—and once the team meets the mission or objective, the group or team returns to the line unit. A Special Operations Supervisor has oversight of the ad hoc or specialty units and teams.

> **Line unit members may lack ownership of their daily assignments in an area of responsibility due to frequent changes in assignment, and in turn, lack familiarity with active intelligence of the area of responsibility.**

Agents assigned on a line unit remain in their assigned areas. This is despite a specific need for more manpower or resources in an area with mounting egress of illegal aliens into the U.S. It is common for illegal aliens to egress areas less patrolled by agents, and remote areas that have topographical obstacles, such as mountains or canyons. These areas are most prevalent for scouts and illegal aliens to seek illegal entry into the U.S. Increases in traffic, or illegal entries, will prompt supervisors to call for more manpower from different areas. However, this only creates gaps in coverage, requiring more adjustments of manpower. Small teams would enable flexibility to address traffic in the field without frequent adjustments of personnel. Small teams can also coordinate with other small teams working south to address gaps in borderline coverage.

Line Units vs. Small Teams: Pros and Cons of Each

Line unit members may lack ownership of their daily assignments in an area of responsibility due to frequent changes in assignment, and in turn, lack familiarity with active intelligence of the area of responsibility. Agents respond to the field, or area of operations, with the intent to locate foot sign or visual. Some days a trail may be active, while the following day another trail is more active, and by the end of the week both trails may be inactive, all based on the observations of scouts in the area. A scout on a higher elevation monitors an agent tracking a group along a trail, and the group reroutes to areas less accessible to patrol agents.

It can take weeks to months for agents to assess a scout site as to activity or inactivity. By this time, agents may be reassigned to different areas on a line unit, losing familiarity with an area. Agents who are not consistently working the same area lack the day-to-day familiarity and continuity that occurs on a small team, and do not have the ability to provide a subject matter expert's knowledge of containment or deterrence of persons illegally entering the country. The expertise agents acquire while assigned to teams will assist oncoming teams with specific intelligence pertinent to their area of responsibility and available whole-of-government[8] assets.

The military's analysis approach for capability gaps is Doctrine, Organization, Training, Materiel, Leadership and Personnel, and Facilities. Analyzing the effectiveness of employing small teams throughout the Border Patrol would apply to Doctrine, Organization, Training, Leadership and Personnel. Doctrine would become accessible through the construct of Tactics, Techniques, and Procedures organized at the sector and station levels to accommodate the number of personnel and topography within the area of responsibility.

	Doctrine	Organization	Training	Leadership	Personnel
Teams	X	X	X	X	X
Line Units/Patrol Groups		X		X	

Figure 2. Comparison of Small Team and Line Unit/Patrol Group Capability Gaps

The organizational structure would change in the Border Patrol with the advent of a team's approach, thus affecting Organization, and Training devised and incorporated in the teams' development, through Tactics, Techniques, and Procedure development and training. Leadership would further be rearranged to provide teams leadership and oversight, while Personnel would be distributed to the field differently, but not changed in expertise, unless Tactics, Techniques, and Procedure's decide otherwise (i.e. Scout identification training, tracking in teams, etc.).

Small teams meet ad hoc to discuss pertinent intelligence akin to their assigned areas and station requirements without the constraints of police musters or shift change briefs, which are the common method of exchanging information for the line unit. Patrol group agents may respond to the field individually, and require overwatch (Air and Marine Operations assets) for support, versus a small team that works together, and does not require immediate overwatch support.[9, 10] In addition, small teams' members apply to teams through the Patrol Agent in Charge, and the member's acceptance onto the teams is dependent on multiple factors. The Border Patrol Council is involved in the selection process, and an agent's seniority in the Border Patrol is considered prior to acceptance onto a small team.

Implementation of Small Teams

As previously discussed, small teams are in use today at the Tucson Border Patrol Station. To implement small teams throughout the area of responsibility (and cease the use of line units) would require a pilot launch of one shift, or line unit broken up into teams. The pilot launch would allow assessment of small team effectiveness versus the effectiveness of line units. Over the course of six months to a year, agents and Supervisory Border Patrol Agents would work together collecting active intelligence on their assigned teams, collaborating with both oncoming teams and teams from previous shifts. The team's level of effectiveness is dependent upon the team's agents working together with the supervision of one to two first line supervisors. It may be necessary to have a team of 5 to 6 working on each patrol group, or line unit, to start, which would make each small team the center of gravity per patrol group, providing essential information of activity in the area of responsibility. The teams would be comprised of volunteers, presumably the high-achievers at a station, whose initiative would lead each line unit.

The division of a line unit into teams would require policy change. According to the Community Work Group for Community Development, "Government Policy" may include the "support of an issue" by policy makers, or members of management and their subordinates.[11] The support of the concept to divide line units into teams requires a mass consensus of the station's agents and the Border Patrol's command staff. Without a unified effort of all team members, to include supervisors, a team approach to operations may fail. A smaller operational unit may be more flexible and responsive, but it can also implode faster than a larger unit if not managed or unified correctly.

Agents working in a team dynamic are more aware of their peers' strengths and weaknesses. This knowledge aids in organizing the team to work criminal alien traffic. For example, if an agent or agents are stronger at sign cutting than other members of the team, they may lead a tracking operation, while a less experienced

agent may cut ahead and provide situational awareness for the agent(s) following the drug trafficking group's sign. A technology-savvy agent who has more knowledge of computer based programs for compiling statistical data and accessing intelligence information would perform these tasks. As a final example, the agent or agents most familiar with the area of responsibility may set strategic goals for the team, insofar as realistically determining an achievable benchmark for seizures within a given period.

> ...small teams should become less ad hoc and more the mainstay, if not the norm.

Challenges

The concept of small teams as an over-arching framework of employing personnel within the Border Patrol would create a cultural change, as the replacement of shifts or line units for teams would alter the norm. The initial reaction of Border Patrol personnel may be hesitation, and there may be pushback from the Border Patrol Union, but over time a vested "shared belief"[12] in the small team concept would become the new norm. A cultural shift toward small team employment of personnel may spur new ideas from agents working in teams, and trust in management should improve. As autonomous decision-making by agents increases, management's confidence will likewise increase. A start to small team implementation may be adding one small team per line unit, or patrol group, in transition from line units to small teams.

In the "8-Step Process" Dr. Kotter begins with "Create a sense of urgency."[13] The need for employing agents to the Tucson Station area of responsibility in a more responsive, unified method requires an assessment of what is lacking in current use of the line unit. The key

to reaching "Step 6: Short term wins" may lie in developing a pilot project, six months to a year in duration, that proves teams are superior to line units. "Pressing harder after successes" (Step 7) involves fielding more teams in the Border Patrol, and increasing the consensus of agents, union stewards, and management.

Teams learn from each other, internally and externally. The members of teams learn from other members of the teams, and their weaknesses and strengths used to help the team reach its goals or complete its mission. As the Army calls for adaptability of their leaders,[14] the Border Patrol likewise requires adaptability of its leaders and agents in the field to fulfill the duties of a Border Patrol Agent. Adaptive employment of personnel is in current use in the U.S. Border Patrol within Special Operations Groups, however, small teams should become less ad hoc and more the mainstay, if not the norm.

Alien smuggling organizations and drug-trafficking organizations provide illegal aliens with camouflage gear and coach them to run when spotted by Immigration Officers, which exacerbates the need for an adaptive workforce. Response of personnel should be rapid, and the team concept at the Tucson Station is the most suitable method. Once situational understanding[15] of an area of responsibility provides context to a team's response needs (resources, technology, unified effort with other law enforcement assets), a determination to rapidly mobilize toward the threat is made, and risk management[16] follows with appropriate resources to respond.

A line unit is fractious. Its parts, several line agents assigned to a portion of the area of responsibility, are lost in communication if a section is working criminal traffic in a remote area. The difficulties inherent in working across separate parts continue when a call is made for more agents to assist with a checkpoint situation with constrained manpower. A small team remains cognizant of its members' whereabouts,

as the members usually work together within an assigned section (or grids) within a 10-15 mile stretch of land, providing ease in communication. Line units stretch 20-25 miles apart at any given time, complicating communication and collaboration.

The National Border Patrol Council is the union that represents Border Patrol Agents. The National Border Patrol Council is a component of the American Federation of Government Employees. The American Federation of Government Employees is comprised of "35 separate councils, to include the Veteran's Administration Council and the [National Border Patrol Council]."[17] According to the National Border Patrol Council, councils can exist if "they comply with the [American Federation of Government Employees]'s constitution."[18] The National Border Patrol Council provides support to the Border Patrol's labor force below first line supervisors. On the National Border Patrol Council website, under "The [National Border Patrol Council] Mission," it states, "We safeguard conditions of employment, agreements, practices, employee rights, and the labor laws of the United States."[19] By this measure, the National Border Patrol Council has leverage with management over employment at the Tucson Station if it entails the selection criteria for specific details or missions. In this context, the use of small teams should be a mainstay in the Border Patrol, not an ad hoc or temporary detail. Even then, if personnel are selected for a team, as they are for horse patrol units and Canine Handler selection, then the National Border Patrol Council would have a say in the selection procedure. The employment of personnel in the field at the Tucson Station currently has a bargaining agreement that allows agents to select the shifts they prefer. The preferences are in a tiered selection of their choices, the first being their most desired. Management officials and union stewards from the Tucson Station divide the units, based on seniority of staff. This allows for an unbiased process of dividing shifts into equal units, in a near even number of agents on each shift, or line unit. Supervisory Border Patrol Agents and Watch Commanders likewise provide their desired shifts. However, higher management will assign these individuals to shifts based on manpower needs and management objectives. The line units may remain with the selected personnel for a three or six-month rotation, but usually less than a year.

> **Line units stretch 20-25 miles apart at any given time, complicating communication and collaboration.**

Recommendation

Dividing personnel into teams and shifting the line units from a centralized command structure to a decentralized command structure allows for ownership of every autonomous agent. Make the change for a year and see what happens. The worst that could happen is that the culture shock would be too significant to maintain the command and control of leadership, or that most agents would not have a "shared belief"[20] in the small team concept. The best that could happen is a significant increase in effectiveness and morale amongst the agents in the Border Patrol. Lastly, leadership may improve with both current leaders and future leaders; leaders who would rise from a smaller team dynamic, a consequence of allowing more autonomy. Experiential knowledge of leadership gained from an agent's autonomous work environment within a team construct will provide the station and the Border Patrol with improved supervisory qualities prior to promotion.

The autonomous agent in the field makes decisions, nested within the team's strategy. With the "commander's intent"[21] conveyed by the supervisor succinctly to the team members,

the agents, make decisions without authorization of a supervisor. Capable agents within a team work autonomously and perform the duties of a Border Patrol Agent more effectively than a line agent performs the same duties. The line agent may require authorization from a supervisor before performing their tasks. In addition, unfamiliarity with the assignment or work environment inhibits confidence and interferes with decision-making, slowing their progress of detection and deterrence of criminal activity.

The small team concept is already underway at Tucson Station. Its methodology and future improvements, consensus and acceptance by management and agents in the field will depend upon lessons learned, through a similar construct to the Army's Center for Army Lessons Learned, which "archives lessons and best practices."[22] At first, the small teams pilot project may have hiccups in implementation, strategic design, and personnel embrace. A two-year study may be necessary to provide the most adequate statistical data, and to hold after action interviews and discussions are a necessity. Increasing small teams utilization by the Border Patrol will depend upon mitigation of vulnerabilities like Border Patrol Union constraints and continuity of information.

Training the line agents, to function well as a small team requires long periods of employment amongst a sustained unit. To build the trust fundamental to small teams will require greater connectivity between the agents and supervisors, which may require increased training together. This concept would entail further research and analysis. Additionally, training of a line unit may necessitate the creation of educational brochures and standards, further creating a small team's doctrine.

Recommendation: Perform an operational simulation for determining whether small teams are more effective than patrol groups or line units. Simulations used in the military would likewise work in the U.S. Border Patrol. There are numerous simulations to pick from and solicitation of vendors may occur at Headquarters for appropriate fit in the Border Patrol. A smaller scale simulation performed at Headquarters level will replicate at the sector and station level. *IAJ*

Notes

1 U.S. Department of the Army, Headquarters, *Special Operations*, Army Doctrine Publication (ADP) 3-05, 13.

2 U.S. Customs and Border Protection, *Tucson Station*, accessed June 1, 2017, https://www.cbp.gov/border-security/along-us-borders/border-patrol-sectors/tucson-sector-arizona/tucson-station.

3 Ibid.

4 U.S. Customs and Border Protection, *Border Patrol 2012-2016 Strategic Plan*, accessed December 20, 2016, https://www.cbp.gov/sites/default/files/documents/bp_strategic_plan.pdf, 12.

5 Interview with Gutierrez, Eugene, Supervisory Border Patrol Agent, Tucson Border Patrol Station, August 20, 2017.

6 Joint Chiefs of Staff. *Command and Control for Joint Land Operations* (Joint Publication 3-31). February 24, 2014.

7 Ibid.

8 U.S. Customs and Border Protection, *2012-2016 Border Patrol Strategic Plan*, accessed June 1, 2017, https://www.cbp.gov/sites/default/files/documents/bp_strategic_plan.pdf. 18.

9 "Cuts" are shorthand for "sign-cutting", which is a method of looking for disturbances in the terrain, or plant life, that would provide evidence of illegal aliens walking through the area of responsibility.

10 U.S. Customs and Border Protection, *2012-2016 Border Patrol Strategic Plan*, accessed June 1, 2017, https://www.cbp.gov/sites/default/files/documents/bp_strategic_plan.pdf. 18.

11 *Community Toolbox*, Workgroup for Community Involvement and Development, University of Kansas, accessed June 20, 2017, http://ctb.ku.edu/en/table-of-contents/implement/changing-policies/overview/main.

12 ADRP 6-22: Army Leadership. August 2012. Headquarters, Department of the Army. 5-4.

13 8-Step Process. *Kotter International*. Accessed June 20, 2017, https://www.kotterinternational.com/8-steps-process-for-leading-change.

14 Department of the Army, Army Doctrine Publication (ADP) 7-0, *Training Units and Developing Leaders* (Washington, DC: Government Printing Office, August 2012), 10.

15 Department of the Army, ADP 6-0 C-2 (2014), 3.

16 U.S. Customs and Border Protection, *Border Patrol 2012-2016 Strategic Plan*, 4.

17 National Border Patrol Council, "NBPC Response to New Yorker Article," accessed February 18, 2017, http://www.bpunion.org/index.php/newsroom/press-releases/1866-nbpc-response-to-new-yorker-article.

18 Ibid.

19 Ibid.

20 Ibid.

21 Department of the Army, ADP 6-0 C-2 (2014), 2.

22 Combined Arms Center, "Center for Army Lessons Learned," accessed May 20, 2017, http://usacac.army.mil/organizations/mccoe/call.

A Solution to

WMD Proliferation

by Michael W. Parrott

Nation-state efforts to develop or acquire weapons of mass destruction, their delivery systems, or their underlying technologies constitute a major threat to the security of the United States, its deployed troops, and allies. Use of chemical weapons in Syria by both state and non-state actors demonstrates that the threat of WMD is real.

— James R. Clapper, Worldwide Threat Assessment (2016)[1]

Summary

Current and future U.S. interagency and military efforts to counter the proliferation of weapons of mass destruction (WMD) throughout the world are thwarted by the complexity of the contemporary global security environment. For brevity, I use the Department of Defense definition of WMD—"chemical, biological, radiological, or nuclear weapons or devices capable of a high order of destruction and/or causing mass casualties."[2] Both the Department of Commerce and U.S. Special Operations Command's (SOCOM) mission priorities are focused on counterterrorism and counter-WMD (CWMD). This article examines the pros and cons associated with embedding Commerce Export Enforcement Officers and analysts in each of the Theater Special Operations Commands (TSOCs) in an effort to counter the proliferation of WMD ideas, materials, technologies, and products by state and non-state actors throughout the world. I contend that embedding Department of Commerce Bureau of Industry and Security (BIS) Export Enforcement Officers and analysts at each of the seven TSOCs would increase the both Department's CWMD/counterproliferation efforts exponentially, improve interagency collaboration, and provide a useful model for other interagency departments to emulate.

Chief Warrant Officer Three Michael W. Parrott serves as a U.S. Army Counterintelligence Technician. He holds a Masters in Strategic Security Studies from National Defense University and a BA in Homeland Security with a concentration in Terrorism Studies from American Military University. His assignments include a myriad of tactical to strategic level assignments within the Special Operations, Counter Weapons of Mass Destruction, and Intelligence communities.

Background

Today's security environment is complex. The transregional nature and "diverse spectrum of WMD threats" prevent any one agency or department in the U.S. government from attacking the problem alone.[3] In 2014, Secretary of Defense Chuck Hagel said, "The pursuit of weapons of mass destruction and potential use by actors of concern pose a threat to U.S. national security and peace and stability around the world."[4] Shortly thereafter the Pentagon ordered the transfer of the Department of Defense's CWMD Coordinating Authority role from U.S. Strategic Command to SOCOM.[5] The Pentagon recognized SOCOM is uniquely positioned and postured to leverage the breadth of the Defense Department's CWMD capabilities and resources in a mutually supportive comportment to the interagency's counterproliferation efforts. Subsequently, SOCOM developed its WMD Pathway Defeat approach, an adaptive framework that facilitates unity of effort and constant vigilance in order to disrupt WMD development and protect the homeland from coercion and attack from existing and emergent threats, as seen in Figure 1.[6] SOCOM relies on its TSOCs to plan CWMD operations and conduct activities that prevent proliferation and disrupt/defeat WMD pathways.

SOCOM has aligned its seven TSOCs with each of the Geographic Combatant Commands to facilitate the Department's and U.S. Special Operations Forces' desired end-states. (See Figure 2, next page.) TSOCs are the special operations headquarters element under operational control of their respective Geographic Combatant Commands, yet remain under the administrative control of SOCOM. TSOCs provide support to their respective Geographic Combatant Commands' special operations planning, logistics, and operational command and control requirements.[8] TSOCs, sub-unified commands, are permanent command and control structures that provide Special Operations Forces with a persistent theater posture and headquarters, in comparison to task

Illustrative Example

Non-Witting Non-State Actors or Businesses

Witting Non-State Actors or Businesses

Non-Witting Non-State Actors

Witting State Actors

Sub-Systems Support Process

WMD Pathway Continuum 1. 2. 3. 4. 5. 6.

1. Intent; 2. Infrastructure & Expertise; 3. Production; 4. Weaponization; 5. Delivery System; 6. Use

Nodes connected by Analytical Model PFITEL2C2M2

Illustrative Example

a. Program Management; b. Facilities; c. Infrastructure; d. Technology; e. Expertise; f. Leadership; g. Logistics; h. Communication; i. Components; j. Materials; k. Money

WMD Pathway: Networks (links among individuals, groups, organizations, governmental entities, etc.) encompassing ideas, materials, technologies, facilities, processes, products, and events that enable actors to conceptualize, develop, possess, and proliferate WMD and related capabilities.
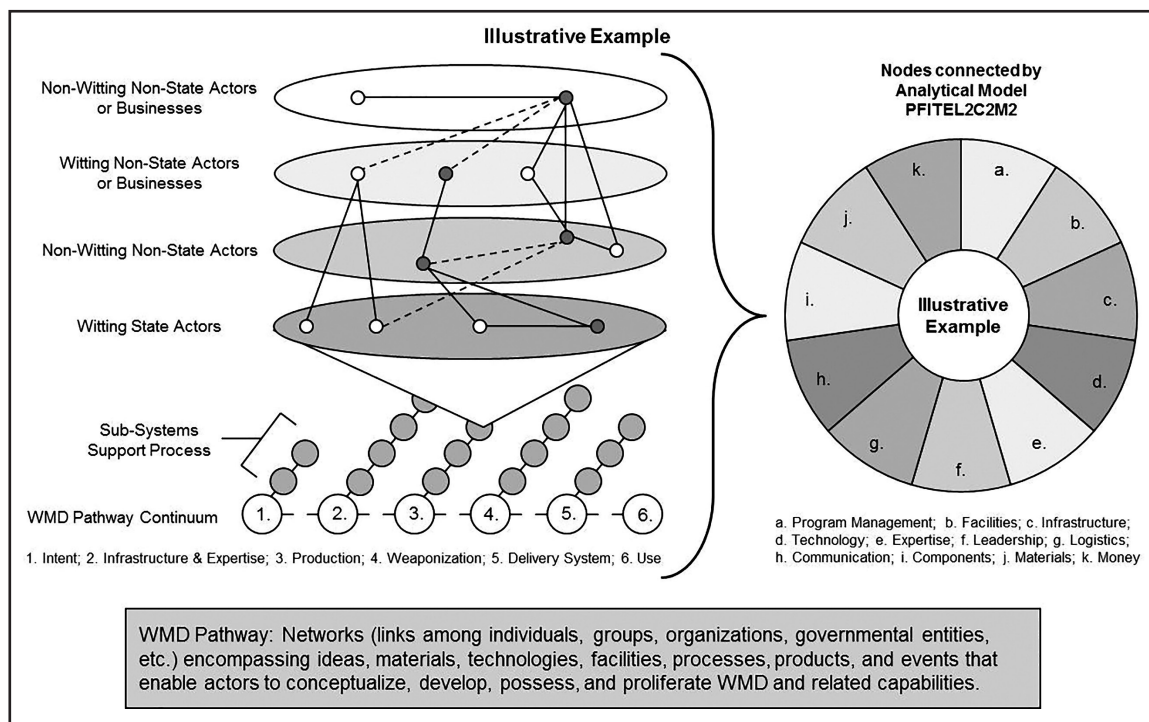
Figure 1. WMD Pathway Diagram, U.S. Army Special Operations Command[7]
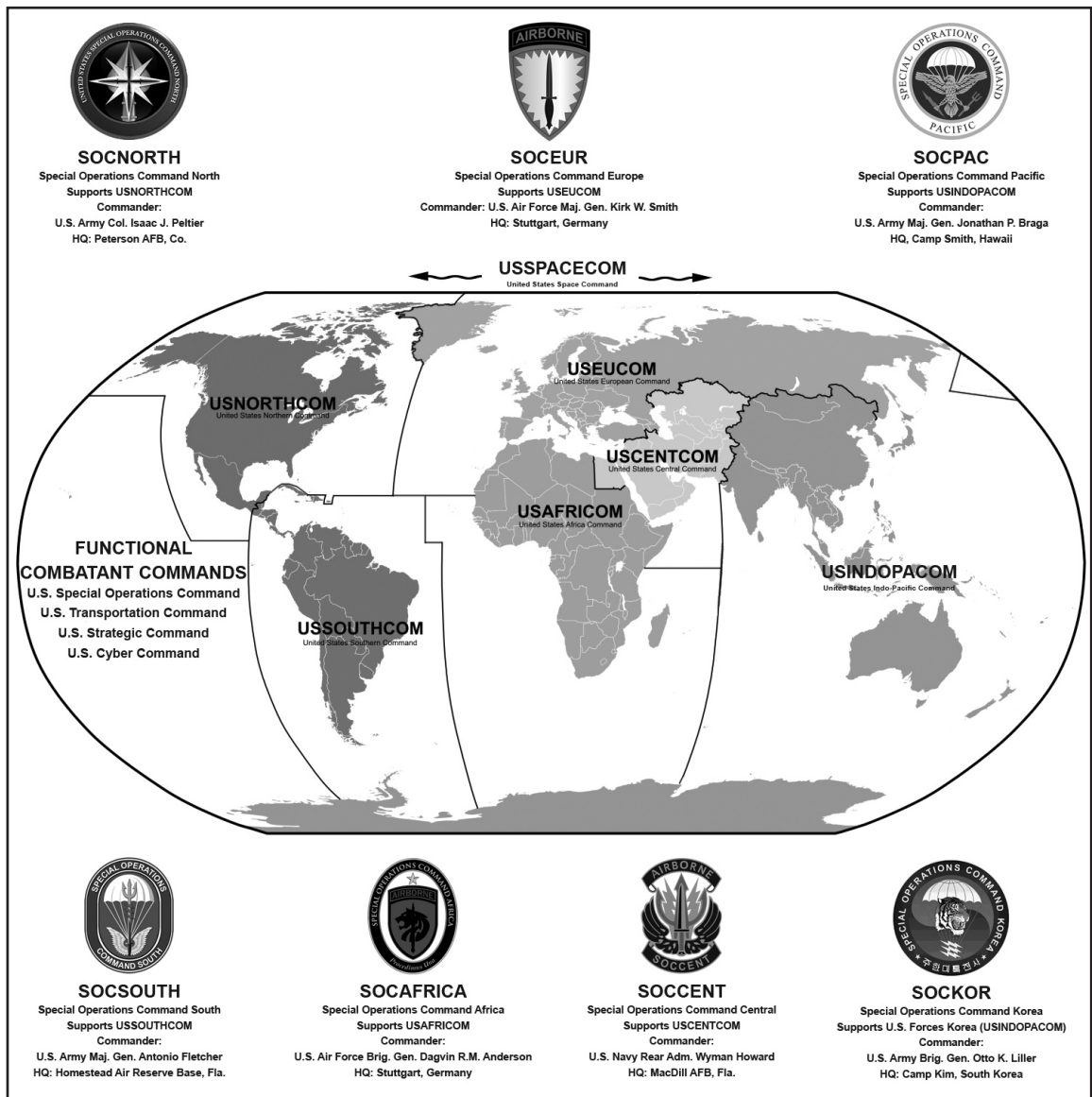
Figure 2. Map of the Combatant Commands' specific Areas of Responsibility and the seven Theater Special Operations Commands' aligned with them [9, 10]

forces that are *ad hoc* formations. The TSOC's permanency enables the employment of Special Operations Forces in a deliberate manner against multi-year objectives, which is necessary to conduct CWMD Pathway Defeat operations.

Similarly, the Department of Commerce has established overseas office locations. The Department of Commerce's Bureau of Industry and Security has six Export Enforcement office locations abroad. The offices employ special agents as Export Control Officers that report directly to their respective embassies and receive their direction and oversight from Export Enforcement.[11] The unique positioning of Export Control Officers in Russia, India, Singapore, the United Arab Emirates, and two locations in China makes partnering with U.S. Special Operations Forces and specifically the TSOCs a mutual necessity for BIS and SOCOM.[12] I explain the rationale, and the pros and cons of this partnership, in the next section.

Pros and Cons

Special Operations Forces' reach dwarfs that of the BIS's Export Enforcement office's international presence. In 2017, Special Operations Forces accounted for 70,000 of the 1.3 million U.S. service members and deployed to 149 countries. In total Special Operations Forces deployments occurred in 75 percent of the world's countries.[13] Special Operations Forces have placement and access to a multitude of locales that BIS lacks the manpower to cover. Likewise, three of six BIS's Export Control Officers are located in Russia and China—both are top threats to the U.S.—where Special Operations Forces are denied access. Both can benefit from cooperating with one-another to accomplish their specific CWMD, counterterrorism, and national security priorities by sharing information, leveraging each other's placement and access, and coordinating their respective efforts.

Both, SOCOM and BIS's mission priorities include CWMD/counterproliferation. Some of the BIS's primary activities include "administering and enforcing controls on exports and re-exports of dual-use items (i.e., those having a commercial and potential military or proliferation application) and various types of military items to counter proliferation of WMD, prevent destabilizing accumulations of conventional weapons, [and] combat terrorism..."[14] Likewise, Special Operations Forces are required to "be educated/trained for WMD [and counterterrorism] related operations" and "capable of tracking, monitoring, and countering WMD" proliferation.[15] Special Operations Forces members train, advise, and assist foreign partners in counterterrorism/CWMD activities and operations that deny violent extremist organizations safe havens, freedom of action, and movement throughout the globe. Special Operations Forces counterterrorism/CWMD operations provide a

wealth of information and are a great resource for BIS Export Control Officers and analysts seeking connections that can identify WMD proliferation pathways, actors, and networks across the WMD pathway continuum.

However, Commerce's Export Enforcement officer and analyst personnel strengths are extremely small, 180-200 in total, in comparison to Special Operations Forces' 70,000 members in 2017. In 2015, the BIS Export Enforcement Officer requested funding for two additional GS-13 analyst positions totaling $178,066 for yearly salaries.[16] In comparison, two Department of Defense Intelligence Analysts with six-years of experience each at the E-6 paygrade is a mere $72,000 in annual salaries.[17] The vast pay and budget discrepancies between the Departments of Defense ($495.6 billion) and Commerce ($14.6 billion) in 2015, may be a factor in Commerce's small Export Enforcement workforce that consists of roughly 200 agents and analysts.[18] Despite their differences, both Departments are creating mutually supportive partnerships.[19]

TSOCs, Geographic Combatant Commands,

> **Special Operations Forces members train, advise, and assist foreign partners in counterterrorism/CWMD activities and operations...**

and SOCOM have embedded liaison officers and analysts within the interagency and at various joint centers to reduce the burden on Department of Commerce and fellow interagency members. One such center is the Export Enforcement Coordination Center, "established to coordinate and deconflict... export enforcement activities... to protect national security through enhanced export enforcement and intelligence exchange."[20] The Export Enforcement Coordination Center has members from every major U.S. Department,

and it "serves as a conduit between federal law enforcement agencies and the U.S. Intelligence Community for the exchange of information related to potential U.S. export control violations."[21] Export Enforcement Coordination Center's unity of effort provides Commerce, SOCOM, and participating TSOCs opportunities to prevent threat actors development, acquisition, and use of WMD.

Recommendations and Conclusion

SOCOM, as the Defense CWMD Coordinating Authority, must continue to collaborate with Commerce to prioritize CWMD/counterproliferation efforts that mutually support both Departments' requirements. CWMD/counterproliferation efforts within each TSOC. Additionally the SOCOM CWMD Fusion Center should conduct a study to determine the best way or ways to fund and integrate interagency CWMD elements into TSOCs to ensure a concerted whole-of-government approach is levied in support of the current U.S. National Security Strategy. The National Security Strategy clearly states an aggressive posture alongside our allies and partners is the best form of defense against violent non-state actors.[22] What better way to stay on the offensive; than a TSOC/BIS partnership focused on counterterrorism/CWMD priorities. Both have similar missions and requirements to counter the proliferation of WMD by threat actors. The European based Export Control Officer and Special Operations Command Europe are ideally poised, positioned, and capable of providing SOCOM and both Departments, the necessary proof of concept for a successful partnership. Embedding BIS Export Enforcement Officers and analysts at the seven TSOCs will increase Department of Defense and Commerce CWMD/counterproliferation efforts exponentially, improve interagency collaboration and info-sharing, and provide a useful model for other interagency partners to emulate. *IAJ*

Notes

1   "Worldwide Threat Assessment of the U.S. Intelligence Community," Office of Director of National Intelligence, February 9, 2016, 6, accessed on February 27, 2019, https://www.dni.gov/files/documents/SASC_Unclassified_ 2016_ATA_SFR_FINAL.pdf.

2   Joint Chiefs of Staff, *Countering Weapons of Mass Destruction,* JP 3–40 (Washington, DC: Pentagon, 2014) vii, http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_40.pdf.

3   Matt Rautio, "Fostering Interagency Collaboration for Upstream Counterproliferation," *Interagency Journal* 8, no. 3, 2017, 37, http://thesimonscenter.org/wp-content/uploads/2017/08/IAJ-8-3-2017-pg35-50.pdf.

4   Department of Defense, *Department of Defense Strategy for Countering Weapons of Mass Destruction 2014*, i, accessed March 5, 2019, https://archive.defense.gov/pubs/DoD_Strategy_for_Countering_Weapons_of_Mass_ Destruction_dated_June_2014.pdf.

5   Joseph Osterman, "Statement before Senate Armed Services Committee," February 7, 2018, 2, accessed on March 10, 2019, https://www.armed-services.senate.gov/imo/media/doc/Osterman_02-07-18.pdf.

6   Shawn Powers, "U.S. Army Special Operations Command WMD Pathway Defeat Approach," (presentation, CWMD Global Synch Conference 17-01, Ft. Belvoir, VA, November 2017).

7   Ibid, 15.

8   Andrew Feickert, "U.S. Special Operations Forces (SOF): Background and Issues for Congress," *Congressional Research Service*, October 29, 2018, 2 accessed March 6, 2019, https://fas.org/sgp/crs/natsec/RS21048.pdf.

9   Wikipedia, "Unified Combatant Command," accessed on January 23, 2020, https://en.wikipedia.org/wiki/Unified_combatant_command#/media/File:GCCMAP_2019.png.

10   U.S. Special Operations Command Office of Communication, "Fact Book 2019," accessed on Feb. 23, 2020, 44-45, https://www.socom.mil/FactBook/2019%20Fact%20Book.pdf.

11   Bureau of Industry and Security (BIS), "Enforcement," U.S. Department of Commerce (DoC), accessed on March 8, 2019, https://www.bis.doc.gov/index.php/enforcement.

12   BIS, "OEE Personnel and Resources," DoC, accessed on March 8, 2019, https://www.bis.doc.gov/index.php/2015-10-29-20-18-41/2015-10-27-14-55-08.

13   Nick Turse, "U.S. Special Operations Forces Deployed to 149 Countries in 2017," December 15, 2017, accessed on February 19, 2019, https://warisboring.com/u-s-special-operations-forces-deployed-to-149-countries-in-2017/.

14   BIS, "Fiscal Year 2015 President's Submission," DoC, (2015), BIS-2, accessed on March 14, 2019, http://www.osec.doc.gov/bmi/budget/FY15CJ/BISFY2015CJFinal508compliant.pdf.

15   U.S. Army Special Operations Command, "USASOC Strategy-2035," April 2016, 5, accessed March 9, 2019, https://www.soc.mil/AssortedPages/USASOCStrategy2035.pdf.

16   BIS, "Fiscal Year 2015 President's Submission," BIS-55.

17   Defense Finance & Accounting Service, "Military Pay Table for 2015 – DFAS," (2015), accessed March 10, 2019, https://www.dfas.mil/dam/jcr:7061e0ca-a436-42f9-aa30.../2015MilitaryPayChart.pdf.

18   Ibid.

19   Lawerence Korb, Max Hoffman, and Katherine Blakeley, "A User's Guide to the Fiscal Year 2015 Defense Budget," April 24, 2014, accessed March 9, 2019, https://www.americanprogress.org/issues/security/reports/ 2014/04/24/88516/a-users-guide-to-the-fiscal-year-2015-defense-budget/; U.S. Department of Commerce, "2015 Department of Commerce Budget-in-Brief," accessed March 24, 2019, http://www.osec.doc.gov/bmi/budget/ FY15BiB/EntireBiB2_508.pdf.

20   BIS, "Fiscal Year 2015 President's Submission," BIS 54.

21   U.S. Immigration & Customs Enforcement, "Export Enforcement Coordination Center," January 3, 2018, accessed on March 20, 2019, https://www.ice.gov/eecc.

22   *National Security Strategy of the United States of America*, December 2017, accessed on March 3, 2019, https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.

A Nation Unprepared:
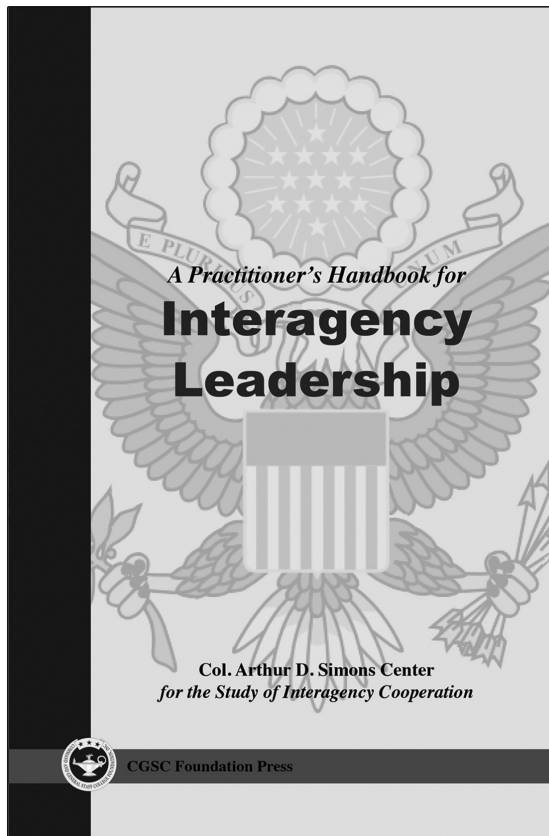
Bioterrorism and Pandemic Response

by John B. Foley

Editor's Note: Many interagency challenges are enduring. The following article was originally published in 2017, in Volume 8, number 2 of the Simons Center's InterAgency Journal. In light of recent outbreaks in the U.S. and across the globe—novel coronavirus and measles in 2019, ebola and E coli in 2018, and zika from 2015 to 2017—is the U.S. prepared for a pandemic or bioterror attack? The editors of the Journal invite our readers to ask themselves what has changed—for better or worse—since this article was originally published.

In 2001, senior U.S. policymakers converged to participate in the still famous Dark Winter exercise. The exercise contemplated a covert, bioterrorist attack against the U.S. The scenario began with simultaneous attacks, involving smallpox, on shopping malls in 3 separate states, resulting in 3,000 people becoming infected. By the end of the exercise, 16,000 smallpox cases had been reported in 25 states, 1,000 people had died, the healthcare system could not meet the patient load, 10 countries were reporting smallpox outbreaks, and Canada and Mexico had closed their borders. The smallpox vaccine stockpile had been depleted, and new stocks would not be available for a month. States had imposed travel restrictions, and food supplies were dwindling. People were fleeing cities, and the economy was faltering.

Even in 2001, a bioterrorist attack was not simply the stuff of science fiction. Between 1970 and 1998, the U.S. recorded over 400 suspected terrorist activities involving chemical or biological agents. In the immediate aftermath of Dark Winter exercise, the U.S. grappled with the 2001 Amerithrax attack on government offices in Washington and subsequently opened the treasury's floodgates to address the shortfalls revealed both by the Dark Winter exercise and the Amerithrax attack.

However, a decade and a half later, as the nation faced the 2014–2016 Ebola crisis, assessments of the U.S. government response led to a sobering conclusion: The U.S. still has not learned the lessons of Dark Winter.

John B. Foley, Lieutenant Colonel, U.S. Army, Ret., serves at the National Guard Bureau, J39 Combating Weapons of Mass Destruction. He received a M.S. in Weapons of Mass Destruction Studies as a National Defense University Countering WMD Graduate Fellow.

Transporting Infected Persons

In the spring of 2014, the first reports of an Ebola outbreak in West Africa came from Guinea. The virus quickly spread throughout the West African countries of Sierra Leone, Liberia, Nigeria, Senegal, and Mali. Of the more than 10,000 people infected with the Ebola virus, more than half died.[1] The initial response by the international community was viewed as a failure. President Obama declared the Ebola outbreak a top national security priority.[2] What had been a distant public health crisis had now been elevated to a national security threat. Obama ordered U.S. troops to West Africa in September to provide humanitarian assistance. U.S. efforts in West Africa centered on containing the epidemic and limiting the spread of disease. The Department of Defense (DoD) spent almost $400 million in its response support. The Ebola outbreak became the predominant news story, and bodies of Ebola victims lying in the streets greeted news watchers. The Centers for Disease Control and Prevention (CDC) assured the public that the U.S. healthcare system could deal with any outbreak.

> **In 1978, the U.S. military developed a patient transport capsule that could safely contain an individual exposed to highly infectious diseases...**

The U.S. military had worked with highly infectious agents like Ebola for many years. Treating highly infectious patients required the highest isolation standards. In 1978, the U.S. military developed a patient transport capsule that could safely contain an individual exposed to highly infectious diseases like Ebola. These isolation capsules were part of the Aeromedical Isolation and Special Medical Augmentation Response Team (AIT-SMART). An AIT-SMART team could transport one infected patient directly into a Biosafety Level 4 (BSL-4), the biosafety level at which the deadliest pathogens can be safely contained, and two such teams could be deployed simultaneously.[3] Given the number of persons likely to be affected by any bioterrorist attack, the idea that this capability could be applied to a mass-infection scenario seems almost farcical. When AIT-SMART teams were retired in 2010 and replaced by U.S. Air Force Critical Care Air Transport Teams (CCQTs), patient capacity expanded from one to five ventilator patients or ten less-critical patients. Naturally, even this tenfold capability increase did nothing to address the mass-infection problem.

Disease Recognition and Response Training

Even a limitless transportation capability is potentially useless unless infected persons can be properly identified. Ebola entered the U.S. hitchhiking in the living cells of an international traveler. The first reported U.S case of Ebola came on September 30, 2014 in Dallas. A man who had recently returned from Liberia became ill. A week later, he was dead. Two of the man's healthcare providers developed similar symptoms. Although they were treated and recovered, both lacked the requisite knowledge and training needed for isolating patients infected with such a deadly pathogen. Protective barrier requirements established for deadly pathogens such as Ebola were nonexistent. Personal protective equipment was inadequate. Isolation of the patient was done in a facility that was not equipped to contain the pathogen. So simple a matter as patient waste removal became a major bureaucratic challenge. Poorly executed coordination and communication between federal and local officials resulted in unnecessary delay in cleanup and disposal of hazardous waste from the victim's apartment. The victim's family was kept in quarantine by law enforcement. Compounding the various

local miscues, the CDC itself was forced to revise its previously published guidelines and protocols for the treatment of Ebola patients. The CDC now assessed that it was possible to become infected from droplets up to three feet away.[4]

A subsequent case of Ebola was diagnosed in in a New York City healthcare worker who had returned from abroad. After several days in New York, he developed a fever, notified city health authorities, and was immediately put in isolation. The governors of New York and New Jersey responded by imposing 21 day quarantines on any medical workers returning from countries affected with Ebola. Conflicts soon arose between the states and the federal government. The federal guidelines called for individuals to self-monitor for fever and regularly report their status to local health departments for 21 days. Reports circulated that people were afraid to ride the subway for fear of catching Ebola. Additional cases of Ebola infection were treated in specialized isolation facilities at Emory University Hospital, Nebraska Medical Center, and at the National Institutes of Health (NIH). By this point, Dr. Francis Collins, the Director of NIH, observed, "We need to take this current outbreak as a wake-up call. Diseases will come, and we have to be prepared, by investing in the public health infrastructure that keeps America safe."[5]

Following the Ebola crisis, two subcommittees (Emergency Preparedness Response and Communications) of the House Committee on Homeland Security assembled to investigate U.S. preparedness for a biological attack. Representative Martha McSally (R-Arizona) raised concern that a terrorist organization could launch a bioterrorist attack against the U.S. homeland. She said, "The risk of a biological terrorist attack to America is an urgent and serious threat. A bio attack could cause illness, and even kill hundreds of thousands of people, overwhelm our public health capabilities and create significant economic, societal and political consequences. Our nation's capacity to prevent, respond to and mitigate the impacts of biological terror incidents is a top national priority."[6]

While the Ebola crisis did not mushroom into a pandemic, it is not clear how much was due to preparedness as opposed to an enormous turn of good luck—as seductive as it might be to assume otherwise.

> **Our nation's capacity to prevent, respond to and mitigate the impacts of biological terror incidents is a top national priority.**

The Interagency Problem

Remarkably, there is not a single official who ensures that all agencies of the federal government work together on biodefense, even though at least five federal departments that have significant responsibilities in the event of a bioterrorist incident. A covert, bioterrorist attack would require a whole unity of effort response by the U.S. Presidential Decision Directive (PDD)-39 attempted to address this concern. PDD-39 specifies how federal agencies are to divide responsibilities among themselves with respect to weapons of mass destruction exercises and incidents.[7] It assigns central roles to the Federal Bureau of Investigation (FBI) and Federal Emergency Management Agency (FEMA) in the federal response to any terrorist event that results in mass casualties—the FBI as the lead agency for crisis management and FEMA as the lead agency for consequence management of mass casualty events. However, epidemic crisis management is not something that the FBI does daily. Likewise, FEMA does not have the skill, the correct personnel, or the authority and responsibility to act as a trusted agent when it comes to coordinating the necessary

public health response required to mitigate an epidemic. FEMA is structured to deal with things such as earthquakes, floods, hurricanes, and tornados involving mass casualties, but not events involving biohazards. Responsibility for planning, equipping, and training requirements likewise must be identified. However, PDD-39 does not address how the U.S. should prepare for a covert, biological event. It does not provide guidance on how to improve existing efforts that were in place or identify areas that could be improved. Moreover, because it states that agencies "will bear the costs of the participation in terrorist incidents and counterterrorist operations, unless otherwise directed,"[8] bureaucratic inertia and protectiveness of budgets serve to create a disincentive for interagency cooperation.

In an effort to move forward in a coordinated, unified fashion, President Obama named an Ebola "Czar"[9]; however, the temporary nature of the positon lacked the authority or power to bring about change. This situation called for the designation of a single responsible federal official to coordinate authority and make executive decisions across the interagency with respect to the biodefense enterprise.

The federal government does not lack funding to protect against bioterrorism as much, it would appear, as it lacks a coordinated investment strategy.

Budging to Protect against Bioterrorism

The federal government does not lack funding to protect against bioterrorism as much, it would appear, as it lacks a coordinated investment strategy. The present piecemeal approach to biodefense preparedness opens the possibility to numerous acquisition problems, including duplication of purchases, over or underestimation of requirements, purchasing improper equipment, and mismanagement of inventory.

- The Department of Homeland Security (DHS) was appropriated $47 million in supplemental funding to prepare for a pandemic. It spent this funding on personal protective equipment, research, and exercises. In 2014, an audit conducted by the DHS Inspector General found that DHS had not effectively managed pandemic personal protective equipment and antiviral medical countermeasures. DHS did not adequately conduct a needs assessment prior to purchasing personal protective equipment and medical countermeasures.[10]

- Following the 2001 anthrax letter attacks, Congress appropriated almost $3 billion to counter biological threats against the populace. The appropriation included over $1 billion to purchase antibiotics and vaccines as part of the Strategic National Stockpile (SNS). The CDC was tasked with determining the most probable and dangerous biological threat to the civil populace. The CDC used the following criteria set to make their determination:[11]

  ○ Impact on public health based on death and illness.

  ○ Ease of delivery to a large population. The stability of the agent, ability to mass produce and distribute and the R_0, its potential for person-to-person transmission of the agent.

  ○ Public fear perception and potential civil disruption.

  ○ Special public health preparedness requirements based on stockpile requirements (vaccines), enhanced surveillance, or diagnostic needs.

- In 2002, Congress also earmarked $1 billion for state-level public health system improvements.

- The Project BioShield Act of 2004 authorized the U.S. government to spend $5.6 billion over 10 years to acquire medical counter measures.[12]

The biodefense enterprise budget witnessed a huge increase in funding from FY 2001 to FY 2014, with civilian biodefense funding totaling $78.8 billion. Of this, $64.93 billion went to programs that included both biodefense and non-biodefense lines of effort. The remaining $13.89 billion went for programs which are solely dedicated to biodefense.[13] A closer look at the FY2001–FY2014 Civil Biodefense Funding shows that approximately $80 billion was spent on biodefense from FY2001 through FY2014. The majority of those expenditures went toward multi-hazard programs, and only about 17 percent went toward biodefense as such.

Although the biodefense enterprise receives multiyear funding for some of its programs, it receives only annual appropriations for others. A case in point is Project BioShield. This annual appropriation approach stymies strategic planning and execution to prepare programs for such things as changing political priorities and continuing budget resolutions. Moreover, budgets for the biodefense enterprise are difficult to predict from year to year. For example, the CDC's FY2014 proposed budget was $47.7 million less than its FY2013 budget. Three of the CDC's biodefense programs had significant reductions. The State and Local Preparedness and Response Capability, which includes the Public Health Emergency Preparedness (PHEP) cooperative agreement grant program, was reduced by $8.2 million to $658 million. PHEP provides funding for public health departments to upgrade their ability to respond to public health threats such as natural disasters, infectious diseases, and nuclear, biological, and chemical

events. This was a 30 percent reduction from FY2002 funding. The SNS's funding was also reduced by $38.4 million to $510.3 million, and the CDC Preparedness and Response Capability would be reduced by $1.1 million. Thus, enormous appropriations notwithstanding, a lack of a comprehensive investment plan, based on a strategic vision not subject to annual caprice, makes it impossible to determine if the biodefense enterprise is adequately funded.

> **A lack of a strategic vision as to what exactly biodefense seeks to accomplish is the greatest barrier to the success of interagency efforts at biodefense.**

A Strategic Approach

A lack of a strategic vision as to what exactly biodefense seeks to accomplish is the greatest barrier to the success of interagency efforts at biodefense. The old maxim that "defense does not win wars" should not be ignored by biodefense planners. History is replete with examples of strategies that circumvented known defenses. If the nation is well protected against, for example, anthrax or smallpox, an intelligent adversary would not attack with anthrax or smallpox when nature is replete with a wide range of pathogens that could be considered for use against humans. Novel viruses and new disease continue to emerge, and advances in biotechnology make it possible to manipulate how a virus behaves. Biological weapons programs, once only the domain of state-sponsored research organizations, are now within the reach of non-state actors. An individual with a graduate-level degree has all the tools and technologies to implement a sophisticated program to create a bioweapon.[14] The costs associated with the setup and operation of facilities to explore, develop, and cultivate biological hazards are within the reach of

well-funded terrorist organizations. A terrorist organization with several hundred thousand dollars, a dedicated group of graduate-level students, and a space of several hundred square meters could establish a small-scale biological weapons program.[15]

On the other hand, the U.S. government has made significant strides in biodefense. It has actively pursued efforts at the federal level and in concert with the states to deter, protect, and respond to a biological event. Funding has been appropriated to provide for the infrastructure, training, and equipping of local, state, and national responders. National-level exercises have been conducted to test and refine local, state, and national level response. The CDC has consolidated various bio surveillance programs into its National Electronic Surveillance System (NEEDS). This consolidation resulted in reducing confusion and easing the reporting process. All 50 states and the District of Columbia use a NEEDS-compatible system.[16] The CDC has provided grants for states to upgrade their laboratories forensic capabilities. The Laboratory Response Network was set up to provide local and state laboratories a rapid confirmatory process of suspected pathogens. The CDC and NIH continue research efforts on vaccines against diseases that have the potential

All 50 states have plans in place that provide a framework to respond to a biological event.

to be weaponized. DoD hospitals, as well as the health facilities of the Veterans Affairs (VA), can be called upon in the event of a national emergency.[17] The Department of Justice (DOJ) has provided biological terrorism training to law enforcement personnel and first responders. DOJ has also provided grants to states and cities to purchase personal protective gear for law enforcement and first providers. DHS has developed a strategy toward improving the

health security of the nation. The National Health Security Strategy (NHSS), published in 2010, provides for a unified approach for improving the health security of the nation. This unified approach relies heavily on the collaborative efforts of government agencies, community organizations, private enterprise, and academia. The NHSS lines of effort focus on community resilience, public health emergency medical countermeasures, health situation awareness, and healthcare coalitions. Community partners have made significant progress in health security improvement. There are now more than 24,000 members in the Hospital Preparedness Program. Of the nation's 6,340 hospitals, 5,288 belong are affiliated with the Hospital Preparedness Program.[18] This consortium has significantly improved hospital to hospital and responder to hospital communication capabilities. Critical information regarding the availability of resource and beds can now track critical data when trying to determine where to route ambulances. These partnership programs have resulted in stronger state and local public health agencies. Federal preparedness grants from DHHS and FEMA have benefited states and local communities' ability to respond to a bioterror event.

The National Response Framework (NRF) incorporates plans from the interagency. These interagency plans become the supporting plans or operational supplements to the NRF. Even though the NRF takes an "all-hazards" approach to consequence management, it is intended to be sufficiently flexible to orient interagency efforts to respond even to a bioterror attack.

All 50 states have plans in place that provide a framework to respond to a biological event. All states have a SNS plan in place. These all-encompassing plans detail the receipt, storage, and distribution of the SNS push packages. Some states that have either large metropolitan statistical areas or large cities have plans in place supporting the Cities Readiness Initiative. The Cities Readiness Initiative, located in 72 cities,

provides coverage to roughly percent of the U.S. population.[19] In important ways, therefore, federal investments have increased the country's ability to respond to a bioterrorists attack. Biodefense funding has provided states and local communities the means to improve their public health networks preparedness and response capabilities. First responders and law enforcement have been trained and equipped to respond to a bioterrorist event. State and local emergency management planners have developed plans to mitigate a bioterrorist event.

Conclusion

In the final analysis, however, the U.S. government is still haunted by, and should give heed to, the principal lessons of Dark Winter:

- The nation still lacks sufficient drugs and vaccines to mitigate an epidemic—which it must have, if for no other reason than as a deterrent against the possibility of an informed adversary attacking with pathogens against which the U.S. is already protected.

- The nation's healthcare cadre is inadequately trained and equipped to confront a major bio-attack.

- The nation's healthcare system lacks adequate surge capacity.

- Lines of authority across the interagency for responding to bioterrorism are ill-defined at best, and centralized leadership and coordinating authority is not firmly in place.

- Coordination efforts at all levels must thoroughly integrate medical expertise.

- Means for ensuring the accurate and timely dissemination of public information must be refined.

Failure to heed these lessons simply leaves the U.S. vulnerable, beyond what prudent risk management would suggest, to the threat of bioterrorism.

The U.S. has never had a bioterror attack that has resulted in an epidemic. The U.S. has had hundreds of suspected terrorist activities that have involved chemical or biological agents. The Anthrax attack mailings, coming just weeks after the attacks of 9/11, demonstrated how vulnerable the U.S. was to a bioterror attack. The federal response to the Anthrax attacks was so fraught with problems and ineptitude, it warranted the government's watch dog agency to proclaim that "the response was not only problematic but the response clearly indicated that the U.S. was not prepared for a terrorist biological attack." The world's largest outbreak of Ebola in West Africa gripped the world's attention and revealed troubling gaps and seams in federal bioterrorism response capabilities even though, despite collective miscues at all levels of government, only one fatality occurred.

The U.S. has conducted a massive effort to prepare the nation to respond to a bioterrorist event against several known weaponized pathogens. Billions of dollars have been spent on biodefense programs, but a very low percentage of those funds have gone toward the biodefense of the civil populace—the sole and proper object of biodefense in the first instance. Sir Ernest Rutherford is reputed to have once said, "we haven't the money, so we've got to think."[20] It may be that no amount of money will adequately substitute for the imperative to think. In any case, instead of waiting for a real "dark winter" to occur, serious thinking—in a coordinated manner across the interagency—about the bioterrorism problem is much needed and long overdue. *IAJ*

NOTES

1   Salaam-Blyther Tiaji, "U.S. and International Health Responses to the Ebola Outbreak in West Africa," Congressional Research Report, Congressional Research Service, October 29, 2014.

2   Daniel Halper, "Obama: 'Ebola A Top National Security Priority,'" *The Weekly Standard*, October 2014, <http://weeklystandard.com/blogs/obama-ebola-top-national-security-priority/article/808599>, accessed on August 26, 2014.

3   George Christopher, "Air Evacuation under High-Level Biosafety Containment: The Aeromedical Isolation Team," *Emerging Infectious Diseases*, Vol. 5, No. 2, 1999, pp. 241–242.

4   Siobhán O'Grady, "What Did the U.S. Learn from Ebola? How to Prepare for Bioterrorist Attacks," *Foreign Policy*, April 2015, <http://foreignpolicy .com/2015/04/23/what-did-the-u-s-learn-from-ebola-how-to-prepare-for-bioterrorist-attacks/>, accessed on August 12, 2015.

5   Rosa Delauro, "Ebola: A Preventable Catastrophe," *Huffington Post*, October 14, 2014, <http://huffi ngtonpost.com/rep-rosa-delauro/ebola-a-preventable-catas_b_5977808.html>, accessed on August 28, 2015.

6   Amanda Vicinanzo, "Biological Terrorist Attack on US an 'Urgent and Serious Threat,'" *Homeland Security Today*, April 23, 2015, <http://hstoday.us/briefings/daily-news-analysis/single-article/biological-terrorist-attack-on-us-an-urgent-and-serious-threat/0ce6ebf3524d83c537bif4f0cc578547.html>, accessed on August 23, 2015.

7   Richard A. Falkenrath et al., *America's Achilles' Heel: Nuclear, Biological, and Chemical Terrorism and Covert Attack*, MIT Press, Cambridge, MA, 1998, pp. 269–274.

8   Ibid.

9   Carol L. Lee, "Obama to Name Ron Klain as Ebola Czar," *The Wall Street Journal*, October 17, 2014, <http://www.wsj.com/articles/obama-to-name-ron-klain-as-ebloa-czar-1413557184>, accessed on August 6, 2015.

10   "DHS Has Not Effectively Managed Pandemic Personal Protective Equipment and Antiviral Medical Countermeasures," Department of Homeland Security Office of the Inspector General, U.S. Department of Homeland Security, August 1, 2014, <http://oig.dhs.gov/assests/Mgmt/2014/OIG_14-129_Aug14.pdf>, accessed on September 12, 2015.

11   Malcom Dando, *Bioterror and Biowarfare*, Oneworld Publications, Oxford, 2006, p. 62.

12 Bruce Maxwell, *Homeland Security: A Documentary History*, CQ Press, Washington, DC, 2004, pp.327–328.

13   Rebecca Katz, "Biological Weapons: A National Security Problem that Requires a Public Health Response," Working Paper 2001–2004, Office of Population Research, Princeton University, Princeton, NJ, 2004, p. 198.

14   "U.S. Unprepared for Biological Attack," *Homeland Security News Wire*, December 1, 2011, <http://homelandsecuritynewswire.com/dr20111201-u-s-unprepared-for-biological-attack>, accessed on October 5, 2015.

15   James Jay Carafano, Ph.D., "Improving Federal Response to Catastrophic Bioterrorist Attacks: The Next Steps," The Heritage Foundation, November 13, <http://heritageorg/research/reports/2003/11/improving-federal-response-to-catastrophic-bioterrorist-attacks-the-next-steps>, accessed on August 28, 2015.

16   "Today, all 50 States and Washington, DC Use a NEDSS-Compatible System to Send Case Notification to NNDSS," Centers for Disease Control and Prevention, <http://cdc.gov/nndss/nedss.html>, accessed on August 31, 2015.

17   Carafano.

18   "2015 National Preparedness Report," Federal Emergency Management Agency, March 30, 2015, <http://fema.gov/media-library-data/1432751954859-fcaf2acc365b5a7213a38bbeb5cd1d61/2015_NPR_508c_20150527_Final.pdf>, accessed on August 16, 2015.

19   Jacqueline Langwith, *Bioterrorism*, Greenhaven Press, Farmington, MI, 2008, pp. 162–163.

20   Sir Ernest Rutherford, quoted by R.V. Jones, *Bulletin of the Institute of Physics*, 1962, Vol. 13, No. 4, p. 102, <http://todayinsci.com/R/Rutherford_Ernest/RutherfordErnest-Quotations.htm>, accessed on January 16, 2016.

Missed Operational Opportunities in The Global War on Terror's

Prisons and Camps

by Hoang Truong

After 9/11 and during the War on Terror, the U.S. military, coalition forces, and associated paramilitary (contractor) elements had to deal with various prisons (convicted criminals) and camps (all other categories of non-convicts, to include criminal suspects—hereinafter, "facilities") under its control or influence, in order to obtain intelligence and other information it deemed useful from high-value detainees.[1, 2] The "War on Terror," which encompassed the Afghanistan and Iraq Wars, was a George W. Bush Administration initiated military campaign in response to the 9/11 Al Qaeda attacks. President Bush announced the War on Terror on September 20, 2001, in a speech to Congress: "Our war on terror begins with al-Qaida," he said, "but it does not end there. It will not end until every terrorist group of global reach has been found, stopped, and defeated."[3] The Bush Administration's War on Terror presumed that the warfighting would be waged against a tactic. However, on May 23, 2013, President Barack Obama announced that the Global War on Terror was over, asserting that U.S. military and intelligence agencies wouldn't wage war against a tactic but would instead focus on specific groups of networks whose goals were to destroy the U.S.[4]

The Abu Ghraib prison debacle, wherein the showcasing of prisoner abuse was strewn across the international media stage, stands out as a glaring missed opportunity for said U.S. military personnel to proactively gain intelligence and actionable information from prisoners. Oussama Atar, the man believed to be the mastermind behind the November 2015 Paris attack and the 2016 Brussels bombings, had been a prisoner at both Abu Ghraib and Camp Cropper, a detention facility that had housed Saddam Hussein.[5] A March 2017 CNN article asserted that Atar had been radicalized in various detention facilities while in U.S. custody and that he had met Abu Bakr al-Baghdadi, the creator of ISIS and currently its presumed leader, in such a facility.[6] There are numerous online accounts and statements by U.S. military officials condemning the torture and murders that occurred

Mr. Tyne Truong is an Assistant Special Agent in Charge for the U.S. Department of Homeland Security, Homeland Security Investigations National Security, Counterterrorism and Counter-Proliferation Investigations Division. He holds a Master's degree in Leadership from the McDonough School of Business, Georgetown University, and is also a Homeland Defense Fellow Distinguished Scholar at the National Defense University, College of International Security.

at Abu Ghraib and specifically, how these tortures either set back U.S. and coalition forces' ability to legitimate its continued participation in Afghanistan, Iraq, and associated regions or even worse, strengthened the resolve of terrorist organizations such as ISIS and Al Qaeda.[7, 8]

Did the U.S. government miss substantive proactive operational opportunities when it had command, control, and or influence of said facilities? If so, what were these opportunities and how could it have gone about realizing measurable gains from such operations? For purposes of this discussion, operational opportunities will be defined as a) confidential informant (CI) cultivation and control, and b) undercover operations.

To answer the aforementioned questions, this article shall analyze the applicability of the following scientific experiments to realizing the aforementioned operational opportunities in prisons. The findings of the "Stanford University Prison Experiment," involving students assuming roles of both prisoner and prison guard within a prison environment and the "Milgram experiment," showcasing obedience to authority versus individual conscience, will be applied to the U.S. military's handling of said facilities, showcasing failures to identify solutions. Had the U.S. military morally acted as an experimental authority over its facilities' prisoner *and* guard subjects to create the conditions/environment to proactively develop CIs, these facilities would have arguably represented a revolutionary paradigm shift from den of thieves to golden intel egg-laying goose in terms of the U.S. military world view applied to prison camp management.

What if morality, ethics, and the rule of law (i.e. Geneva Convention), which were lacking at Abu Ghraib, had been clearly communicated and inculcated into these facilities' guards by military leadership as the crux to realizing the operational opportunities defined above? Had U.S. military senior leadership clearly prioritized to its staff the long-term mission

importance of CI cultivation and control within these facilities and had the same leadership emphasized how important this was to future undercover missions throughout the world, the U.S. might have put itself in a better position to disrupt or dismantle terrorist or criminal groups. This case study asserts that had the U.S. military appropriately leveraged the Stanford Prison and Milgram experiment findings to Abu Ghraib and other camps under its dominion and control, it would have realized significant opportunities to 1) cultivate and control high-value CIs to be purposely infiltrated within the jihadi community, and 2) proactively leverage these CIs, via long-term undercover operations, to obtain actionable operational intelligence into future destructive plots. However, because the U.S. military had not leveraged the Milgram and Stanford Prison Experiments' findings to the prisons it controlled, it missed being able to capitalize on said operational opportunities.

> **What if morality, ethics, and the rule of law...had been clearly communicated and inculcated into these facilities' guards...?**

Background

The Milgram Experiment (1961)

The Milgram Experiment attempted to measure the obedience of people to authority figures and it was led and conducted by Yale University Psychologist Stanley Milgram in July 1961, shortly after the beginning of the trial of Nazi Adolf Eichmann for war crimes he had committed during World War II. Among a number of research questions, the Milgram Experiment sought to answer a particular question: "Could it be that Eichmann and his million accomplices in the Holocaust were just following orders? Could we call them all accomplices?"[9] The Milgram Experiment

measured study participants' willingness to obey an authority figure who instructed them to do things that went against their personal conscience.

The teachers, who were the subjects of the [Milgram Experiment], all believed that for each wrong answer, the learner was receiving real shocks...

In the Milgram Experiment there were three persons involved, each with a distinct role: 1) the experimenter ran the experiment (an authoritative role); 2) the subjects of the experiment, all male volunteers, role-played as the teacher (obeyed the experimenter's orders); and 3) the learner was a confederate of the experimenter pretending to be a volunteer (received stimulus from the teacher). The teacher and learner were taken into an adjacent room where the learner was strapped into what appeared to be an electric chair with electrodes attached to the learner's arms, with the experimenter telling the subject teachers that this was to ensure that the learner would not escape.[10] The learner and teacher were put in separate rooms and could communicate with one another but not see each other. The teacher and experimenter together went into a room adjacent to the learner, where the teacher could see and use an electric shock generator and a row of switches marked from 15 volts, defined as a slight shock, to 375 volts defined as danger/severe shock, to 450 volts, defined only as "XXX." Prior to the actual experiment starting, the teacher (volunteer) was given a sample electric shock so that he could personally experience what the learner would feel when the learner was given shocks. The teacher was then given a list of word pairs that he was to teach the learner and then instructed to read the word pairs to the learner, beginning with the first word of each pair and reading four possible answers. The teacher would give a shock to the learner each time the learner gave a wrong answer and the shocks increased in 15-volt increments for each of the learner's wrong responses. If correct, the teacher would read the next word pair without administering a shock.[11]

The teachers, who were the subjects of the experiment, all believed that for each wrong answer, the learner was receiving real shocks, but in actuality, the learners weren't receiving any real shocks at all. After the confederate learner was separated from the teacher, the confederate played pre-recorded sounds for each shock level administered by the teacher, making electroshock generator sounds that the teacher heard each time the teacher administered a shock to the learner. The confederate actor also started to bang on the wall that separated him from the teacher after each voltage level increase and after banging on the wall a couple of times and complaining about his heart condition, the confederate learner stopped responding to any shocks administered by the teacher.[12] At this point, a number of subject teachers wanted to stop the experiment and check on the learner, with several subject teachers pausing at 135 volts and questioning the experiment's purpose. However, most continued after being assured that they would not be held responsible. Some subject teachers started to nervously laugh or show signs of extreme stress when they heard screams of pain coming from the learner.[13]

Whenever a subject teacher said that he wanted the experiment to stop, the experimenter would tell the subject the following, in this order:[14]

1. Please *continue*.

2. The experiment requires that you *continue*.

3. It is absolutely essential that you *continue*.

4. You have no other choice, you *must* go on.

The experiment was stopped if the teacher still wished to stop after the experimenter had

given all four of the aforementioned verbal prods, otherwise, the experiment was stopped if the teacher had given the maximum 450-volt shock three times in a row. If the teacher raised concerns about his conduct during the experiment, the experimenter would say certain things to see if the teacher would continue. One of the questions asked by teachers was whether or not the learner would be permanently harmed physically, to which the experimenter would tell the teacher that there wouldn't be any permanent physical injury despite the shocks being painful. If the teacher said that the learner clearly wants to stop, the experimenter replied, "Whether the learner likes it or not, you must go on until he has learned all the word pairs correctly, so please go on."[15]

The first set of Milgram Experiment results revealed that 65 percent (26 of 40) of experiment participants (teachers) administered the experiment's final massive 450-volt shock,[16] though many were uncomfortable doing so. All participants paused and questioned the experiment at points during the experiment, with some subjects stating that they would refund the money they had been paid for participating in the experiment. Throughout the Milgram Experiment, subjects displayed different levels of stress and tension, such as sweating and trembling, with some even having nervous laughing fits or seizures.[17]

In his 1974 article, "The Perils of Obedience," Milgram said that he tried to see how much pain a regular person (experiment's subject) would exact on another person just because he was told to do so by an authority figure. He concluded that experimental subjects, who had no pre-disposed inclination to hurting others (i.e., Philip Zimbardo's dispositional or inherent evil argument, explained in the next section), clearly knew that they were doing so just because they were told to by an authority figure the subject did not have the wherewithal to resist.[18]

In summary, the Milgram Experiment revealed that approximately 2 out of 3 people were prepared to obey authority, although unwillingly, even if those people believed they were causing serious injury and distress.

> ...the Milgram Experiment revealed that approximately 2 out of 3 people were prepared to obey authority...

The Stanford Prison Experiment (1971)

The Stanford Prison Experiment was a study funded by the U.S. Office of Naval Research based on the U.S. Navy's and U.S. Marine Corps' interest in the causes of conflict between military guards and prisoners.[19] Led by Stanford University Professor Philip Zimbardo, this experiment occurred between August 14 and 20, 1971, and sought to determine whether "the brutality reported among guards in American prisons was due to the sadistic personalities of the guards (i.e., dispositional) or had more to do with the prison's social structure/environment (i.e., situational)."[20] The experiment involved 24 Stanford University male students who were randomly selected out of an original 75 volunteers to randomly play either the role of prisoner or guard and to live and interact in a mock prison in the basement of the Stanford University psychology building. There were a total of 10 prisoners, 11 guards, and 2 reserves, all picked at random from these 24 volunteers. Researchers set up the prison environment to be as realistic as possible, though one of the main rules during the experiment was that no physical violence was allowed. Deindividualization also occurred, wherein prisoners could only refer to each other by number as to make each one feel anonymous. Guards wore the same uniform, possessed whistles and batons, and had been instructed by researchers to do whatever they needed to in order to maintain law and order and the prisoners' respect.

On the second day of the experiment, a prisoners' rebellion ensued and guards were called in for reinforcement. Guards stripped prisoners naked and also put prisoner ringleaders into solitary confinement. Some of the resulting effects of the Stanford Prison Experiment on the prisoners, as based on the guards' abusive behavior, were "acute emotional disturbance, disorganized thinking, uncontrollable crying (3 prisoners) and rage."[21] Experimenters tried to get one of the prisoners to leave the experiment but this prisoner said he couldn't leave because other prisoners had labeled him a bad prisoner. Zimbardo had to go out-of-role to remind the student that this was just an experiment, and that he and the others were students, not prisoners, in order to convince this student to leave.[22]

[The Stanford Prison Experiment] conclusions were that the prison's social structure and environment...caused the guards and prisoners to behave the way that they did...

The experiment was supposed to last two weeks but ended after six days when Stanford Ph.D. student Christina Maslach, who was supposed to interview the guards and prisoners, objected to the abuse that the guards had inflicted on the prisoners. She was the only person to question the morality of the experiment, out of roughly 50 outsiders who observed the prison conditions.[23]

This experiment's conclusions were that the prison's social structure and environment (situational explanation) caused the guards and prisoners to behave the way that they did and not because the guards or prisoners had a sadistic or passive disposition (dispositional explanation) prior to the start of the experiment. Another Stanford Prison Experiment finding was that the experimental subjects had conformed to stereotyped social roles that persons in that

situational circumstance (prison environment) were expected to play. Also, deindividualization among the guards was found to have contributed to the loss of individual morality because of their being surrounded by the guards' group norm of brutality.[24] Among the prisoners, learned helplessness exhibited itself so that whatever a prisoner did had no effect on the guards' treatment of the individual prisoner.

After the experiment, students said they couldn't believe they behaved in the brutalizing (guards) or subservient (prisoners) manner that they did. Three types of guards emerged from the interview of prisoners: 1) tough but fair guards who followed prison rules; 2) guards who were "good guys" who did little favors for the prisoners and never punished them; and 3) about a third of the guards were hostile, arbitrary, and inventive in their forms of prisoner humiliation—these guards appeared to thoroughly enjoy the power they wielded, yet none of the Stanford Prison Experiment's preliminary personality tests were able to predict this behavior.[25] Zimbardo made observations throughout the experiment and had role-played as the prison superintendent, later saying in 2008 that, "It wasn't until much later that I realized how far into my prison role I was at that point—that I was thinking like a prison superintendent rather than a research psychologist."[26] The Stanford Prison Experiment results showed that the students who role-played as prison guards exercised authoritarian measures and even subjected the students who role-played as prisoners to torture.

Undercover Operations

For purposes of defining undercover operations for this case study, the open-source definitions set forth by the Undercover and Sensitive Operations Unit, Attorney General's Guidelines on Federal Bureau of Investigations (FBI) Undercover Operations, revised 11/13/92, shall be used:[27]

Undercover operations are investigations involving a series of related undercover

activities over a period of time by an undercover employee. A "series of related undercover activities" generally consists of more than three separate contacts by an undercover employee with the individual(s) under investigation. "Undercover activities" means any investigative activity involving the use of an assumed name or cover identity by an employee of the FBI or another Federal, state, or local law enforcement organization working with the FBI. However, undercover activity involving sensitive or fiscal circumstances constitutes an undercover operation regardless of the number of contacts involved. An "undercover employee" means any employee of the FBI, or employee of a Federal, state, or local law enforcement agency working under the direction and control of the FBI in a particular investigation, whose relationship with the FBI is concealed from third parties in the course of an investigative operation by the maintenance of a cover or alias identity. A registered confidential informant may also be deemed an "undercover employee" for purposes of this definition. An undercover operation may also utilize a "proprietary," which means a sole proprietorship, partnership, corporation, or other business entity operated on a commercial basis, which is owned, controlled, or operated wholly or in part on behalf of the FBI, and whose relationship with the FBI is concealed from third parties. Please note that even though the aforementioned undercover operations definitions are that of the U.S. Attorney General's Office for the FBI, the author asserts that they also apply to other U.S. law enforcement agencies.

Confidential Informants

As defined by the open-source "U.S. Government Accountability Office's Report To The Chairman, Committee On The Judiciary, U.S. Senate, Confidential Informants: Updates To Policy And Additional Guidance Would Improve Oversight By [U.S. Department of Justice] And [U.S. Department of Homeland Security] Agencies" (September 2015): confidential informants provide information and take action at the direction of law enforcement agencies to further investigations, and agencies may rely on confidential informants in situations in which it could be difficult to utilize an undercover officer.[28] An informant can be motivated by many factors, including financial gain or reduced sentencing for criminal convictions. confidential informants who assist Department of Justice or Department of Homeland Security law enforcement agencies often have criminal histories, though some are concerned citizens with no criminal connections.[29] Additionally, the identities of CIs are privileged in order to protect these individuals against retribution from those being investigated and involved in crime.[30]

> **U.S. Army personnel were found to have committed human rights violations against detainees at Abu Ghraib...**

Abu Ghraib Prison Camp

Abu Ghraib was a prison that had been used by Saddam Hussein to hold approximately 50,000 men and women in squalid conditions where torture and execution were frequent.[31] Following the invasion of the U.S. military and allied forces, the U.S. Army refurbished it and turned it into a military prison, which became the largest of several detention centers in Iraq used by the U.S. military.[32, 33] In April 2004, CBS News published photographs of the abuse by the U.S. Army and brought the crimes committed at Abu Ghraib to the world's attention. U.S. Army personnel were found to have committed human rights violations against detainees at Abu Ghraib,[34] and according to the CNN article, these abuses included torture and sexual abuse.[35] In subsequent U.S. military trials of crimes related to the abuse and humiliation of Abu Ghraib prisoners, 11 U.S. soldiers were convicted.[36]

Analysis

The one glaring shortcoming of the U.S. military's performance at Abu Ghraib, besides the atrocities that it inflicted upon prisoners, was that it had a chance to apply the findings of both the Milgram and Stanford Prison experiments, the latter ironically being a study it had funded, to prevent the atrocities and negative outcomes that occurred. As the saying goes, "hindsight is 20/20" and rather than illuminate and criticize all of the shortcomings that occurred at Abu Ghraib and other U.S. military prison camps, and there are many, it is hoped that the following provides solutions to these shortcomings. As the Milgram Experiment conclusions showed, and because the U.S. military is a hierarchy wherein strictly following and complying with the chain of command is expected, it is more likely than not that a U.S. soldier at Abu Ghraib

> ...psychological testing to become a U.S. soldier was not a prerequisite for the 11 soldiers convicted at Abu Ghraib.

or any one of the prison camps run by a U.S. military chain of command would have explicitly followed the orders of an authority figure, even if those orders were abusive. Realizing that soldiers are sensitive to the authority of his chain of command, military leadership (and again, the emphasis on leadership cannot be overstated) must be cognizant of proactively giving legal and moral orders, despite how heinous the environment (i.e., prison camps) might be. The Stanford Prison Experiment's situational argument for why atrocities might be committed in a prison environment should not be subconsciously used by military leadership as an excuse or crutch for atrocities that occur from having given immoral or illegal orders to subordinates. Zimbardo himself asserted that

the environment was to blame for U.S. Army soldiers at Abu Ghraib having committed atrocities, succinctly asking, "Should these few Army reservists be blamed as the 'bad apples' in a good barrel of American soldiers, as our leaders have characterized them? Or are they the once-good apples soured and corrupted by an evil barrel? I argue for the latter perspective after having studied the psychology of evil for many decades. In fact, I have been responsible for constructing evil barrels that produced many bad apples."[37] However, this argument can be attacked and is indeed countered by the fact that possible sadistic traits may already exist in some U.S. military recruits, as psychological testing to become a U.S. soldier was not a prerequisite for the 11 soldiers convicted at Abu Ghraib. In fact, it wasn't until 2014 that a new mental health screening bill, which supporters say could help stem the high rate of U.S. military suicides or even stop shooting rampages, passed the U.S. House of Representatives as part of the 2015 defense budget. This bill directed the National Institutes of Health's mental health unit to develop a screening procedure for those who want to join the military.[38] According to U.S. Army studies published in March 2014 by the *Journal of the American Medical Association*, 1 in 5 soldiers had a common mental disorder, and more than 1 in 100 had a past suicide attempt.[39] These studies also found that suicides among service members who had never deployed to war zones had risen, despite perceptions that combat trauma drove suicide rates.[40]

Even though one of Zimbardo's main arguments was that the situation created the monster, it must be noted that the monster may have already existed in some of the U.S. soldiers at Abu Ghraib, and that official psychological/emotional screening methods for new soldiers had not been employed by the U.S. military for the 11 convicted soldiers at Abu Ghraib. Taking the analysis further, even if U.S. military psychological/emotional screening for the 11

soldiers did exist and these 11 had never become soldiers and another 11 different soldiers who had passed the screening were subjected to the Abu Ghraib prison environment, would the monster still have showed itself in these other 11 soldiers? If the reader of this article believes Zimbardo's argument holds true and constant absent dispositional factors of the soldier, that the situational influence of Abu Ghraib is stronger than a soldier's disposition for overcoming negative situational influences, then yes, potential monsters and cruel acts would also be evident in this other 11 soldier sampling. As Milgram stated in 1974, "Ordinary people, simply doing their jobs, and without any particular hostility on their part [i.e., dispositional], can become agents in a terrible destructive process."[41] Because the Milgram Experiment (1961) occurred before the Stanford Prison Experiment (1971), and because Zimbardo himself was fully aware of the former experiment before conducting his own—and had actually noted to Milgram that Milgram's participants who had refused to administer the final shocks, neither insisted that the experiment be terminated, nor left the room to check the health of the victim without requesting permission to leave[42]—could it be possible that Zimbardo was reinforcing his non-dispositional hypothesis to explain atrocities committed by an experimental subject by reinforcing Milgram's non-dispositional attribution? The importance of this question lies in the fact that if it is valid and true that the situation causes people to commit evil acts, and that this is further detrimentally compounded by the influence of authority facilitating the acts, then the U.S. military who funded the Stanford Prison Experiment should have benefited from the conclusions of both experiments and applied these findings (which it had received decades earlier) to the environment that was Abu Ghraib.

As Zimbardo would have us believe, if the situation will always dominate a soldier's dispositional ability to overcome that situation, i.e., an environment as challenging as Abu Ghraib, then this "nature overcoming nurture" dominance makes the Milgram Experiment's findings and applicability to military leadership even more important because military leadership's cognizance of subordinates' sensitivity to obeying authority allows that leadership to firmly and unequivocally communicate 1) the terms of engagement with prisoners and how interacting with prisoners can facilitate CI cultivation and control, and 2) what CI cultivation means for either military or law enforcement undercover operations to disrupt/dismantle a criminal/terrorist organization. Even if the soldier were innately evil, Milgram's findings attest to the importance of moral authority exercised by military leadership to overcome the dispositional argument. Moral military leadership and its correlating orders could have created the following outcomes for U.S. military, law enforcement, and intelligence units, opposite of what actually occurred at Abu Ghraib:[43]

> **...Milgram's findings attest to the importance of moral authority exercised by military leadership...**

Framing

Reinforce to subordinate soldiers that Abu Ghraib represented opportunities for appropriate personnel (CIA case officers or those who could operationalize intelligence information obtained from prisoners) to cultivate and control informants in the fight against terrorism.

Rapport

Tell subordinate soldiers that the only way to accomplish the aforementioned described in "Framing" was to treat prisoners with dignity and to develop rapport with same. As stated by a U.S. law enforcement lieutenant:

The real key to gathering information is

in the development of relationships with the people you encounter and with them broaching the subject of crime. Some of the biggest arrests I've seen were the result of patrol officers getting information from people they have arrested for minor infractions. What these officers simply did was treat the arrestees with dignity and respect and simply asked them if they knew anything about any crimes. It is amazing how willing people are to talk, but it is even more amazing how some police officers are unwilling to listen. Develop a positive relationship with the people you encounter while on the job and you cultivate potential informants. They can be people you assist, arrest, or just chat with in any capacity. Take the opportunity to listen to them, understand their perspectives and concerns, establish trust, educate, and ultimately make yourself available—you will soon find yourself with a flock of people willing to tell you stuff.[44]

> **There does not appear to be any open-source evidence of situations where despite cruel treatment by prison guards, good intelligence was gathered or reliable CIs were cultivated.**

Independent Corroboration

Assuming that CIs are successfully cultivated by U.S. government personnel from a sea of prisoners and they provide information, this information must then be independently corroborated to ensure accuracy and to prevent negative outcomes from happening by acting on bad information. Even if positive rapport between U.S. government personnel and the CI occurred, which would presume information so obtained would not be as unreliable as that obtained through coercion, it can be presumed that there could still be prisoners who are loyal to the terrorist ideology and who would exercise

counterintelligence tradecraft to make the person controlling the CI ("controlling agent") hear what they wanted to in order to receive rewards of one type or another.

Using CIs in Targeted Undercover Operations

Once a CI has been deemed a reliable CI, based on that CI's information being independently corroborated over a period of time, the controller could then use the CI to infiltrate an identified terrorist or criminal organization in order to obtain actionable intelligence or prosecutable evidence. Going back to the importance of framing described previously, the cultivation of CIs in targeted undercover operations is what military leadership needs to communicate and even order as a performance metric to ensure that potentially negative perceptions of Abu Ghraib are framed positively to counter any evil dispositional tendencies being realized by innately cruel soldiers.

Counterargument

A counterargument to the above analysis and thesis would be whether or not there are any examples of prisons/camps where substantive intelligence collection or CI cultivation opportunities were not missed, despite cruel treatment by prison guards. There does not appear to be any open-source evidence of situations where despite cruel treatment by prison guards, good intelligence was gathered or reliable CIs were cultivated. In fact to the contrary, open-source information revealed that despite the military having funded the Stanford Prison Experiment and knowing about the conclusions from this experiment and that of the Milgram Experiment decades before prisoner abuses at the various U.S.-controlled prisons and camps, it did not apply these findings to the prisoners at Abu Ghraib or Guantánamo Bay ("Gitmo"), another publicized prison camp run by the U.S. military where abuses also occurred.[45] Though U.S. officials asserted that information obtained from Gitmo detainees revealed terrorist

cells, prevented terrorist attacks and provided important intelligence about Al Qaeda, the *New York Times* asserted that U.S. government and military officials have repeatedly exaggerated both the danger (Gitmo) detainees posed and the intelligence they provided.[46] Furthermore, the aforementioned *Times* article asserted that "while some Guantánamo intelligence has aided terrorism investigations, none of it has enabled intelligence or law-enforcement services to foil imminent attacks… Compared with the higher-profile Al Qaeda operatives held elsewhere by the CIA, the Guantánamo detainees have provided only a trickle of intelligence with current value."[47]

Conclusion

The Stanley Milgram Experiment concluded that people were willing to obey authority, even if they questioned the authority's commands, as they clearly knew that by obeying the commands their actions were inflicting pain to others. The Philip Zimbardo Stanford Prison Experiment stated that situational dynamics, such as group norms and deindividualization within a prison environment caused one group of test subjects (guards) to commit atrocities against another (prisoners). This article's thesis argued that to counter the situational conclusion posited by Zimbardo, wherein people committed atrocities as a function of a negative environment that a person finds himself in, the authority entity (U.S. military leadership) needs to understand and leverage Milgram's findings to ensure that moral leadership that gives legal and moral commands towards a framed goal (CI cultivation, using undercover operations) is firmly and unequivocally ordered in a prison environment to overcome any inherently dispositional (evil) tendencies of subordinate soldiers that formal screening methods (psychological testing) might miss. A clear legal and moral game plan at Abu Ghraib and the moral and legal application of authority by military leadership would have

been the keys to cultivating CIs and advancing undercover operations with these CIs.

> **A clear legal and moral game plan at Abu Ghraib and the moral and legal application of authority by military leadership would have been the keys to cultivating CIs and advancing undercover operations with these CIs.**

Even though prison abuse and "enhanced interrogation techniques" (a euphemism for torture) occurred at Gitmo outside the boundaries of the Geneva Convention,[48] the assertion by U.S. officials that substantive intelligence was still gathered as a result of guards being cruel is questionable. However, if it were true that reliable CIs were cultivated and actionable intelligence gathered as a result of guards being cruel, this would effectively attack this case study's thesis, with the caveat that quantitative performance metrics (number of arrests, indictments, convictions, terrorist financing dollars seized, number of terrorist acts thwarted) would need to be proffered in support of the effectiveness of information obtained cruelly by guards. As evidence that information obtained cruelly has little value, Lieutenant Colonel Anthony Christino III, a retired Army intelligence officer who specialized in counterterrorism and was familiar with the Guantánamo intelligence stated:

> I doubt that anyone (prisoners) detained at Guantánamo ever had access to that type of information; if some claim that they did, they probably did so to either earn the incentives or avoid the maltreatment that General Miller instituted. The quality of the interrogations and the quality of the analysis were all very poor. Efforts were made to improve things, but after decades of neglect of human intelligence skills, it can't be fixed in a few years.[49]

According to *The Guardian*, Christino's conclusions were backed by three other intelligence officials, who spoke on condition of anonymity. One, a 30-year veteran of the FBI who worked on tracking terrorist financing, said, "I'm unaware of any important information in my field that's come from Gitmo…. It's clearly not a significant source."[50]

A recurring theme throughout this article is contemporary military leadership not applying lessons learned from the past, even when it was the military who funded the very experiments and research that brought those answers. The glaring example is the U.S. Office of Naval Research funding the Stanford Prison Experiment to determine the causes of conflict between military guards and prisoners, only to abandon those findings decades later. However, the *New York Times* published an article in 2004 that showed American and foreign officials becoming increasingly concerned about Guantánamo detainees who posed little threat to the United States becoming radicalized by the conditions of their imprisonment and those held with them.[51] A senior Arab intelligence official familiar with Guantánamo operations said, "Even those who were not hard-core extremists have now been indoctrinated by the true believers. Like any other prison, they have been taught to hate. If they let these people go, these people will make trouble."[52]

In the words of philosopher George Santayana, "those who cannot remember the past are condemned to repeat it." In 2006, decades after the findings of the Milgram and Stanford Prison Experiments had been published, U.S. military leadership of prison camps missed opportunities to cultivate, because of the conduct of their subordinate charges, arguably one of the highest value human intelligence assets during the post-9/11 war on terror. That asset was Oussama Atar, who was imprisoned at Camp Cropper and who had been radicalized in U.S. custody, perhaps due in part to mistreatment. Because the U.S. military missed the opportunity to cultivate Atar as a CI, it also missed the opportunity to use Atar and others like him to proactively infiltrate worldwide terrorist or criminal networks and obtain actionable intelligence on terror/criminal plots. Atar, who had met Abu Bakr al-Baghdadi, the creator of ISIS and its presumed leader, in such a facility,[53] clearly would have had access to the highest echelons of ISIS terrorist leadership and the leadership of associated terrorist networks. *IAJ*

Notes

1   Rosenberg, Carol. 2017. "Guantánamo Prison: A Primer". Miami Herald. http://www.miamiherald.com/news/nation-world/world/americas/guantanamo/article1939250.html.

2   Davis, Morris D. 2009. "Historical perspective on Guantánamo Bay: the arrival of the high value detainees."

3   eMediaMillWorks, "President Bush Addresses the Nation". 2001. *Washingtonpost.Com*. http://www.washingtonpost.com/wp-srv/nation/specials/attacked/transcripts/bushaddress_092001.html.

4   Shinkman, Paul D. 2013. "Obama: 'Global War on Terror' Is Over". Usnews.Com. https://www.usnews.com/news/articles/2013/05/23/obama-global-war-on-terror-is-over.

5   HASSAN, ATEF. 2009. "U.S. Closes Big Military Prison in Iraq". Msnbc.Com. http://www.nbcnews.com/id/32884156/ns/world_news-mideast_n_africa/t/us-closes-big-military-prison-iraq/#.Wht1tkqnE2w.

6   CNN exclusive investigation Erin McLaughlin and Margot Haddad; written with Lauren Said-Moorhouse, CNN. 2017. "How Top ISIS Operative Slipped Through the Net". CNN. http://www.cnn.com/2017/03/16/europe/oussama-atar-profile/index.html.

7   Khatib, Lina. 2015. "How Blackwater And Other Horrors Are Used by ISIS - CNN". CNN. http://www.cnn.com/2015/04/15/opinions/blackwater-abu-ghraib-isis/index.html.

8   Postel, Thérèse. 2013. "How Guantanamo Bay's Existence Helps Al-Qaeda Recruit More Terrorists". The Atlantic. https://www.theatlantic.com/international/archive/2013/04/how-guantanamo-bays-existence-helps-al-qaeda-recruit-more-terrorists/274956/.

9   Stanley, Milgram. "Obedience to authority." *An Experimental View* (1974)

10   Milgram, Stanley. 1963. "Behavioral Study of Obedience." The Journal of Abnormal and Social Psychology 67 (4): 371-378. doi:10.1037/h0040525.

11   Ibid.

12   Ibid.

13   Ibid.

14   Ibid.

15   Ibid.

16   Ibid.

17   Ibid.

18   Milgram, Stanley (1974). *"The Perils of Obedience"*. Harper's Magazine. Archived from the original on December 16, 2010.

19   "The Stanford Prison Experiment". 2015. Psychology Today. https://www.psychologytoday.com/blog/the-time-cure/201507/the-stanford-prison-experiment.

20   "Stanford Prison Experiment | Simply Psychology". 2015. Simplypsychology.Org. https://www.simplypsychology.org/zimbardo.html.

21   Zimbardo, Philip G., Craig Haney, W. Curtis Banks, and David Jaffe. *The Stanford prison experiment*. Zimbardo, Incorporated, 1971.

22   Ibid.

23   Haney, Craig, W. Curtis Banks, and Philip G. Zimbardo. "A study of prisoners and guards in a simulated prison." *Naval research reviews* 9, no. 1-17 (1973).

24   Milgram, Stanley, and Christian Gudehus. "Obedience to authority." (1978).

25   Haney, Craig, W. Curtis Banks, and Philip G. Zimbardo. "A study of prisoners and guards in a simulated prison." *Naval research review* 9, no. 1-17 (1973).

26   "Stanford Prison Experiment | Simply Psychology". 2015. Simplypsychology.Org. https://www.simplypsychology.org/zimbardo.html.

27   Undercover and Sensitive Operations Unit, Attorney General's Guidelines on FBI Undercover Operations, November 13, 1992 | AG | Department of Justice". 2017. Justice.Gov. https://www.justice.gov/archives/ag/undercover-and-sensitive-operations-unit-attorney-generals-guidelines-fbi-undercover-operations#definitions.

28   "U.S. Government Accountability Office, Report to The Chairman, Committee on The Judiciary, U.S. Senate; CONFIDENTIAL INFORMANTS: Updates to Policy and Additional Guidance Would Improve Oversight by DOJ And DHS Agencies". 2015. Gao.Gov. http://www.gao.gov/assets/680/672514.pdf.

29   Ibid.

30   US Legal, Inc. 2017. "Confidential Informant Law and Legal Definition | Uslegal, Inc.". Definitions. Uslegal.Com. https://definitions.uslegal.com/c/confidential-informant.

31   Hersh, Seymour M. "Torture at Abu Ghraib." (2004).

32   Ibid.

33   Murphy, Sean D. "US abuse of Iraqi detainees at Abu Ghraib Prison." *The American Journal of International Law* 98, no. 3 (2004): 591.

34   Scherer, Michael, and Mark Benjamin. 2003. "Other Government Agencies". *Salon.Com*. https://web.archive.org/web/20080212035108/http://www.salon.com/news/abu_ghraib/2006/03/14/chapter_5/index.html.

35   "CNN.Com – Iraq Prison 'Abuse' Sparks Outrage - Apr 30, 2004". 2017. Cnn.Com. http://www.cnn.com/2004/WORLD/meast/04/30/iraq.photos.reaction/index.html.

36   Bierman, Noah. 2015. "Few Have Faced Consequences for Abuses at Abu Ghraib Prison in Iraq." Latimes.Com. http://beta.latimes.com/nation/la-na-abu-ghraib-lawsuit-20150317-story.html.

37   Zimbardo, Philip G. 2004. "Boston.Com / News / Boston Globe / Opinion / Op-Ed / Power Turns Good Soldiers Into 'Bad Apples'". Archive.Boston.Com. http://archive.boston.com/news/globe/editorial_opinion/oped/articles/2004/05/09/power_turns_good_soldiers_into_bad_apples/.

38   Tritten, Travis J. 2014. "House Passes New Recruit Mental Health Screening". Military.Com. http://www.military.com/daily-news/2014/05/23/house-passes-new-recruit-mental-health-screening.html.

39   Ibid.

40   Ibid.

41   Milgram, Stanley (1974). *"The Perils of Obedience"*. Harper's Magazine. Archived from the original on December 16, 2010

42   "Resource: Discovering Psychology: Updated Edition". WGBH Educational Foundation. 2001. Learner.Org. https://www.learner.org/resources/series138.html.

43   For contextual purposes and to validate the following discussion of CIs, undercover operations, and the missed opportunities at Abu Ghraib, it is hereby noted that the author of this case study has been a practitioner of U.S. federal law enforcement and its accompanying instruments and tools of U.S. national power for over 22 years. Specifically, this practitioner-scholar has cultivated, controlled, registered, paid and overseen a number of CIs as the initiating/controlling operational agent and has paid/authorized the payment of millions of U.S. dollars to CIs who have advanced lawful criminal investigations on behalf of the U.S. government. Additionally, the practitioner has established, utilized, managed, and written national policy for U.S. federal law enforcement undercover operations.

44   Glennon, Lieutenant Jim. 2008. "Developing Informal Informants". Policeone. https://www.policeone.com/police-products/training/services/articles/1766841-Developing-informal-informants.

45   Fenton, Jenifer. 2011. "Ex-Guantanamo Guard Tells of Violence Against Detainees - CNN". CNN.

http://www.cnn.com/2011/10/28/world/meast/guantanamo-guard/index.html.

46   Golden, Tim, and Don Van Natta Jr. 2004. "THE REACH OF WAR; U.S. Said to Overstate Value of Guantánamo Detainees". Nytimes.Com. http://www.nytimes.com/2004/06/21/world/the-reach-of-war-us-said-to-overstate-value-of-guantanamo-detainees.html.

47   Ibid.

48   Ibid.

49   Rose, David. 2004. "The Real Truth About Camp Delta". The Guardian. https://www.theguardian.com/world/2004/oct/03/bookextracts.usa.

50   Ibid.

51   Golden, Tim, and Don Van Natta Jr. 2004. "THE REACH OF WAR; U.S. Said To Overstate Value Of Guantánamo Detainees". Nytimes.Com. http://www.nytimes.com/2004/06/21/world/the-reach-of-war-us-said-to-overstate-value-of-guantanamo-detainees.html.

52   Ibid.

53   CNN exclusive investigation Erin McLaughlin and Margot Haddad; written with Lauren Said-Moorhouse, CNN. 2017. "How Top ISIS Operative Slipped Through the Net". CNN. http://www.cnn.com/2017/03/16/europe/oussama-atar-profile/index.html.

The First 21st Century
Water War

by J. M. Landreth

If the wars of this century were fought over oil, the wars of the next century will be fought over water — unless we change our approach to managing this precious and vital resource.

— Ismail Serageldin, 1995

D r. Ismail Serageldin, founding director of Bibliotheca Alexandria, forecasted in 1995 that wars in the 21st century would be fought over water rather than oil. While an increasing number of countries are experiencing fresh water shortages, Serageldin's prophesy may first come true in his native country, Egypt.

Egypt's history and modern-day economy inextricably link to a healthy Nile River. However, large dam construction in upstream Ethiopia may soon jeopardize the strength of the Nile in Egypt. The case of the Grand Ethiopian Renaissance Dam (GERD) provides a window into the future and is instructive for the international community on the evolving nature of water insecurity. If the U.S. wishes to aid in the peaceful resolution of the GERD issue, then the U.S. must martial a truly interagency approach since the Nile bridges many of the geographic seams that divide U.S. military, intelligence, and diplomatic institutions. The U.S.'s approach towards the GERD must leverage the existing network of allies and regional partners, not conflict with existing or create new kinetic conflicts and harmonize with the U.S.'s strategy towards the Great Power Competition.

In each section of this article, I outline various concerns and potential areas of contention, providing recommendations to alleviate these problems. A complete listing of recommendations can be found at the end of this article.

Lieutenant Commander James Landreth is a U.S. Navy submarine officer. He holds degrees from the U.S. Naval Academy (B.S.) and the University of South Carolina (M.Eng.), and completed Joint Professional Military Education at the U.S. Naval War College. Landreth publishes frequently on joint interagency matters and is a veteran of U.S. Central Command's Plans, Policy and Strategy Directorate.

Framing the Issue of the Grand Ethiopian Renaissance Dam

While Egypt's attention was dominated by domestic issues related to the Arab Spring, in 2011 Ethiopia began construction of the GERD. When completed the dam will supply 6.45 gigawatts of electrical generation capacity—the largest hydroelectric power plant in Africa. The GERD will be filled by the Blue Nile, one of two rivers upstream of Egypt's Nile River. In order for Ethiopia to receive a timely return on investment on the GERD, the dam operator is economically incentivized to fill the dam as fast as possible—a multi-year task on the most aggressive track.

However, if the Ethiopian's impound rate of the Blue Nile exceeds 15% of total volumetric flow, then the detrimental impacts to fresh water in Sudan and Egypt will be significant.[1] Such a loss in fresh water flow would have devastating consequences to agriculture, fresh water access, waste water treatment, fisheries, and other adjacent industries.

Additionally, the Nile River spreads across a huge delta as it enters the Mediterranean. The Nile River Delta depends on a certain amount of freshwater flow to maintain a balance with the saline Mediterranean. If fresh water flow dramatically diminishes, then seawater will encroach upon the delta. The salination of the delta could have disastrous and largely irreparable consequences upon the delta's biome, which would further harm Egypt's economy.

While the current Egyptian administration is diplomatically engaging with Ethiopia, past leaders and security officials have threatened Ethiopia with war over the GERD.[2] Additionally, even if Egypt and Ethiopia can come to a diplomatic solution over the Nile's impoundment rate to fill the GERD, Sudan's fragile security situation could deteriorate further and create conditions that nullify prior diplomatic efforts.

Leverage Existing Network of U.S. Allies and Regional Partners

The Nile River: Straddling the Seams

While the United State maintains multiple cabinet-level agencies engaged in international affairs, the U.S. Department of Defense possesses the largest budget and most personnel. Additionally, it has robust liaison channels with the intelligence community. Also, due to long term security challenges within the near east, the Department of Defense arguably has an outsized role in developing U.S. strategy for the region.

> **...if the Ethiopian's impound rate of the Blue Nile exceeds 15% of total volumetric flow, then the detrimental impacts to fresh water in Sudan and Egypt will be significant.**

While the GERD does not currently represent a security threat for the U.S., the conflict that could evolve would likely obligate Defense resources. Regardless of whether Department of Defense receives designation as the lead agency for implementation of U.S. policy towards the coming crisis, the following analysis provides a framework for Department of Defense and the interagency's resource planning efforts for the GERD and provides context for many of the critical security issues that define the region.

The U.S. military engages the globe via geographic combatant commands. The Nile River bridges the seams between three combatant commands: U.S. Africa Command (AFRICOM), U.S. Central Command (CENTCOM) and U.S. European Command (EUCOM). Additionally, the GERD issue directly affects the equities of the U.S. Indo-Pacific Command. In addition to geographic combatant commands, the U.S. military maintains functional combatant commands that provide specific capabilities

to the geographic combatant commands. U.S. Transportation Command, Special Operations Command, and Cyber Command would likely receive orders to support any U.S. military engagement surrounding the GERD.

Recommendations

R1. Office of the Secretary of Defense: Coordinate with the Joint Staff to designate supported and supporting combatant commands. Designate AFRICOM as supported and other combatant commands supporting due to the percentage of landmass and population effected.

R2. AFRICOM and CENTCOM: Convene an initial planning conference and recurring planning efforts between "Plans, Policy, and Strategy" directorates. EUCOM, U.S. Indo-Pacific Command, and relevant functional combatant commands should provide liaison officers for planning and awareness.

> **Any type of conflict in Ethiopia, Africa's second most populous country, would be highly destabilizing for the continent as a whole.**

Ethiopia, AFRICOM and Restless Neighbors

A growing Ethiopia requires the same basic resources every modernizing state requires: reliable electricity, food security, and peace. To address its electrical generation capacity and bolster its agricultural sector, in 2011 Ethiopia commenced construction of the GERD. While Ethiopia ranks poorly economically, Ethiopian sources and the United Nations state that domestic taxes and individual pledges are providing the needed $4.8 billion in financing for the project.[3] While a positive asset for Ethiopia, the GERD has the potential to destabilize the region by disrupting water access to Sudan's and Egypt's combined population of 140 million people.

AFRICOM wants a stable and prosperous Ethiopia. Ethiopia's large population (105 million) and proximity to bases in Djibouti make Ethiopia's stability a priority for AFRICOM. Any type of conflict in Ethiopia, Africa's second most populous country, would be highly destabilizing for the continent as a whole. While Africa is no stranger to violent conflict (e.g., Somalia, Rwanda, Congo, Sierra Leone), Ethiopia borders Djibouti. Djibouti, which is barely larger than the greater Tampa, Florida area, provides the western land border of the Bab-el-Mandeb Strait. Also, this small country provides military basing for the U.S., United Kingdom, France, China, Japan, and Saudi Arabia.[4] Any instability in Ethiopia could have negative spillover effects to Djibouti's significant and non-aligned military basing footprint.

Beyond the GERD related tension between Ethiopia and Egypt, numerous security issues challenge Africa analysts and policy developers. Massive immigration flow towards Europe, exploding populations, water scarcity, violent extremism, and piracy provide a glimpse of the security challenges for the African continent. In light of such a tenuous security environment, significant efforts must be made to ensure the stability of functioning states like Ethiopia in the Horn of Africa.

Recommendations

R3. Office of the Secretary of Defense: Coordinate with U.S. Department of State and U.S. Ambassador to the United Nations to introduce a resolution in support of diplomatic resolution to any disputes over the Nile River. Incorporate Ethiopian economic needs into requests to World Bank and International Monetary Fund to support a longer fill timeline for the GERD.

R4. Office of the Secretary of Defense: Coordinate with Chiefs of Defense with basing in Djibouti to discuss concern and contingency

plans in the event of crisis or conflict over the GERD. Designate specific communication pathways in the event of crisis.

Egypt, CENTCOM and the Forever Wars

Egypt's population of 100 million people endured great hardship over the past several decades. While negative conditions under President Mubarak helped spark the Arab Spring, subsequent political transitions caused even greater social turmoil, opened pathways for violent extremist organizations, and created economic hardships. Besides the recent political transients, Egypt's long-standing tensions and multiple wars with Israel also shape the current environment. While resilient, Egyptians need a period of stability and prosperity.

When Egypt gained independence from the British in 1922, the U.S. provided diplomatic recognition and support. Throughout the decades since, the U.S. supported Egypt even when it strained other alliances (e.g., 1956 Suez Crisis). Along with generations of diplomatic support, the U.S. continues to provide Egypt significant financial aid and places a high priority on U.S.-Egyptian security cooperation.[5] Today, CENTCOM needs Egypt as a stable security partner. Additionally, the global maritime shipping industry requires unfettered access to the Suez Canal.

While Egypt and its neighbor Israel have enjoyed decades of peace, the two countries' share a history of war. When not at war, the two countries remain deeply suspicious of each other. For example, while United Nations sources confirm Ethiopia's statements that financing has been internally sourced, social media sentiment analysis shows some Egyptians and even more non-identifiable Arabic speakers suspect that the Israelis are secretly funding the GERD in order to weaken Egypt. In addition to the Egyptian-Israeli conflict, Israel and the broader Arab world have been somewhere between tension and crisis over the Israel-Palestine issue since the

1917 Balfour Declaration. While Egypt's earnest diplomatic engagement in the Middle East Peace Process provides a source of optimism for peace, a century of conflict provides multiple obstacles for optimism. Additionally, the U.S. should monitor Egyptian social media sentiment on the GERD. As seen during the Arab Spring, Egyptian unrest on social media can rapidly transform into tangible political unrest and even violence.

Recommendations

R5. AFRICOM and CENTCOM: Coordinate with Egypt in crisis management planning. Consider creating a releasable compartment for classified information sharing with the Egyptians. (Link with R2 and R4)

R6. Department of State: Incorporate Egyptian concerns in United Nations resolution. (Link with R3)

> **…the U.S. should monitor Egyptian social media sentiment on the GERD.**

Israel and EUCOM

Israel and the U.S. share numerous bi-lateral agreements and national interests. While the U.S. has long supported Israel, the Trump administration's political decisions to move the U.S. Embassy to Jerusalem (2017) and recognize the Israeli annexation of the Golan Heights (2019) show an increasingly close partnership between the two countries. While Israel falls within the EUCOM area of responsibility, Egypt and the surrounding Levantine countries fall into the CENTCOM area of responsibility.

While Israel is not directly impacted by the health of the Nile, it has tangential security interests to the GERD. Even if Israel is innocent of providing shadow funding for the GERD, Egypt's suspicion over the GERD as an Israeli attempt to weaken Egypt reduces Israel's chances

for peace. Israel needs a cooperative Egypt as a neighbor as well as an Arab advocate within the Middle East Peace Process. Israel has extensive technical resources and capabilities that could aid Egypt, Sudan, and Ethiopia. Extending technical assistance in exchange for publicized diplomatic recognition could benefit all parties.

Recommendation

R7. Department of State: Coordinate with Israeli counterparts to support the technical challenges of filling the GERD without negatively impacting Egypt.

> ...a destabilizing event in North Africa or Horn of Africa over the GERD could generate an order of magnitude more refugees and extremist fighters than Syria.

Integrate Efforts amidst Existing Regional Security Challenges

Middle East Peace Process

While recent decades witnessed multiple U.S.-led attempts to broker peace between the Israelis and Palestinians, the Trump administration will soon release the "deal of the century." While the contents of the deal have been closely guarded, the Arab nations have clearly stated that any deal that does not include a two-state solution with East Jerusalem as the capital of Palestine will be unacceptable. Further, even proposing a deal that does not include these terms may result in a spike in violence among the region.

Recommendation

R8. Department of State: Conduct strategic communication across the U.S.-led diplomatic and security enterprise that the Middle East Peace Process has three primary tiers of

stakeholders: (a) Israel and Palestinians, (b) regional Muslim countries, and (c) the broader community of Muslim nations.

Russia, Turkey, Iran and the Syrian Civil War

The civil war in Syria casts a long shadow. During the war the embattled regime of Bashar al-Assad received an infusion of life support from Russia, which enabled the regime to survive the conflict. However, the war destroyed the Syrian infrastructure, devastated the economy and displaced over 10 million Syrians from their homes. Due to the shared border between Syria and Turkey and the large number of refugees, Turkey's increasing diplomatic and military involvement in post-conflict Syria further complicates the chessboard.

In addition to the civil war, Syrian territory also hosted the battle against the Islamic State in Iraq and Syria (ISIS). For multiple reasons, Iranian forces were among those attempting to destroy ISIS. Even though the battle of Baghouz marked the defeat of ISIS's physical caliphate, Iranian military forces remain in Syria. Due to the long-standing enmity between Iran and Israel, Israel interpreted the lingering presence as hostile intent, and has conducted numerous aerial strikes against Iranian forces in Syria.

The fall of Baghouz appears to be the origin of a diaspora of ISIS fighters, and many are fleeing to Africa. The pre-conflict Syrian population of approximately 15.5 million generated an incredible number of refugees that promptly drained the resources and political good will of neighboring countries and foreign aid donors.

The combined population of Egypt, Sudan and Ethiopia is greater than 240 million. If given time and space to sew their ideology in the midst of a conflict, then a destabilizing event in North Africa or Horn of Africa over the GERD could generate an order of magnitude more refugees and extremist fighters than Syria.

Recommendations

R9. Department of State: Ensure United Nations resolution martials technical and financial resources to provide targeted support for northern Africa and Horn of Africa. Ensure resources sufficiently alleviate potential for human suffering, create conditions for economic growth and eliminate space for ISIS affiliates to proliferate. Assign specific measures of performance for continued aid. (Link with R3)

R10. Department of State: Create opportunity within the United Nations resolution for great power coordination between the U.S., European Union and China.[6] (Link with R3)

Harmonize Support with the U.S.'s Strategy towards the Great Power Competition

Suez Canal: The Maritime Bridge between Europe and Asia

The Suez Canal provides a critical transport link between the Mediterranean Sea and Indian Ocean. Any instability surrounding the Suez Canal could trigger a dramatic increase in insurance premiums for maritime shipping, which would immediately translate to higher prices globally on consumer goods and energy. Additionally, the Suez Canal shortens the transit between the Atlantic and Indian oceans by thousands of miles.

If maritime shippers were required to transit the southern route around the Cape of Good Hope, the additional weeks in transit would trigger a global shortage of available shipping. The combination of increased insurance premiums and global shortage of shipping would have dramatic cascading impacts on any goods transported on the sea. As such, the national security interests of the European Union countries need a reliable operator of the Suez Canal—a stable Egypt.

Recommendations

R11. Department of State: Coordinate with the European Union countries who are the biggest beneficiaries of the Suez Canal in order to ensure continued flow.

R12. Joint Staff: Continue to plan security exercises like Bright Star 18—a multilateral CENTCOM field exercise and senior leader seminar held with Egypt and other partner nations—to ensure interoperability with regional partners.

> **…the national security interests of the European Union countries need a reliable operator of the Suez Canal — a stable Egypt.**

U.S. National Security Strategy

The 2017 National Security Strategy highlighted the return of Great Power Competition.[7] Russian, Chinese, and U.S. activity in the Levant and northern Africa provide a perfect example of this competition. In the competition for markets, influence, and security, Egypt's Suez Canal and Ethiopia's prominent position in the Horn of Africa will play significant roles in the strategies of the great powers.[8] The U.S. will seek to maintain its network of partners and allies in order to maintain security and stability in the region.

Successful U.S.-led management of the GERD issue could provide a winning platform in the much-discussed Great Power Competition. To achieve success, the U.S. can coordinate the resources of federal agencies as well as non-governmental organizations to support the GERD. For example, the U.S. can send specialists from agencies such as the Department of Energy, Army Corps of Engineers, National Weather Service, and other agencies to advise on the construction of the GERD and subsequent

safe impoundment of the Blue Nile River. Additionally, the same resources could provide technical assistance with the Egyptian Aswan High Dam, which has been challenged by an excessive silt deposit rate. Finally, the United Nations resolutions could provide a much-needed framework and future precedence for international engagement in conflicts over fresh water resources.

Recommendations

R13. Department of State: Coordinate via appropriate channels with major shipping insurance providers to understand market perceptions and values of risk. Communicate risks in order of priority.

R14. AFRICOM and CENTCOM: Develop prioritized risk mitigation plan to ensure market stability to greatest extent practicable. (Link to R13)

China's Belt and Road Initiative

China's interests are antithetical to violent extremism, and China's Belt and Road Initiative has already made massive financial investments in Egypt and Horn of Africa. However, China usually cites its "developing nation" status when countries call on it to bare any international burdens for the sake of the world order. However, the Suez Canal plays an essential role in the Belt and Road Initiative since it provides maritime access to European markets.[9] The canal unifies the land and maritime links of the Eurasian land mass and Africa. Given China's investments to date and the vulnerability of these investments if violent extremist organizations proliferate, the U.S. should press China to funnel more technical and financial resources to the region to ensure the GERD does not challenge regional stability.

Recommendation

R15. Joint Staff: Coordinate with the Chinese Chiefs of Defense to ensure de-confliction between U.S. and Chinese security planning in order to (a) support regional stability, and (b) avoid a Sino-U.S. miscalculation in Djibouti in the event of instability in the Horn of Africa. (Link to R4, R10-12, R14)

Conclusion

The U.S. must establish a proactive posture to assist Egypt, Sudan and Ethiopia since a destabilized Nile would have rippling consequences throughout Africa, Europe, and Asia. The proactive posture must focus on coordinated diplomatic engagement of all countries with equities in the GERD, coordinated military engagement by U.S. geographic combatant commands s and targeted economic assistance. Importantly, the U.S. must ensure its aiding institutions approach the challenge with a unified solution since the goals of sister agencies may conflict in the GERD debate. Above all, any U.S. assistance must leverage its existing network of allies and regional partners, not conflict with existing or create new kinetic conflicts and harmonize with the U.S.'s strategy towards the Great Power Competition. *IAJ*

Recommendations (Recap)

R1. Office of the Secretary of Defense: Coordinate with the Joint Staff to designate supported and supporting combatant commands. Designate AFRICOM as supported and other combatant commands supporting due to the percentage of landmass and population effected.

R2. AFRICOM and CENTCOM: Convene an initial planning conference and recurring planning efforts between "Plans, Policy, and Strategy" directorates. EUCOM, U.S. Indo-Pacific Command, and relevant functional combatant commands should provide liaison officers for planning and awareness.

R3. Office of the Secretary of Defense: Coordinate with U.S. Department of State and U.S. Ambassador to the United Nations to introduce a resolution in support of diplomatic resolution to any disputes over the Nile River. Incorporate Ethiopian economic needs into requests to World Bank and International Monetary Fund to support a longer fill timeline for the GERD.

R4. Office of the Secretary of Defense: Coordinate with Chiefs of Defense with basing in Djibouti to discuss concern and contingency plans in the event of crisis or conflict over the GERD. Designate specific communication pathways in the event of crisis.

R5. AFRICOM and CENTCOM: Coordinate with Egypt in crisis management planning. Consider creating a releasable compartment for classified information sharing with the Egyptians. (Link with R2 and R4)

R6. Department of State: Incorporate Egyptian concerns in United Nations resolution. (Link with R3)

R7. Department of State: Coordinate with Israeli counterparts to support the technical challenges of filling the GERD without negatively impacting Egypt.

R8. Department of State: Conduct strategic communication across the U.S.-led diplomatic and security enterprise that the Middle East Peace Process has three primary tiers of stakeholders: (a) Israel and Palestinians, (b) regional Muslim countries, and (c) the broader community of Muslim nations.

R9. Department of State: Ensure United Nations resolution martials technical and financial resources to provide targeted support for northern Africa and Horn of Africa. Ensure resources sufficiently alleviate potential for human suffering, create conditions for economic growth and eliminate space for ISIS affiliates to proliferate. Assign specific measures of performance for continued aid. (Link with R3)

R10. Department of State: Create opportunity within the United Nations resolution for great power coordination between the U.S., European Union and China.6 (Link with R3)

R11. Department of State: Coordinate with the European Union countries who are the biggest beneficiaries of the Suez Canal in order to ensure continued flow.

R12. Joint Staff: Continue to plan security exercises like Bright Star 18—a multilateral CENTCOM field exercise and senior leader seminar held with Egypt and other partner nations—to ensure interoperability with regional partners.

R13. Department of State: Coordinate via appropriate channels with major shipping insurance providers to understand market perceptions and values of risk. Communicate risks in order of priority.

R14. AFRICOM and CENTCOM: Develop prioritized risk mitigation plan to ensure market stability to greatest extent practicable. (Link to R13)

R15. Joint Staff: Coordinate with the Chinese Chiefs of Defense to ensure de-confliction between U.S. and Chinese security planning in order to (a) support regional stability, and (b) avoid a Sino-U.S. miscalculation in Djibouti in the event of instability in the Horn of Africa. (Link to R4, R10-12, R14)

NOTES

1   B. Keith, D.N. Ford, and R. Horton, 2017: "Considerations in Managing the Fill Rate of the Grand Ethiopian Renaissance Dam Reservoir Using a System Dynamics Approach", *J. Def. Model. Simul.*, 14, no. 1, 33-43, https://pubs.giss.nasa.gov/abs/ke00200u.html.

2   Steven Cook, "Is War about to Break Out in the Horn of Africa? Will the West Even Notice?" Council on Foreign Relations, January 16, 2018, https://www.cfr.org/blog/war-about-break-out-horn-africa-will-west-even-notice.

3   Kingsley Ighobor and Busani Bafana, "Financing Africa's Massive Projects," Africa Renewal Magazine, December 2014, https://www.un.org/africarenewal/magazine/december-2014/financing-africa%E2%80%99s-massive-projects.

4   Zineb Boujrada, "This Tiny Country Has the Most Foreign Military Bases," Culture Trip, March 16, 2018, https://theculturetrip.com/africa/djibouti/articles/why-does-djibouti-have-the-most-foreign-military-bases.

5   Bureau of Near Eastern Affairs, "US Relations with Egypt: Fact Sheet," July 18, 2018, https://www.state.gov/r/pa/ei/bgn/5309.htm.

6   Benjamin Miller "Explaining Great Power Cooperation in Conflict Management" *World Politics*, Vol. 45, No 1 (Oct 1992), pp 1-46 Cambridge University Press

7   The White House, "National Security Strategy of the United States of America," December 2017, 25.

8   James Jacobs and Kevin Boldt "Assessing the Impact of American and Chinese Economic Competition in Sub-Saharan Africa"

9   Shannon Tiezzi, "Xi's Visit Cements Egypt's Place on the Belt and Road," The Diplomat, January 22, 2016, https://thediplomat.com/2016/01/xis-visit-cements-egypts-place-on-the-belt-and-road.

Empowering U.S. National Security with

Artificial Intelligence Capabilities

by Shannon L. Gorman

If we fail to adapt... at the speed of relevance, then our military forces... will lose the very technical and tactical advantages we've enjoyed since World War II.

— Secretary of Defense James N. Mattis
National Defense Magazine
"Mattis: More Engagement Needed with Industry, Allies"
by Vivienne Machi

The National Geospatial-Intelligence Agency (NGA) is the principal Department of Defense (DoD) intelligence agency that possesses and processes "Geospatial" information. The agency is aggressively pursuing innovative solutions regarding artificial intelligence (AI)-based enhanced capabilities, automation, and human-machine teaming augmentation. The NGA will use these advancements to "automate routine [geospatial intelligence] tasks and corporate business processes and invest in technology-transfer opportunities from commercial or nontraditional sources as appropriate."[1]

The NGA has the proper organizational cultural vision, goals, and mindset, to pursue creative public-private sector partnerships in innovation while adapting to change in an ever increasingly abstruse and technological world. The DoD sister-service components can emulate NGA's model and further their advanced-based initiatives by contributing data and using the agency's epistemological organization to remain viable. In a time, where there is significant peer rivalry across the competitive continuum of technological advancement from China and Russia that is challenging the United States National Security interests, there needs an adequate model and framework for governmental entities to use AI-based technological advancements to empower senior policy-makers and the warfighter in sound timely decision-making.

Major Shannon L. Gorman is a graduate of the U.S. Army Command and General Staff College.

NGA Using Advanced Methods to Meet National Security Interest in 2030

According to the *National Security Strategy* 2017 and the *National Defense Strategy 2018*, the national security interests, competitive advantage, and prosperity are to ensure the nation's power projection continues to propagate in the decades to come in an oppositional, competitive volatile operational environment from peer and near-peer adversaries. *National Defense Strategy* highlights are:

- Defend the homeland from attack;

- Sustain Joint Force military advantages, both globally and in key regions;

- Deter adversaries from aggression against our vital interests;

- Enable U.S. interagency counterparts to advance U.S. influence and interests;

- Maintain favorable regional balances of power in the Indo-Pacific, Europe, the Middle East, and the Western Hemisphere;

- Defend allies from military aggression and bolstering partners against coercion, and equitably sharing responsibilities for the common defense;

- Dissuade, prevent, or deter state adversaries and non-state actors from acquiring, proliferating, or using weapons of mass destruction;

- Prevent terrorists from directing or supporting external operations against the United States homeland and our citizens, allies, and partners overseas;

- Ensure common domains remain open and free;

- Continuously deliver performance with affordability and speed as we change Departmental mindset, culture, and management systems; and

- Establish an unmatched twenty-first century National Security Innovation Base that effectively supports Department operations and sustains security and solvency.[2]

Revolutions in military affairs is described as "the assembly of a complex mix of tactical, organizational, doctrinal, and technological innovations in order to implement a new conceptual approach to warfare or to a specialized sub-branch of warfare."[3] The proper integration and synchronizing of advanced technology can promote the achievement of national interests of the United States, whether the world is currently in Revolutions in military affairs in the twenty-first-century warfare.

In order to achieve the strategic, operational, and tactical objectives based on national interests, the intelligence community needs to work more coherently and intelligently with our allied and multinational partners to achieve and maintain superiority in a multi-domain environment, such as the electrometric spectrum, information, air, land, sea, space, and cyberspace domains. Further, we need to look at the unclear concurrent battlefield from a multi-dimensional perspective. To achieve the nation's interests, we need to employ all capabilities available to project our influence and national power on our adversaries in the next decade.

The National Geospatial-Intelligence Agency is one of seventeen intelligence components across the intelligence community. The NGA "delivers world-class geospatial intelligence (GEOINT) that provides a decisive advantage to policy-makers, warfighters, intelligence professionals, and first responders. NGA is the lead federal agency for GEOINT and manages a global consortium of more than 400 commercial and government relationships."[4]

The NGA's expertise of geospatial

intelligence known as "GEOINT is the exploitation and analysis of imagery and geospatial information to describe, assess and visually depict physical features and geographically referenced activities on the Earth. GEOINT consists of imagery, imagery intelligence and geospatial information."[5]

The NGA's Strategy 2025 describes the agency's overall mission is to "provide GEOINT for our nation's security." The agency is able to complete its mission and remain viable by being committed to areas of data integration and relentless innovation.[6]

Assisting its customers across the full spectrum in the range of military operations, as well as providing senior policy-makers with pertinent information, GEOINT brings significant attributions in time and space. NGA employs the full force of GEOINT capabilities through working with government and allied partners, industry, and academia. The nation can achieve its objectives by establishing opportunities across the strategic, operational, and tactical application levels that provide actionable intelligence to leadership, which allow them to make informed, sound decisions at every level of the decision-making spectrum and increasingly rapid response.

Due to emerging technologies and threats by our various adversaries, the nation must adapt and adjust accordingly. Adversaries at all levels have developed sophistication in various realms, such as, in the electromagnetic spectrum and cyberspace realm, firepower and range capacities, accuracy and precision progress, and informational warfare headways, to name a few. To respond accordingly, the national interests must adapt and adjust by providing information to our customers in a more timely fashion. So how does the nation move from the current operating demands to future operating demands to deter or defeat the enemy? The focus should be on the element of time. Time is the element in which we can best defeat our enemy in the

various competitive domains during any future engagements. That is, providing customers with sound data and information, to be used at the appropriate level to allow customers to execute their mission requirements successfully.

National Technical Means and commercial platforms provide data and information to customers at the senior military and policy-makers level to assist in formulating a national strategy. Likewise, various information is provided to the elements at the tactical level which support their level of operations. The NGA will need to provide the customer, who works in a time-constrained, ambiguous and chaotic environment, with timely data and information. Further, in order for the customer to maintain a position of relative and decisive advantage, both

> **NGA employs the full force of GEOINT capabilities through working with government and allied partners, industry, and academia.**

senior leaders and the warfighter must maneuver significantly quicker (speed of decision-making, the speed of action, operational tempo and momentum, the agility of action, quality and competency of an interdependent joint force) than the adversary. How will the nation accomplish this? This task can be accomplished by the proper incorporation of robust automation and AI-enabled capability integrated into the daily practices of the GEOINT processes.

The DoD has established the Joint Artificial Intelligence Center. The purpose being the "overarching goal of accelerating the delivery of AI-enabled capabilities, scaling the Department-wide impact of AI, and synchronizing DoD AI activities to expand Joint Force advantages."[7] Overall, the purpose of this agency inaugurates new collaboration across the Joint DoD Community and ensures proper "execution in

AI that includes the tools, shared data, reusable technologies, processes, and expertise to enable rapid delivery and Department-wide scaling of AI-enabled capabilities."[8]

To meet DoD advanced-enabled capability needs, NGA's commercial components established a focus on "emphasizing innovation in the face of a rapidly advancing technological landscape. The strategy focuses on partnerships, information assurance and the integration of commercial GEOINT with automation and artificial intelligence."[9] The key to the strategy is the assimilation of partnerships interrelated in governmental and non-governmental areas, as well as, ensuring the quality and accuracy of information provided by the entities. The established of these areas will safeguard the guarantee that "strategy meets the advancing operating environment and reflects the priority of sustaining American leadership through research, technology, and innovation outlined in the National Security Strategy."[10]

> ...it is imperative NGA's calculus ensures the future of incorporating the vitality of AI-enhanced initiatives...

Consequently, it is imperative NGA's calculus ensures the future of incorporating the vitality of AI-enhanced initiatives that will improve customer success, in addition to maintaining the customer's strategic and tactical competitive advantage in a multi-domain fluid environment. However, the amount of data that will be available for the NGA team to analyze will be insurmountable. According to the previous director of the NGA, "6 million imagery analysts [are needed] to keep up with that kind of [data] flow" from both classified government satellites and unclassified commercial satellite systems.[11]

It is imperative to appreciate the problematic context and related issues concerning big data.

"Today's worldwide geospatial data production is measured in exabytes—a single exabyte equals one million terabytes. For context, digitizing every book within the Library of Congress would produce about 10 terabytes. The sheer volume of geospatial data—much of it relevant to NGA's national security mission—highlights how large a big data problem it poses."[12] The amount of GEOINT data an intelligence agency would work with would be voluminous. To deal with this problem-set, NGA has initiatives that establish offices and hire the best and brightest talent in the Silicon Valley area to assist the agency with the issue.[13]

There is still the element of deception that the NGA will need to prepare for by letting the AI systems conduct analytics of imagery for the agency. Case in point, according to Valerie Browning, Director of the Defense Sciences Office at the Defense Advanced Research Projects Agency (DARPA), "It's important that we understand the limitations of where AI is today," she said on a panel discussing the relationship between technology and human analysis. "There are numerous examples of where the current state of the technology can be very easily fooled and unfortunately, we don't really quite understand the mechanisms. We have some hints."[14]

This article will focus on United States DoD initiatives, with an in-depth focus on the NGA's AI-enhanced capabilities and initiatives, as well as, the *NGA Strategy 2025*. Additionally, the article will compare and analyze China's aggressive approach to be the world leader in AI by 2030, investigate leaders in the AI industry (such as Google's DeepMind AI Alpha variants initiative), and look at the implications of using AI enhancements and the ethical considerations involved. The primary purpose of this examination is to explore the research question: should the various governmental agencies and DoD sister-service components, which lag in AI innovation and adaptation, profitably use the

NGA's AI-initiatives as a lead model, partner with NGA in AI development, and contribute their data to unified AI efforts using the Agency's epistemological and organizational advantages to assist them to remain apace?

Artificial Intelligence-based Capabilities

There are many differentiating opinions of what is AI. Corporations are pushing smart-enabled devices such as Apple HomePod, Apple Siri, Google Home, Amazon Alexa, and the Amazon Echo as AI-advanced devices. However, for the context of this article, the author will use the Intelligence Community's definition of AI.

According to the Office of the Director of National Intelligence's Augmenting Intelligence Using Machines Initiative, which is the Intelligence Community's strategic focus for the augmentation of intelligence using machines. The community's definition of AI is:

"the branch of computer science focused on programming machines to perform tasks that replicate or augment aspects of human cognition," a term coined in the 1950s. At that time, scientists began to harness nascent computer capabilities to perform advanced information manipulations much more rapidly. In particular, it was realized that computers could be used not only to perform calculations on numbers, but also to perform inference on other types of information such as symbols, data, and text. This popularized the idea of a "thinking machine" that could, if filled with all the right knowledge and rules for access and retrieval, simulate a human response.[15]

The examination of the author's research pertains predominantly on AI-based capabilities, machine learning, and human-machine augmentation teaming. The Office of the Director of National Intelligence and the Intelligence Community include "Technologies and research areas generally considered to be sub-domains to AI," such as automated planning and scheduling, computer vision, decision support, predictive analytics and analytic discovery, distributed AI/agent-based systems, human language technologies, identity intelligence, machine learning, process modeling, as well as robotics/autonomous systems.[16] The future success of ensuring the U.S. maintains its overmatch in the competitive and conflict continuums, as well to promote the National Security Strategy interests, is to adequately and succinctly incorporate these advanced-based technologies appropriately across the governmental spectrum.

> **There are many differentiating opinions of what is AI.**

The National Geospatial-Intelligence Agency to Harness Data-Centric Technology

Various components of the private sector and government agencies at all levels are enthusiastic about the prospects of using AI-based enhancements, as well as other closely related technological advancements. Advances of these technologies in the private sector are proliferating, and will eventually affect society, military, and the government at various levels. Major Christopher Telley's item in the Land Warfare Paper, titled "The Influence Machine: Automated Information Operations as a Strategic Defeat Mechanism," highlights an established AI expert, Andrew Ng, who explains "[j]ust as electricity transformed almost everything 100 years ago, today I actually have a hard time thinking of an industry that I don't think AI will transform in the next several years."[17] Leaders within the intelligence community are implementing many bold initiatives about their agency.

The National Geospatial-Intelligence Agency Director Richard Cardillo would like to use machine learning to more effectively and

efficiently analyze the vast increase amount of imagery data to enable the NGA analysts to accomplish more pertinent advanced geospatial-intelligence analytics. That is "Instead of analysts staring at millions of images of coastlines and beachfronts, computers could digitally pore over images, calculating baselines for elevation and other features of the landscape." The NGA's automation and AI-enhanced initiatives have greater determination and expectations for the agency to achieve "NGA's goal, which is to establish a 'pattern of life' for the surfaces of the Earth and be able to detect when patterns change, rather than looking for specific people or objects."[18]

The NGA leadership has the mindset that

> ...[the NGA] is establishing public-private sector relationships with companies... which are focusing on...AI-enhancements and automation.

the use and integration of human and machine interaction will propel innovation. The agency is establishing public-private sector relationships with companies, including Concurrent Technologies Corporation, HRL Laboratories, Raytheon, and Soar Technology, Inc., which are focusing on the initiative of AI-enhancements and automation.[19] A senior analyst at the agency indicated, "This research provides NGA with great opportunities to explore how humans and machines can team together to sift, sort, and process in a data rich environment."[20]

Each of the aforementioned four public-private partnered companies will specialize in a specific area regarding automation and AI. The various areas of research are:

1. Advance an interdependent human-machine network concept designed to enable task automation and management;

2. Will identify correlations between analysts' interactions and automatically share relevant data across like-user groups;

3. Autonomously provide workflow recommendations and suggested courses of action to help analysts become aware of unconscious bias when making key judgments; and finally,

4. Provide automated mining of streamed data to alert analysts to anomalous activity that could be of interest.[21]

These initiatives are part of a broader three-year enterprise established in 2016 by NGA. The boarder initiative by NGA established a working relationship, with both academia and the private sector, to provide feedback by gauging the impact of the value of its products and services to NGA's various customers. NGA's campaign is named the Boosting Innovative GEOINT Broad Agency Announcement. The three main areas of the Boosting Innovative GEOINT Broad Agency Announcement deal with optimizing "value" for the customer, AI-enhancements, and automation, and lastly "Area 3 is classified and titled 'Synthetic Aperture Radar Image Formation.'"[22]

The NGA has a public-private partnership contract with Commonwealth Computer Research, Inc., which used "machine learning and neural networks to identify GEOINT user communities and characteristics of GEOINT data that contribute most to the success of each user community."[23] The objective is to determine what is of importance and value to those that use the NGA's services and assist customer's knowledge gaps to "steer users to specific GEOINT data that has the highest likelihood of providing value to the user."[24]

The NGA is seeking additional and more robust collaboration in the arenas of data to further its successes with the aforementioned initiatives.[25] Essentially, many agencies and private sector companies understand that

future success will come down to a proper understanding of the volume and propagation of data. The data will need to be characterized in a coherent and structured framework in which the analytical system, whether autonomous or AI-enhanced, can process, comprehend, and exploit for accurate and precise useable analysis. The NGA additionally solicits ideas from areas of academia and the private sector for its Boosting Innovative GEOINT Broad Agency Announcement Topic Area 10, Amendment 10, regarding Structured Observation Management Automation, which is a focus area of data structure.[26]

The superior flexibility and enhanced innovations of the free market enterprise and academia, allows NGA to use their creative capacities to ensure foundation GEOINT data is adequately characterized and structured in an understandable format. In September 2018, NGA awarded seven new contracts regarding foundation GEOINT data and advanced geospatial analytics.[27]

The NGA is focusing on enhancing and bolstering the agency's data, information, analytics, products, and its services by establishing various areas of research on the "Characterization of Geospatial Data," by using contracted academia and private sector machine learning, deep learning capabilities, structured spatiotemporal inference, and automation incorporation. A portion of seven contracts components deal with the following areas to improve foundation GEOINT data:

1. "panchromatic electro-optical imagery for land use characterization and agricultural crop assessment" to bolster NGA's crop analytics;

2. Processing of spectral datasets into an understandable categorized structure and into a big-data database by using machine learning;

3. Site activity monitoring large temporal spans and methods that identify temporal variations, trends and spatial correlation; and finally,

4. Provide automated geospatial product generation including, "images and point clouds collected using any sensor," and the "discovery and classification of foundation data," thereby improvements of geolocation accuracy, as well as validation of terrain surface models.[28]

> **In September 2018, NGA awarded seven new contracts regarding foundation GEOINT data and advanced geospatial analytics.**

These advanced initiatives are using cooperation and collaboration between NGA, the private sector and, academia, in hopes that the initiative will bolster the NGA's foundation GEOINT data in a more accurate and timely manner; as well as, "measuring the value of GEOINT content delivered to diverse customers in a cloud environment."[29]

Case in point, an October 2018 NGA press release announced the "Release 7" of the ArtcicDEM Project, a collaborative effort of NGA, the private sector, and academia to develop 3-D digital elevation models of the Arctic with a resolution of 2-meters. The 2-meter resolution is five times the original release.[30] This is a powerful example of the productivity and capability of incorporating three enterprises of public-private-academic sector partnerships.

The NGA continuously announces various welcoming White Papers for its Boosting Innovative GEOINT efforts.[31] The agency is seeking ideas for Boosting Innovative GEOINT Broad Agency Announcement Topic Area 1 pertaining to "value." NGA continues to seek

the positive impact regarding how working and partnering with the private sector and academia can propel the agency's utility. Not only in production but actual worth of value to the agency's various customers. Further, the agency is promoting and encouraging "White Papers from collaborations of entities (industry and industry, industry and university, university and university, etc.) because research in multidisciplinary Topic Areas may require forming teams with strengths in multiple science and engineering fields."[32]

> **The NGA leadership's ultimate goal and vision is to simplify the time that it takes the NGA analysts to do repetitive responsibilities.**

The NGA's robust initiatives are providing opportunities and challenges for the agency with regards to what analysts are asked to do and the ever-increasing amounts of data impacting NGA. Former NGA Director Cardillo's perspective, AI and automation will only empower the analyst and not replace them, which various analysts had raised concerns about.[33] However, these new methodologies will allow the NGA's analysts to do even more advanced analytical work. Cardillo explained, "automation 'isn't to get rid of you—it's there to elevate you.... It's about giving you a higher-level role to do the harder things.'"[34] The NGA leadership's ultimate goal and vision is to simplify the time that it takes the NGA analysts to do repetitive responsibilities. Thus, the push is to enhance practitioners to be unencumbered to complete advanced projects, as well as analytics such as pattern of life and activity-based intelligence examination, which require much more multifariousness.

Activity-based Intelligence is an intelligence discipline that emerged during the Iraq and Afghanistan campaigns against insurgents and terrorist. Unlike the military footprint signatures, insurgents and terrorists have a different smaller signature. Their signatures would include computer and cell phone footprint data. Further, activity-based intelligence expert Gregory F. Treverton explains, "[activity-based intelligence] disrupts that linear collection, exploitation, dissemination cycle of intelligence. It is focused on combining data—any data—where it is found."[35] The important aspects of activity-based intelligence analysis will be the NGA using the components of automation, algorithms, and AI-advancements simultaneously that will use more significant quantities of data to assist in fostering faster, as well as more accurate and precise practitioner analytics.

Next, the vast amount of data will present NGA with great opportunities and challenges. Data will be produced from various platforms and algorithms, ranging from commercial smallsats to the utilization of machine learning. This will be accomplished by establishing a standard or baseline from which algorithms can automatically analyze the substantial increase of imagery instead of analysts continuing with mundane exploitation. Ultimately, the utilization of these advances of AI-enhanced capabilities will assist NGA's goals to "establish a 'pattern of life' for the surfaces of the Earth to be able to detect when [the] pattern changes, rather than looking for specific people or objects."[36]

Consequently, the empowerment of AI capabilities and technological advances will assist decision-makers across the strategic, operational, and tactical spectrum. Sound timely decisions can be fostered with more exactitude. By harnessing AI-advancements, machine learning, deep learning, automation, and human-machine collaboration, the "NGA will evolve GEOINT from providing authoritative observations of recent activities to delivering models and modeling capabilities that satisfy customer needs, such as strategic warning, mission forecasting, and humanitarian

preparations."[37] Further, these technological capabilities will assist the NGA practitioners to recognize, prepare, and organize for pattern shifts regarding human migration, humanitarian concerns, and environmental complications, catastrophic weather crises such as tornadoes, hurricanes, floods, mudslides, and wildfires.

Artificial Intelligence Global Initiatives

Looking at AI-enhancements from a macro global perspective, nations have understood the significance to pursue research and development in this arena of advancements. China has taken the lead and to date has dominated the race of AI advancements, with the United States a distant second place.[38] There are significant factors that explain why China is leading.

First, in 2017, China's President, Xi Jinping, conveyed the nation's strategic establishment of their desire to be the technological dominant rising power in the world, when China communicated its nations' New Generation AI Development Plan.[39] China's national strategic goals include a desire to be a global "science and technology superpower" by 2030. These areas include aerospace, fifth generation wireless technological advancements, offensive and defensive cyber technology, and quantum information sciences (e.g., quantum communications and quantum computing), emergent technologies such as nanotechnology and biotechnology, and leveraging AI, the internet, and big data. Jinping's regime's desire is to be the premier world leader in AI by 2030 by investing and supporting research and development of next-generation AI advanced technologies, such as "brain-inspired neural network architectures and quantum-accelerated machine learning." China further realizes "that innovation is a critical determinant of national power and competitiveness."[40]

Second, expansions in AI-based enhancements are happening at such a rapid rate, nations struggle with the "ability to structure governance and growth frameworks around" various industries.[41] The reason for success in peer-to-peer competition in AI dominance and growth has to do with factors such as innovation cycles and national level structural improvements, according to a Boston Consulting Group study titled "Mind the (AI) Gap: Leadership Makes the Difference." Chinese success is due to a shorter innovation cycle than their near-peers. Next, the Boston Consulting Group found that the national level involvement plays a significant role for growth in AI, by investing in "data infrastructure, in research hubs and networks, and higher education for IT and data-related fields."[42]

> **China has taken the lead and to date has dominated the race of AI advancements, with the United States a distant second place.**

So why is China dominating compared to its various near-peer competitor's regarding AI-enhanced competition? The Boston Consulting Group study highlights three areas for China's success in the AI race for success.

First, the study found that of seven countries, including 2700 managers, a very high percentage of the companies in China are active participates (AI piloting or AI adopting) in the field of AI, compared to the other six countries, surveyed in Boston Consulting Group's December 2018 study. China's overall participants totaled a significant 85 percent, whereas the U.S. totaled 51 percent, and France and Germany were next at 49 percent. The survey explains that China's domination in this area is due to the national strategic plan introduced in 2017, which empowered Chinese companies to "adopt AI into some existing processes" or assists companies to generate "pilot initiatives."[43]

The second significant takeaway of the Boston Consulting Group study is that China's 2017 New Generation Artificial Intelligence Development Plan empowered and impacted Chinese managers approach regarding AI-based innovation. Consequently, Chinese initiatives are across and dominate all industries, whereas, the United States and the other countries are strong in "one or two particular industries."[44]

> **It is increasingly clear that China and Russia want to shape a world consistent with their authoritarian model...**

Lastly, the Boston Consulting Group study indicates that there are four significant factors that empower AI success pertaining to adaption and piloting initiatives. Success in adaption and piloting initiatives are dependent on technical infrastructure, available skills, execution of speed and responsiveness, as well as support from upper management. According to this study, the U.S. has an edge regarding its start-up companies due to the "small engineering and R & D teams comprised of highly skilled and talented technical professionals and can move much faster than their larger competitors." Thus, the United States' success is in the start-up of companies that have "tax incentives in new technologies," investments in AI activity in the digital realm, which business participants are conveying a 90 percent success rate.[45]

National Security, Ethics, and Big Tech Ties to State-Controlled Authoritarian Regimes

It is apparent that the national strategic strategy regarding China's 2017 New Generation Artificial Intelligence Development Plan, has been considerably successful and it has taken the Western world by surprise. According to the *National Defense Strategy 2018*, "The central challenge to U.S. prosperity and security is the reemergence of long-term, strategic competition by what the National Security Strategy classifies as revisionist powers. It is increasingly clear that China and Russia want to shape a world consistent with their authoritarian model—gaining veto authority over other nations' economic, diplomatic, and security decisions."[46] Further, the *National Defense Strategy* goes on to convey that China uses "predatory economics to coerce" other countries nearby in the Indo-Pacific region and seeks "regional hegemony in the near-term and displacement of the United States to achieve global preeminence in the future."[47] However, China's strategic and military ambition is not limiting it to its Indo-Pacific region, but it is aggressively pursuing its AI initiatives in other global geographical areas as well.

Case in point, in March of 2018, the Chinese state-controlled artificial-intelligence company, CloudWalk Technology, entered into a deal with the Republic of Zimbabwe's government.[48] The Republic of Zimbabwe has approximately sixteen million people and has been an unstable nation. For example, the country's army led a *coup d'état* in November 2017.[49] A result of unstable nations permits China strategy to "take advantage of the weak legal systems and low privacy standards of developing nations." The benefit and advantage of these types of agreements between China and other countries, allows China's state-owned CloudWalk Company, to expand its facial data and thereby improving its AI algorithms; whereas, the Zimbabwean authoritarian regime, gains superfluous empowerment by "an advanced facial-recognition system that it can use to identify, track, and monitor citizens." An ethical consideration here, is it moral to monitor citizens via facial recognition; more importantly, is it ethical to surveil citizens and give them a social score based on behavioral patterns regarding citizens "social and economic performance[?]"[50]

The vision of China's plan for the Social Credit System to monitor its 1.3 billion citizens was announced in June of 2014, by the State Council of China.[51] Since then, China started implementing digital algorithm recordings, and this allowed the generation of a credit score for its citizens, which will determine entitlements or potential blacklists of services. Services included that may impact the Chinese citizenry are components such as insurance premiums, access to essential social services, banking loan rates and loan amounts, traveling abroad out of China, school admission and university scholarships, assess to boats, planes, and high-speed trains, access to social media and internet services, and eligibility for work, particularly governmental jobs.[52]

China's authoritarian President, Xi Jinping, further conveyed his push for "social governance" and his state-owned government's vision of the utilization that "Algorithms would use a range of data to calculate a citizen's rating, which would then be used to determine all manner of activities, such as who gets loans, or faster treatment at government offices or access to luxury hotels."[53]

The communist party is pushing their ethics, values, and morality by controlling their peoples' every move through establishing and enforcing the social-credit system, which is to "allow the trustworthy to roam everywhere under heaven while making it hard for the discredit to take a single step."[54] Establishing a defined algorithm that determines whether a citizen is compliant with "government-mandated social behaviors" and then can impose government "sanctions and penalties," hence is an ethical topic of coercion or conformity that needs to be addressed by humanitarian organizations, western countries, and like-minded liberal governments.[55]

It is of interest to the United States' National Security, as well as, our various allies' national interests, to pursue an aggressive counter AI-enhanced strategies posture and incorporate methodologies of competitiveness contrary to China's social governance of control. Those who believe in liberty, freedom, and the democratic or republican form of governance must be vigilant and act against repressive authoritarian regimes. For if the United States and the West delay "dire consequences will follow for global democracy."[56] A former Ronald Regan Administration Assistant, Under Secretary of Defense for Policy Planning, Mr. Michael Phillsbury, conveys that much of the Chinese philosophy and strategy to replace America's superpower status is built upon the ideology that "Chinese states prized deception above all as they jockeyed for supremacy."[57] Additionally, Phillsbury explained that a former Chinese Dictator and Moe's successor, Mae Zedong, conveyed "hide your brilliance and bide your time."[58] The United States and the Western allies need to be vigilant against these tactics in the era of technological evolution and AI-advancements.

> **It is of interest to the United States' National Security...to pursue an aggressive counter AI-enhanced strategies posture...**

In order for a nation to be successful, it needs to work and collaborate with those of AI enhanced technical means and understanding. The United States Department of Defense has the Algorithmic Warfare Cross-Functional Team, to work on a project named Project Maven.[59] The goal of the DoD initiative is to incorporate big data, AI, and machine learning and to service the "Project Maven to Deploy Computer Algorithms to War Zone by Year's End." The Pentagon's project would assist the United States' allies to maintain its competitive advantage over the "capable adversaries and competitors" by accomplishing more precise actions in a more timely manner, which should assist in limiting collateral damage.[60]

According to the DoD News, Defense Media Activity, in July 2017, Project Maven uses computer vision, which is "an aspect of machine learning and deep learning—that autonomously extracts objects of interest from moving or still imagery."[61] Further, the addition of "Biologically inspired neural networks" will assist in the project's goal to free up time and allow analysts to complete additional tasks for effective efficiency. Additionally, the Maven Project integrates analysts, software engineers, algorithm developers, and a data-labeling company to properly label data, and "prepare it for machine learning." Lastly, the design and development of an AI and human operators interface will be established on government platforms, and thereby the AI will "compliment the human operator" during its deployment to the war zone.[62]

> **...big tech organizations have significant influence and promote the technological direction regarding AI-advanced capabilities.**

However, in June of 2018, there was a Pentagon setback when Google had announced it would not renew a contract regarding the Maven Project.[63] Google had approximately 4,000 employees sign a petition or "resign in protest" due to the Pentagon Google Cloud business contract.[64] The employees' concerns were in regards to the use of AI technology by "Google's work" as well as the use of AI "software to improve the sorting and analysis of imagery from drones, and some drones rely on such analysis to identify human targets for lethal missile shots."[65] The employees and AI researchers were protesting and concerned that the "contract was the first step toward using the nascent technology in advanced weapons."[66] Subsequently, Google conveyed that its newly established AI principles preclude "the use of

A.I. in weaponry."[67] Thus, the organization made a cognizant withdrawal from assisting the United States from pursuing its competitive advance in the realm of AI advancements, which impacts the U.S. national security interests.[68]

Google's AI principles and ethical considerations were the final determining factors for its withdrawal the Pentagon's AI Maven initiative; however, the company has determined it's fine to work conscientiously with Beijing's research center.[69] Google's principles do not restrict it from working with the Chinese government, which actually "convert consumer technologies to military applications" and incidentally help to potentially thrust Chinese dominance in a variety of technological progressions, including global AI-advancements.[70]

Google, Silicon Valley, and other big tech organizations have significant influence and promote the technological direction regarding AI-advanced capabilities. These companies are advancing AI-enhancements that potentially will transform society and the world. AI advancements are an "optimization technology, meaning it carries out defined tasks as efficiently as possible" in countless industries, which the big tech companies hold the "intellectual property" to advance the methodologies.[71] The DoD would like to work and collaborate with these companies. However, these enterprises "have opaque chains of ownership often tied to Chinese or Russian interests," which is problematic to the DoD.[72]

The reason that these organizations, particularly ones such as Google, have interrelated interests ultimately boils down to money. Nevertheless, there have been recent global governmental concerns and humanitarian backlash, particularly the United States and other western democracies, against the giant tech organizations.[73]

Case in point, in 2018, Google was getting significant attention from both the United States

government and the European Union partners. In December 2018, the United States Congress called Google's CEO, Sundar Pichai, to testify about a variety of issues such as political bias, privacy, and congressional interest of Google's project, Project Dragonfly, and their "concerns over it launching a censored search product in China."[74]

Additionally, the European Union passed the General Data Protection Regulation, which restricts the use of "consumer data for research." As a result, Google is pursuing investments in countries that do not have this type of governmental oversight towards its companies' initiatives and sadly "where illiberal values dominate."[75]

The significance of Google's Project Dragonfly, eventually terminated in July 2019,[76] is how it would have further empowered the Chinese government and the Communist Party. In August of 2018, a Google employee leaked the project's details, which were subsequently reported by the news organization, the Intercept. The Intercept's reporting explained that Google's Project Dragonfly would assist the Chinese government in blocking and blacklisting various websites from the Chinese citizens. Project Dragonfly would also block various word searches that a free republic or democracy would possess, such as, "student protests" or "human rights." More importantly, the Dragonfly initiative would link phone numbers and the searches of a user for the expressed purpose of government exploitation, "meaning that [their] searches could be tracked and traced."[77]

Conversely, Google decided not to work with the Pentagon's AI Maven Project. However, it was willing to work on initiatives, such as the Dragonfly Project, that assist in the linkage of personnel to their online search history and ultimately assist the Chinese government in having greater control of their citizenry.[78] As a result of the backlash of Google's employees pertaining to the AI initiative with the Pentagon,

during the summer of 2018, Google published seven principles for its use of AI:

1. Be socially beneficial;

2. Avoid creating or reinforcing unfair bias;

3. Be built and tested for safety;

4. Be accountable to people;

5. Incorporate privacy design principles;

6. Uphold high standards of scientific excellence;

7. Be made available for uses that accord with these principles.[79]

Interestingly, Google conveyed that "they won't pursue weapons or tech that are likely to cause harm, and that they'll avoid surveillance that violates internationally accepted norms and human rights."[80] Google's AI initiatives (the Maven Project and Project Dragonfly) and its seven principles seem to conflict with each other. As such, Google's employees and humanitarian organizations such as Amnesty International, are establishing initiatives like the "global day of action against" these inconsistencies.[81]

> **...it is likely that Google and the DoD will find partnerships in future initiatives...**

However, it is likely that Google and the DoD will find partnerships in future initiatives with regards to the "military in other domains." More significantly, the DoD and the companies in Silicon Valley all gain from the "substantial cross-pollination of investment and research and development," as in the case of "CIA's venture capital fund In-Q-Tel."[82] In-Q-Tel is a non-profit organization that focuses on research and development, which is "useful to the CIA mission of intelligence gathering."[83] This type

of interrelated cooperation between government and the private sector has brought technological advancements such as Google Maps and is developing potential capabilities like "scanners to create 3-D printed objects."[84]

There are implications of the U.S. government working with industry that is essential to national security. Even though China may be the aggressor in the AI-advanced initiatives, other powerful authoritarian governments know its potential power. As Russian President, Vladimir Putin, conveyed the power that produces AI mastery shall "become the ruler of the world."[85]

> **China is pushing aggressively to be the world leader not only in AI supremacy but other cutting-edge based advancements...**

Consequently, Western nations need to ensure there is a proper balance between national security technological advancements in AI and ethical standards when super-intelligence algorithms are considered, analyzed, developed and eventually established for use. Former leaders such as Henry A. Kissinger, former National-Security Advisor and Security of State, was not too impressed with AI, until 2015, when he was introduced to the facts surrounding how various computer algorithms, that were not "preprogrammed," but how algorithms were able to acquire understanding, by playing "games against itself, learning from its mistakes and refining its algorithms accordingly."[86] Shortly thereafter, AI-advanced algorithms AlphaGo would go onto beat the human Go players "decisively."[87]

Due to his astonishment of the AI achievements, Kissinger went on to write a lengthy piece in the *Atlantic*, in June 2018, titled "How the Enlightenment Ends," where the former National-Security Advisor believes that AI is of national security concern. Additionally, AI needs to be a "major national project" analyzing AI's "full scope," possible implications of AI implementation, and analyzing the "process of ultimate learning." Furthermore, Kissinger expressed concerns that the President and Congress should establish "a presidential commission of eminent thinkers to help develop a national vision." Ultimately, Kissinger's concerns that we as a society consider the possible ramifications of the AI-superintelligence revolution; moreover, societally, have we considered the magnitudes of the "culmination may be a world relying on machines powered by data and algorithms and ungoverned by ethical or philosophical norms." Thus, Mr. Kissinger highlights the importance of AI-superintelligence as a United States national security concern, but the ethical components are essential throughout the process of implementation. Lastly, from his perspective, the technological revolution should be "given a high national priority, above all, from the point of view of relating AI to humanistic traditions."[88]

The United States of America's national security interests are at stake due to authoritarian regimes like China and Russia, which have state-owned organizations giving the governments more control and power. These nations' governmental structure allows them more flexibility and ability to be more intrusive globally. Big technology companies, for example Google, assisting them should be a significant concern regarding America's national security, as well as the security of its like-minded allies.

China is pushing aggressively to be the world leader not only in AI supremacy but other cutting-edge based advancements such as the fifth generation communications improvements, known as 5G, which will have ramifications to bolster the communist's interests of dominance and surveillance globally. Additionally, other invasive regimes, such as Russia, are constantly using military invasions, false

information campaigns, propaganda, technology encroachments, and social media to continuously push the boundaries of war in countries such as Georgia, Crimea, Ukraine to improve its competitive advantage. Russia is using the previously stated technologies to destroy their enemy in ways that have not been observed before.

Lastly, the U.S. government needs to analyze the ramifications of big technology organizations' support to totalitarian regimes and the promotion of desires other than U.S. national security interests, as well as its impact on U.S. and U.S. allies' objectives to preserve ethics, freedom, liberty and the rule of law. The proper development of a strategy and use of AI-based advancements can assist in maintaining those aspirations.

Google's DeepMind Artificial Intelligence Research and Development Initiative

The ultimate goal of artificial intelligence experts is to create or design "an algorithm that learns, tabula rasa, superhuman proficiency in challenging domains."[89] According to *Merriam-Webster*, "*tabula rasa*" means "the mind in its hypothetical primary blank or empty state before receiving outside impressions."[90] *Tubula rasa* is a sixteenth-century concept and gained prominence due to British philosopher, John Locke, who promoted and advocated for the concept in the "*Essay Concerning Human Understanding* in 1690 that the term gained widespread popularity in our language."[91] Moreover, today's AI promoters like to endorse the idea of *tabula rasa*; however, even though recent results in AI progressions have been phenomenal advancements, the algorithm(s) did not exactly start at a "blank state."[92] According to a December 2018 PBS and NOVA Next's article, AI-based capabilities and actual true intelligence, "Programmers are still feeding it one crucial morsel of human knowledge: the rules of the

game it is about to play. 'It does have far less to go on than anything has before,' ...'but the most fundamental thing is, it's still given rules. Those are explicit.'"[93] Thus, technology is moving incredibly fast, and with every new day and with various AI projects, there seem to be significant advances since the prior year. Following is a look at initiatives in recent years and what noteworthy advancements were achieved.

Scientists and researchers have used AI platforms to challenge individual gaming champions for years. One of the most monumental accomplishments of AI advancements happened in 1997 when International Business Machines (also known as IBM) designed and developed a supercomputer, named Deep Blue, which subsequently "beat the world chess champion Garry Kasparov."[94]

> The ultimate goal of artificial intelligence experts is to create or design "an algorithm that learns..."

Fast-forward, a score of years later, the story of computer programs AlphaGo Lee, AlphaGo Fan, AlphaGo Master, AlphaGo Zero, and AlphaZero, which exemplifies the astonishing advancements, and potential of the implementation of technology and AI. These algorithmic computer programs use the complicated game of "Go," a "two-player strategy game" which was invented 3,000 years ago in China and is still very popular in East Asia.[95] The game of Go is difficult and challenging conceptually due to the number of possible strategic movements during each of the opponent's moves. Google's DeepMind AI Project, developed a computer program named AlphaGo, which integrates machine learning processes into a computer program that plays the game Go.[96]

First, DeepMind's programmers used

an AlphaGo variant named AlphaGo Fan to challenge Mr. Fan Hui, a Go master and European Champion of the game Go. In October of 2015, this AlphaGo variant, AlphaGo Fan, was the first computer "program to achieve superhuman performance in Go."[97] Subsequently, in March of 2016, the computer program went up against another one of the world's greatest players of the game and beat "South Korean Go master Lee Se-dol–was viewed as an important test of how far research into artificial intelligence has come in its quest to create machines smarter than humans."[98] This time the DeepMind programmers used an AlphaGo variant, named AlphaGo Lee, to challenge and defeat Lee Se-dol. The chief executive and founder of Google's AI Team of DeepMind, Mr. Demis Hassabis, conveyed that AlphaGo's victory over Lee Se-dol was a "historic moment," moreover, the computer program's "central advantage of AlphaGo was that 'it will never get tired, and it will not get intimidated either.'"[99]

> **...the DeepMind AI Project's programmers adjusted the computer program to play against itself and learn from these processes.**

Between 2015 and 2016 the two AlphaGo variants, Fan and Lee, were programmed similarly by the DeepMind programmers. In an October 2017 article, published by *Nature*, the DeepMind Team explained in detail how the AlphaGo variants were designed:

> AlphaGo Fan used two deep neural networks: a policy network that outputs move probabilities and a value network that outputs a position evaluation. The policy network was trained initially by supervised learning to accurately predict human expert moves, and was subsequently refined by policy-gradient reinforcement learning.

The value network was trained to predict the winner of games played by the policy net-work against itself. Once trained, these networks were combined with a Monte Carlo tree search to provide a look ahead search, using the policy network to narrow down the search to high-probability moves, and using the value network (in conjunction with Monte Carlo rollouts using a fast rollout policy) to evaluate positions in the tree.[100]

Subsequently, the computer program significantly matured in one year. During May 2017, in Wuzhen, China, a Go summit had taken place, however, interestingly the conference was censored to Chinese citizens.[101] Furthermore, the government had websites blocked to ensure all broadcasts were expurgated to its citizenry. The significance of the event was that the AlphaGo Program would beat the Chinese national, Mr. Ke Jie, the Go master and world champion of the game Go. Ke Jie explained that when he played a previous version the year before, it was "still quite humanlike." However, he went on to convey that due to the astonishing strategic moves that AlphaGo made, "this year, it became like a god of Go." Further, other various Go players "have praised the technology's ability to make unorthodox moves and challenge assumptions core to a game that draws on thousands of years of tradition."[102]

The way the AlphaGo Computer Program had learned to play the game of Go is that the DeepMind AI Project's programmers adjusted the computer program to play against itself and learn from these processes.[103] Moreover, the significant development of AlphaGo was due to the programmers' adjustments to improve the "algorithms' efficiency and potential to be generalized across a broader set of problems."[104] The big take away from this event between the AI Computer Program and Go's Champion, Ke Jie, is that "AlphaGo showed yet another way that computers could be developed to perform

better than humans in highly complex tasks, and it offered a glimpse of the promise of new technologies that mimic the way the brain functions."[105]

Successively, DeepMind's programmers developed AlphaGo Zero. Four components differentiate Zero against the predecessor AlphaGo variants. According to the October 2017 article published in *Nature*, the four components are:

First and foremost, it is trained solely by self-play reinforcement learning, starting from random play, without any supervision or use of human data. Second, it uses only the black and white stones from the board as input features. Third, it uses a single neural network, rather than separate policy and value networks. Finally, it uses a simpler tree search that relies upon this single neural network to evaluate positions and sample moves, without performing any Monte Carlo rollouts. To achieve these results, we introduce a new reinforcement learning algorithm that incorporates lookahead search inside the training loop, resulting in rapid improvement and precise and stable learning. Further technical differences in the search algorithm, training procedure and network architecture are described in Methods.[106]

DeepMind's programmers have matched AlphaGo Zero against the earlier versions of AlphaGo variations, "which were trained from human data using handcrafted futures, by a large margin."[107] When matched against the variant, AlphaGo Master, which is similar to the Lee and Fan variants and additionally beat the world best players in January of 2017 60-0, the Zero variant of AlphaGo would beat the Master variant eighty-nine games to eleven games. Consequently, DeepMind's research concluded "that a pure reinforcement learning approach is fully feasible" and what is needed is only a couple of more hours to train for the game

properly; additionally, this "achieves much better asymptotic performance, compared to training on human expert data."[108]

The significant difference between its predecessors, the AlphaGo variants, is that AlphaZero can play chess, shogi, as well as Go, simultaneously.[109] These are impressive advancements of scientists, researchers, programmers, and innovators to reach the objective of AI computer superintelligence. However, there is much innovational improvement that needs to be accomplished in regards to the amount of energy consumed to conduct these AI computational tests: "This intensive regimen also used 5,000 of Google's proprietary machine-learning processor units, or TPUs, which by some estimates consume around 200 watts per chip. No matter how you slice it, AlphaZero requires way more energy than a human brain, which runs on about 20 watts."[110]

> **...AlphaZero requires way more energy than a human brain, which runs on about 20 watts.**

However, the progress of Google's DeepMind AI-initiatives and achievements cannot be denied. These DeepMind initiatives are achieving "A long-standing goal of artificial intelligence is an algorithm that learns, tabula rasa, superhuman proficiency in challenging domains."[111]

Limitations of Artificial Intelligence

In order for the full spectrum of IA-enabled capabilities to be fully realized, it is prudent to see where the private sector and academia are within the spectrum of AI capabilities, AI struggles, and AI limitations. According to Macy Bayern at Techrepublic, there are three limitations. The three areas of concern are (1) data, (2) bias, and (3) lack of process knowledge by employees.[112] Consequently, the big takeaway

is that data needs to be organized suitably in order to implement AI-based initiatives appropriately. Thus, the United States Congress needs to legislate and ensure that all GEOINT partners, from the NGA to various DoD partners, allied partners, and commercial partners develop and use a recognized standard of the organization and proper storage of data and information. This order of storage should start immediately to ensure that AI-based advancements, deep learning, and machine learning can be used rapidly to assist leaders in their decision-making processes.

> **...in order for the DoD to use AI-based advancements properly the data structure needs to be controlled and categorized in a format AI algorithms can comprehend.**

Therefore, in order for the DoD to use AI-based advancements properly the data structure needs to be controlled and categorized in a format AI algorithms can comprehend. Case in point, if we analyze the English language and the Spanish language, the languages are structured differently. Consequently, an AI algorithm would be unable to understand the noise of unstructured data if the algorithms were only designed to understand the Spanish language, but not the English language. The AI algorithms need to be programmed with knowledge of items and nicely classified in a common language for it to work efficiently and effectively. That is the great challenge in order to incorporate AI-advancements properly.

Artificial Intelligence-based Initiatives in Government

The AI initiatives are proving to be extremely beneficial. In Phil Goldstein's article titled, "Air Force, NGA Embrace AI in Different Ways," Goldstein explains that the United States' Air Force is unitizing AI enhancements to improve the DoD component's operations. In collaboration with the Defense Innovation Unit the Air Force is looking to save cost and time on its equipment's maintenance. Defense Innovation Unit's mission is "identifying highly relevant technology companies and matching them to Defense Department customers through collaborative, agile business processes." By providing data on a specific platform the Air Force "cut unscheduled maintenance time for aircraft by 30 percent, boosting the fleet's maintenance reliability rate."[113]

The AI-advanced initiatives are also ensuring security against various malicious attacks. In December of 2018, the Intelligence Advanced Research Project Activity announced a draft Broad Agency Announcement regarding its TrojAI Program to combat attacks on AI systems by various Trojans. Intelligence Advanced Research Project Activity-BAA-19-03 synopsis for solicitation number is explained as follows:

> Using current machine learning methods, an artificial intelligence (AI) is trained on data, learns relationships in that data, and then is deployed to the world to operate on new data. For example, an AI can be trained on images of traffic signs, learn what stop signs and speed limit signs look like, and then be deployed as part of an autonomous car. The problem is that an adversary that can disrupt the training pipeline can insert Trojan behaviors into the AI. For example, an AI learning to distinguish traffic signs can be given just a few additional examples of stop signs with yellow squares on them, each labeled "speed limit sign." If the AI were deployed in a self-driving car, an adversary could cause the car to run through the stop sign just by putting a sticky note on it. The goal of the TrojAI program is to combat such Trojan attacks by inspecting AIs for Trojans.[114]

Thus, the overall goal of the TrojAI program is to protect AI systems from adversary's attempts to place malicious malware within the platform. The desire of Intelligence Advanced Research Project Activity would be "a system that can process about 1,000 AIs per day."[115]

An additional AI-based initiative that the DoD is working on is from the.Defense Advanced Research Projects Agency (DARPA). DARPA is responsible for the improvement of evolving technologies for DoD. Their AI initiative, named Knowledge-directed Artificial Intelligence Reasoning Over Schemas, or KAIROS, will use "something called schema-based AI to better comprehend events around the world, specifically helping uncover complex events found in multimedia information and bring them to the attention of system users."[116]

The NGA has models of collaborative challenges similar to both DARPA and Intelligence Advanced Research Project Activity initiatives that offer "financial incentives to compel and inspire investment/innovation, promote diversity, and drive solutions in automation and GEOINT Assurance." The NGA is implementing a collaborative challenge approach, as well as ensuring appropriate Structured Observation Management for geospatial data, and incorporating new ideas such as the SpaceNet "Open data initiative with IQT Lab CosmiQ Works to foster innovation in automation of imagery analytic tasks. It brings a collaborative approach from machine learning analysis to commercial imagery and training data in order to develop algorithms to extract information." The use of the aforementioned GEOINT advanced-AI strategy processes will incorporate a unity of effort, build confidence and trust, promote innovation, enhance relevance, encourage anticipatory intelligence, and ensure the U.S. government will outpace the nation's near-peer and peer adversaries and maintain its competitive advantage in the future battlespace.[117]

Nevertheless, on October 27, 2018, on the Federal Executive Forum regarding technological advances in machine learning and AI in government, government principals from various agencies deliberated about the new technological advancements and their development for organizational implementation for AI initiatives. Participant Mr. William "Buzz" Roberts, the NGA representative, explained that the NGA problem set and GEOINT sphere is significantly more challenging and complex than initiatives such as Google's DeepMind AlphaGo project, albeit impressive that the latest AlphaGo variant can beat fifty players simultaneously.[118] "NGA is an open-ended issue. Further, the NGA has to master a deluge of data which it sifts through and master the data as quickly as possible with increased accuracy, quantity, [and] persistence of results." Roberts explains that organizational leadership pursuing AI initiatives should ensure that there needs to be clarity of objectives operationally.[119]

> ...the NGA problem set and GEOINT sphere is significantly more challenging and complex than initiatives such as Google's DeepMind AlphaGo project...

In addition, Roberts clarified that there are three focus areas to ensure there is a proper understanding thereof. Those participants in AI initiatives need to focus on the comprehension of technology and advanced methods, ensure that data is structured adequately from partnerships (both indirect and direct), and finally get a proper understanding of the organization's domain.[120]

Roberts expounded that the NGA's global mission set regarding the safety of navigation, impacts both aircraft and vessels globally. The NGA has to be accurate continuously and leverage what is emerging and then apply it to the NGA's problem set. The NGA must ensure

there is accurate data for all those making intelligence decisions and ensure adequate and accurate delivery.[121]

In order to successfully implement a proper AI-based initiative the data needs to be adequately structured. Consequently, data is the problem. AI-based initiatives need to properly understand the data to complete their algorithms' intended purpose. The process of conflation is the solution that can assist organizations to accurately and precisely categorized divergent datasets.

> **Humans have abilities in awareness, perception, and decision-making...AI is excellent at tracking and monitoring massive amounts of data, transactions, and components.**

Citygate GIS has a methodology that is explained as "Conflation is the process of matching features between data sets created at different times and based on different levels of accuracy and precision. Once features have been matched the goal is often to transfer attribute data from one data set to the other."[122] Citygate GIS has a fully automated conflating system, named ConfleX, which is compatible to work with ArcGIS analyzing large data sets.[123] The process of conflation is able to assist the governmental components or other organizations ready to implement AI-based initiatives to overcome the problematic issues of unstructured or uncategorized data.

The concept of conflation is not new. Through collaboration efforts in 2015, the NGA entered into public-private sector partnership with DigitalGlobe in an unclassified initiative named Hootenany to "harness the power of the power of crowdsourced mapping for Geospatial Big Data Analytics."[124]

Thus, the NGA has incorporated the process of conflation into its architecture. The NGA's technology and integration initiatives are leveraging advancements and incorporated automation, AI-based capabilities, and augmentation to improve the agency's processes. There are six focus areas including change detection, data utility and generalization, automated feature extraction and automated attribute population, data validation, as well as map finishing. The final focus area of mass data conflation and metadata tagging is significantly profound because it "conflates all vector and attribute types from multiple datasets into a 'best of breed' final dataset."[125]

The Future of Human, Machine, and Artificial Intelligence-Based Augmentation

According to AI expert Mr. Maurice Conti, society is moving into a new era when it comes to humanity working.[126] Conti explains that four major historical eras define how humans worked: the Hunter-Gather Age, the Agricultural Age, the Industrial Age, and the Information Age. Further, he explains that humans are "on the cusp of our next great era as a species," which would be considered as the Augmented Age. There will be an interconnectional relationship between humans, robots, as well as AI-based capabilities to complete tasks and solve complex problems. Humans have abilities in awareness, perception, and decision-making, whereas, robotics are excellent at exercising instructions with perfect precision and repetitiveness. Finally, AI is excellent at tracking and monitoring massive amounts of data, transactions, and components.[127]

Thus, Conti goes on to explain that our cognitive, physical, and perceptual abilities will be augmented and amplified by the advancements in AI-based abilities by assisting humans "to imagine and design new stuff, robotic systems are going to help us build and make things that we've never been able to make before."[128]

A 2016 project, named the HIVE, exemplified a cross-disciplinary collaboration experiment in which professionals across the spectrum of computer advancements, robotics, manufacturing, engineering, and design to develop a task working together.[129] "The project involved a 12' tall bamboo pavilion that was built by attendees of the 3 day event, through a unique human, machine, and robot collaboration. With this multi-disciplinary project, we were exploring a number of future-of-design themes, such as emergent design, wearables, internet of things, and human-robotic interaction."[130] Thus, the HIVE experiment demonstrated how the future would incorporate the working relationship of humans, robots, and AI-based advancements, which will control and monitor data, activity, and ensure components accurately and precisely applied.

Thus, AI-based advancements, automation, human-machine teaming will assist organizations by supporting with mundane labor skills to allow humans the freedom to focus on more consequential realms. Further, AI-based processes will be supplementary expedient since the innovation "thinks in ways that humans can't. Algorithms that can monitor and process massive amounts of data, and make conclusions based on patterns in that data are poised to change every avenue of society."[131]

Conclusions

Artificial intelligence technological advancements present numerous possibilities to empower and provide advantages to nations and non-state actors in the future, even though this innovation is only "one of the new battlegrounds for a technology-based arms race."[132] The NGA is the premier DoD intelligence agency that possesses and processes geospatial information, which assists customers to answer critical intelligences issues, challenges, and questions.

The NGA's GEOINT provides products and services to enhance decision-making advantage for senior policy-makers, warfighters, and various governmental and non-governments customers. As an indirect result of its evolution as the leader in geospatial competence, the agency is also positioned to provide the way forward in artificial intelligence-enhanced capabilities, machine learning, deep learning, automation, human-machine teaming, and material infrastructure for all other DoD and non-DoD government agencies, as well as state and local organizations. The agency models leadership by establishing research and development, as well as incorporating appropriate relationships across the spectrum of government, academia, and industry. Ensuring accurate and precise incorporation of advanced technologies of AI will ensure the national security interests and prosperity of United States are well-advanced and well-preserved, and the "NGA will propel the continued dominance of GEOINT to protect American interests."[133]

> **Ensuring accurate and precise incorporation of advanced technologies of AI will ensure [U.S.] national security interests and prosperity...are well-advanced and well-preserved...**

Recent aggressiveness of the DoD's apparatus regarding its AI-based implementation and strategies—the formation of the Joint Artificial Intelligence Center, the Office of the Director of National Intelligence's introduction of the framework of the Augmenting Intelligence using Machines initiative, and the 2019 AI executive order by President Donald Trump—all assist enabling the United States of America to remain competitive in the technology advancement race and proliferation of technology against our competitors and adversaries, principally China and Russia. Additionally, these initiatives allow a strategic

framework in dealing with the private sector organization, which otherwise might hinder the U.S. government's competitive technological advantage; as well as guidance to ensure the government will not be reliant on any one major AI big-tech organization, such as Google.

Partnerships need to be promoted and established across the spectrum of the private sector, academic institutions, international community, federal and state and local civil governmental agencies, NGOs, as well as other partners to ensure sound data with standardization, and to enhance discoverability. The cross-disciplinary collaboration efforts between public-private-academic arenas with allied organizations, both domestic and abroad, will promote the aforementioned analytics and advancements amongst the U.S. government's partners.

Finally, the frameworks allow those who design AI-based initiatives to be well-focused on ethical considerations, protect against existential threats of the United States and its allies, and ensure rigorous preservation of the United States of Constitution, safeguarding America's norms, principles, and values are also well-preserved and well sustained.

Recommendations

For further study, future researchers should focus on ethical considerations pertaining to AI initiatives. Research should be examined by analyzing how authoritarian regimes will use high-tech innovations to control their populace, as well as pursue initiatives to strengthen their competitive and strategic advantage globally. Examination should explore the impact of the ease in which these advancements will be established, promoted, and implemented, in nations that are surveillance states and have state-owned businesses.

A second consideration for future research is to examine the ethical considerations in which various militaries will start to incorporate advanced technology, such as AI-based enhancements, machine learning, deep learning, autonomous machinery, as well as human-machine teaming within their organizations. The research should analyze the new technological advances noted above, as well as the human-in-the-loop notion with how military components will start to incorporate and use these progressions and examine what impact these technological advances have on the future battlefield.

The U.S. Army Command and General Staff College's Officers Course encourages officers to look at war through the prism of ethical apparatuses, such as the ethical triangle—a balance of principles-based, virtues-based, and consequences-based ethical decision-making[134]—and the Just War Theory—a doctrine of military ethics that . postulates that war, while terrible, is not always the worst option.[135] There should be further research on how future technological advancements can be tested by these and other ethical examination methods.

Another possibility for future research is to examine the big technology companies' positions regarding these new innovation and what is their working relationship with the U.S. government. In 2018, Google pulled out of the Project Maven AI initiative with the Pentagon's relating to the company's ethical issues. However, subsequently it was revealed that the Google organization was pursuing other AI initiatives to assist the Communist Chinese regime, which is to advance the totalitarian interests to control their citizenry.

Additionally, the research can explore how American citizens need to be vigilant to ensure they protect their constitutional and civil liberties as big technology evolves and becomes more intrusive in citizens' lives. Lastly, further examination is needed of authoritarian regimes' unrestricted freedom to capitalize on new advancements and how these regimes will use such technologies to enhance

their position globally, whereas Western democracies and Constitutional republics are subject to limitation such as varying laws, regulations, and political bureaucracy. *IAJ*

NOTES

1   Director, National Geospatial-Intelligence Agency (NGA), *NGA Strategy 2025* (Springfield, VA: National Geospatial-Intelligence Agency, 2018), 5, accessed 13 March 2019, https://www.nga.mil/Documents.

2   Department of Logistics and Resource Operations, "F104: Determine, Document, and Resource Organizational Authorizations" (PowerPoint Presentation, Force Management Course, US Army Command and General Staff College, Fort Leavenworth, KS, 2018), slide 4.

3   MacGregor Knox and Williamson Murray, ed., *The Dynamics of Military Revolutions, 1300-2050* (Cambridge, NY: Cambridge University Press, 2009), 12.

4   Office of the Director of National Intelligence (DNI), "How the IC Works/Our Organizations/National Geospatial-Intelligence Agency," INTEL.gov, accessed 13 March 2019, https://www.intelligence.gov/how-the-ic-works/our-organizations/414-nga.

5   National Geospatial-Intelligence Agency (NGA), "Mission," accessed 14 March 2019, https://www.nga.mil/ProductsServices/Pages/default.aspx.

6   Director, NGA, *NGA Strategy 2025*, 2.

7   Susan B. Cassidy, "Covington Artificial Intelligence Update: Department of Defense Establishes Joint Artificial Intelligence Center," *National Law Review*, 16 July 2018, accessed 13 March 2019, https://www.natlawreview.com/article/covington-artificial-intelligence-update-department-defense-establishes-joint.

8   Ibid.

9   National Geospatial-Intelligence Agency (NGA), "Releases Updated Commercial GEOINT Strategy," National Geospatial-Intelligence Agency News Release, 2 August 2018, accessed 17 March 2019, https://www.nga.mil/MediaRoom/PressReleases/Pages/CommercialGEOINTstrategy.aspx.

10   Ibid.

11   Carten Cordell, "NGA Embraces the Promise of AI, But Not Without the Human to Match," *FedScoop*, 28 September 2018, accessed 27 April 2019, https://www.fedscoop.com/nga-embraces-promise-ai-not-without-humans-match.

12   Frank Konkel, "NGA Launches Bold Recruitment Plan to Hire Silicon Valley's Best," Nextgov, 8 December 2017, accessed 27 April 2019, https://www.nextgov.com/analytics-data/2017/12/nga-launches-bold-recruitment-plan-hire-silicon-valleys-best/144410.

13   Ibid.

14   Cordell, "NGA Embraces the Promise of AI, But Not Without the Human to Match."

15   Office of the Director of National Intelligence, *The AIM Initiative*, 13.

16   Ibid.

17   Major Christopher Telley, *The Influence Machine: Automated Information Operations as a Strategic Defeat Mechanism*, The Land Warfare Papers, no. 121 (Arlington, VA: The Institute of Land Warfare, Association of the United States Army, October 2018), 1.

18   Elana L. Gross, "How Artificial Intelligence Is Transforming the Intelligence Community," Dell Technologies, 1 February 2018, accessed 8 December 2018, https://www.delltechnologies.com/en-us/ perspectives/how-artificial-intelligence-is-transforming-the-intelligence-community/.

19   National Geospatial-Intelligence Agency (NGA), "NGA Awards Four Contracts to Enhance Artificial Intelligence and Automation," National Geospatial-Intelligence Agency News Release, 15 February 2017, accessed 14 March 2019, https://www.nga.mil /ProductsServices/Pages/NGA-awards-four-contracts-to-enhance-artificial-intelligence-and-automation. aspx.

20   Gross, "How Artificial Intelligence Is Transforming the Intelligence Community."

21   NGA, "NGA Awards Four Contracts to Enhance Artificial Intelligence and Automation."

22   National Geospatial-Intelligence Agency (NGA), "NGA Awards First Contract for Broad Agency Announcement to Boost Innovative GEOINT," National Geospatial-Intelligence Agency News Release, 13 July 2016, accessed 25 April 2019, https://www.nga.mil/MediaRoom/PressReleases/Pages/NGA-awards-first-contract-for-Broad-Area-Announcement-to-boost-innovative-GEOINT.aspx.

23   Ibid.

24   Ibid.

25   Federal Business Opportunities, "Broad Agency Announcement (BAA) for Boosting Innovative GEOINT (BIG) Topic Area 10," NC DEFTECT, 21 June 2018, accessed 14 March 2019, https://deftech. nc.gov/opportunities/2018-06-21/broad-agency-announcement-baa-boosting-innovative-geoint-big-topic-area-10.

26   Ibid.

27   National Geospatial-Intelligence Agency (NGA), "NGA Awards Seven Contracts for Advanced Geospatial Analytics," National Geospatial-Intelligence Agency News Release, 11 September 2018, accessed 10 April 2019, https://www.nga.mil/MediaRoom/PressReleases/Pages/NGA-awards-seven-contracts-for-Advanced-Geospatial-Analytics-under-the-Boosting-Innovative-GEOINT-Broad-Agency-Announcement.aspx.

28   Ibid.

29   Ibid.

30   National Geospatial-Intelligence Agency (NGA), "NGA, Partners Complete 2-Meter Resolution Map of Arctic," National Geospatial-Intelligence Agency News Release, 5 October 2018, accessed 27 April 2019, https://www.nga.mil/MediaRoom/PressReleases/Pages/NGA,-partners-complete-2-meter-resolution-map-of-Arctic--.aspx.

31   Federal Business Opportunities (FBO), "Broad Agency Announcement (BAA) for Boosting Innovative GEOINT (BIG)," USA.gov, 8 December 2015, accessed 16 March 2019, https://www.fbo.gov/index?s=op portunity&mode=form&id=315b29fbfd424e0b85facd2acd4ee8fb&tab=core&_cview=0.

32   Ibid.

33   Jenna McLaughlin, "Artificial Intelligence Will Put Spies Out of Work, Too," *Foreign Policy*, 9 June 2017, accessed 18 March 2019, https://foreignpolicy.com/2017/06/09/artificial-intelligence-will-put-spies-out-of-work-too.

34   Ibid.

35   Patrick Biltgen and Stephen Ryan, *Activity-Based Intelligence Principles and Applications* (Norwood, MA: Artech House, 2016), xx, xxiv.

36   Gross, "How Artificial Intelligence Is Transforming the Intelligence Community."

37   Director NGA, *NGA Strategy 2025*, 5.

38   Louis Columbus, "How China is Dominating Artificial Intelligence," *Forbes*, 16 December 2018, accessed 13 March 2019, https://www.forbes.com/sites/louiscolumbus/2018/12/16/how-china-is-dominating-artificial-intelligence/#285d29e42b2f.

39   Elsa Kania, "Emerging Technology Could Make China the World's Next Innovation Superpower," *The Hill*, 6 November 2017, accessed 13 March 2019, https://thehill.com/opinion/technology/358802-emerging-technology-could-make-china-the-worlds-next-innovation-superpower.

40   Ibid.

41   Columbus, "How China is Dominating Artificial Intelligence."

42   Sylvain Duranton, Jörg Erlebach, and Marc Pauly, *Mind the (AI) Gap Leadership Makes the Difference* (Boston, MA: Boston Consulting Group, December 2018), 3, 10.

43   Ibid., 2, 5.

44   Ibid., 6.

45   Columbus, "How China is Dominating Artificial Intelligence."

46   Department of Defense, *Summary of the 2018 National Defense Strategy of The United States of America: Sharpening the American Military's Competitive Edge* (Washington, D.C.: Government Printing Office, 2018), 4, accessed 13 March 2019, https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.

47   Ibid.

48   Ryan Khurana, "The Rise of Illiberal Intelligence," *National Review*, 10 August 2018, accessed 13 March 2019, https://www.nationalreview.com/2018/08/china-artificial-intelligence-race.

49   Wikipedia, "Zimbabwe," Wikipedia Foundation, last updated 11 March 2019, accessed 12 March 2019, https://en.wikipedia.org/wiki/Zimbabwe.

50   Khurana, "The Rise of Illiberal Intelligence."

51   Rachel Botsman, "Big Data Meets Big Brother as China Moves to Rate its Citizens," *Wired*, 21 October 2017, accessed 16 April 2019, https://www.wired.co.uk/article/chinese-government-social-credit-score-privacy-invasion.

52   Josh Chin and Gillian Wong, "China's New Tool for Social Control: A Credit Rating for Everything," *The Wall Street Journal*, 28 November 2016, accessed 25 April 2019, https://www.wsj.com/articles/chinas-new-tool-for-social-control-a-credit-rating-for-everything-1480351590.

53   Ibid.

54 Ibid.

55   Audrey Murrell, "Pushing the Ethical Boundaries of Big Data: A Look at China's Social Credit Scoring System," *Forbes*, 31 July 2018, accessed 16 April 2019, https://www.forbes.com/sites/audreymurrell/2018/07/31/pushing-the-ethical-boundaries-of-big-data-a-look-at-chinas-social-credit-scoring-system/#6dfaa9125e56.

56   Khurana, "The Rise of Illiberal Intelligence."

57   Howard W. French, "Panda Hugger Turned Slugger," *The Wall Street Journal*, 26 February 2015, accessed 13 March 2019, https://www.wsj.com/articles/book-review-the-hundred-year-marathon-by-michael-pillsbury-1424996150.

58   Ibid.

59   Cheryl Pellerin, "Project Maven to Deploy Computer Algorithms to War Zone by Year's End," Department of Defense, 21 July 2017, accessed 13 March 2019, https://dod.defense.gov/News/Article/Article/1254719/project-maven-to-deploy-computer-algorithms-to-war-zone-by-years-end.

60   Ibid.

61   Ibid.

62   Ibid.

63   Daisuke Wakabayashi and Scott Shane, "Google Will Not Renew Pentagon Contract That Upset Employees," *The New York Times*, 1 June 2018, accessed 13 March 2019, https://www.nytimes.com/2018/06/01/technology/google-pentagon-project-maven.html.

64   Ibid.

65   Ibid.

66   Ibid.

67   Ibid.

68   Ibid.

69   Khurana, "The Rise of Illiberal Intelligence."

70   Ibid.

71   Ibid.

72   Ibid.

73   Ibid.

74   Alex Knapp, "Google CEO Sundar Pichai Answered Congressional Questions on China, Privacy, Political Bias and More," *Forbes*, 11 December 2018, accessed 13 March 2019, https://www.forbes.com/sites/alexknapp/2018/12/11/follow-along-with-google-ceo-sundar-pichais-testimony-before-congress-here-1/#6978b6103272.

75   Khurana, "The Rise of Illiberal Intelligence."

76   "Google finally says it will kill censored Chinese search engine Project Dragonfly". *The Independent*. July 17, 2019. Accessed February 12, 2020. https://www.independent.co.uk/life-style/gadgets-and-tech/news/google-china-ban-project-dragonfly-search-engine-project-a9007956.html.

77   Claire Hansen, "Google Employees Protest Controversial Chinese Search Engine Project," *U.S. News and World Report*, 27 November 2018, accessed 14 March 2019, https://www.usnews.com/news/national-news/articles/2018-11-27/google-employees-protest-controversial-chinese-search-engine-project.

78   Ibid.

79   Tom V. Ark, "Google Launches Learning Resources, Publishes AI Principles," *Forbes*, 28 June 2018, accessed 14 March 2019, https://www.forbes.com/sites/tomvanderark/2018/06/28/google-launches-learning-resources-publishes-ai-principles/#6733cca1188b.

80   Ibid.

81   Hansen, "Google Employees Protest Controversial Chinese Search Engine Project."

82   Jimmy Quinn, "Google, AI, and National Defense," *National Review*, 12 June 2018, accessed 20 April 2019, https://www.nationalreview.com/corner/google-artificial-intelligence-national-defense.

83   Damian Paletta, "The CIA's Venture-Capital Firm, Like Its Sponsor, Operates in the Shadows," *The Wall Street Journal*, 30 August 2016, accessed 20 April 2019, https://www.wsj.com/articles/the-cias-venture-capital-firm-like-its-sponsor-operates-in-the-shadows-1472587352.

84   Quinn. "Google, AI, and National Defense."

85   Ibid.

86   Henry A. Kissinger, "How the Enlightenment Ends," *The Atlantic*, June 2018, accessed 14 March 2019, https://www.theatlantic.com/magazine/archive/2018/06/henry-kissinger-ai-could-mean-the-end-of-human-history/559124.

87   Ibid.

88   Ibid.

89   David Silver, Julian Schrittwieser, Karen Simonyan, Loannis Antonoglou, Aja Huang, Arthur Guez, Thomas Hubert, Lucas Baker, Matthew Lai, Adrian Bolton, Yutian Chen, Timothy Lillicrap, Fan Hui, Laurent Sifre, George van den Driessche, Thore Graepel, and Demis Hassabis, "Mastering the Game of Go Without Human Knowledge," *Nature* 550 (19 October 2017), 354, accessed 14 March 2019, https://www.nature.com/articles/nature24270.epdf?author_access_token=VJXbVjaSHxFoctQQ4p2k4tRgN0jAjWel9jnR3ZoTv0PVW4gB86EEpGqTRDtpIz-2rmo8-KG06gqVobU5NSCFeHILHcVFUeMsbvwS-lxjqQGg98faovwjxeTUgZAUMnRQ.

90   Merriam-Webster, "Tabula," Merriam-Webster, last updated 11 March 2019, accessed 14 March 2019, https://www.merriam-webster.com/dictionary/tabula%20rasa.

91   Ibid.

92   Katherine J. Wu, "Google Says It Built A 'Superhuman' Game-Playing AI. Is It Truly Intelligent?" *Nova Next*, 6 December 2018, accessed 27 April 2019, https://www.pbs.org/wgbh/nova/article/google-alphazero-artificial-intelligence.

93   Ibid.

94   Choe Sang-Hun and John Markoff, "Master of Go Board Game Is Walloped by Google Computer Program," *The New York Times*, 9 March 2016, accessed 20 April 2019, https://www.nytimes.com/2016/03/10/world/asia/google-alphago-lee-se-dol.html?action=click&module=RelatedCoverage&pgtype=Article&region=Footer.

95   Dawn Chan, "The AI That Has Nothing to Learn from Humans," *The Atlantic*, 20 October 2017, accessed 18 March 2019, https://www.theatlantic.com/technology/archive/2017/10/alphago-zero-the-ai-that-taught-itself-go/543450.

96   Ibid.

97   Silver et al., "Mastering the Game of Go Without Human Knowledge," 354.

98   Sang-Hun and Markoff, "Master of Go Board Game Is Walloped by Google Computer Program."

99   Ibid.

100   Silver et al., "Mastering the Game of Go Without Human Knowledge," 354.

101   Paul Mozur, "Google's AlphaGo Defeats Chinese Go Master in Win for A.I.," *The New York Times*, 23 May 2017, accessed 20 April 2019, https://www.nytimes.com/2017/05/23/business/google-deepmind-alphago-go-champion-defeat.html.

102   Ibid.

103   Ibid.

104   Deepmind, "AlphaGo's next move," *Deepmind Blog*, 27 May 2017, accessed 20 April 2019, https://deepmind.com/blog/alphagos-next-move.

105   Mozur, "Google's AlphaGo Defeats Chinese Go Master in Win for A.I."

106   Silver et al., "Mastering the Game of Go Without Human Knowledge," 354.

107   Silver et al., 358.

108   Ibid. 358.

109   Wu, "Google Says It Built A 'Superhuman' Game-Playing AI. Is It Truly Intelligent."

110   Ibid.

111   Silver et al., 354.

112   Macy Bayern, "The 3 Most Overlooked Limitations of AI in Business," *TechRepublic*, 3 October 2018, accessed 18 March 2019, https://www.techrepublic.com/article/the-3-most-overlooked-limitations-of-ai-in-business.

113   Phil Goldstein, "Air Force, NGA Embrace AI in Different Ways," *FedTech*, 18 January 2019, accessed 25 April 2019, https://fedtechmagazine.com/article/2019/01/air-force-nga-embrace-ai-different-ways.

114   Federal Business Opportunities, "TrojAI BAA Draft Funding Opportunity Description," FedBizOpps.Gov, 7 December 2018, accessed 18 March 2019, https://www.fbo.gov/index.php?s=opportunity&mode=form&id=93e7534a60d62bc7c44d810c5ea0fdee&tab=core&_cview=0.

115   Phil Goldstein, "Intelligence Community Searches for Ways to Protect AI from Tampering," *FedTech*, 23 January 2019, accessed 25 April 2019, https://fedtechmagazine.com/article/2019/01/intelligence-community-searches-ways-protect-ai-tampering.

116   Mark Pomerleau, "DARPA's Plan for AI to Understand the World," C4ISRNET, 7 January 2019, accessed 25 April 2019, https://www.c4isrnet.com/it-networks/2019/01/07/darpas-plan-for-ai-to-understand-the-world.

117   National Geospatial-Intelligence Agency (NGA), *Commercial GEOINT Strategy - 2018 Update* (Springfield, VA: National Geospatial-Intelligence Agency, 2018), 8, 12, accessed 25 April 2019, https://www.nga.mil/Partners/Pages/Commercial-GEOINT-Strategy.aspx.

118   Federal Executive Forum, "FEF Machine Learning and AI in Government October 2018," *YouTube*, 28 September 2018, accessed 25 April 2019, https://www.youtube.com/watch?v=_7yKoT7EWiM.

119   Ibid.

120   Ibid.

121   Ibid.

122   Citygate GIS, "What is Conflation?" accessed 28 April 2019, http://www.citygategis.com/what-is-conflation.

123   Ibid.

124   National Geospatial-Intelligence Agency (NGA), "NGA and Digital Globe Open Source Toolkit to Harness the Power of Collaborative Mapping," National Geospatial-Intelligence Agency News Release, 22 June 2015, accessed 5 May 2019, https://www.nga.mil/MediaRoom/PressReleases/Pages/2015-16.aspx.

125   NGA, *Commercial GEOINT Strategy - 2018*, 8, 12.

126   TED, "The Incredible Inventions of Intuitive AI/Maurice Conti," *YouTube*, 28 February 2017, accessed 4 May 2019, https://www.youtube.com/watch?v=aR5N2Jl8k14.

127   Ibid.

128   Ibid.

129   Autodesk Research, "HIVE," accessed 4 May 2019, https://autodeskresearch.com/projects/hive.

130   Ibid.

131   Digital Trends Staff, "How A.I. will change your world in 2019, For Better or Worse," Digital Trends, 26 December, 2018, accessed 4 May 2019, https://www.digitaltrends.com/cool-tech/artificial-intelligence-changes-everything-2019.

132   Office of the Director of National Intelligence, *The AIM Initiative*, 11.

133   Director, NGA, *NGA Strategy 2025*, 6.

134   Jack D. Kem, "Ethical Decision Making: Using the 'Ethical Triangle,'" Command and General Staff College, Fort Leavenworth, KS, August 2016. Accessed February 12, 2020. http://www.cgscfoundation.org/wp-content/uploads/2016/04/Kem-UseoftheEthicalTriangle.pdf.

135   Guthrie, Charles; Quinlan, Michael (2007). "III: The Structure of the Tradition". *Just War: The Just War Tradition: Ethics in Modern Warfare*. pp. 11–15.

Proxy Warfare on the Roof of the World:

Great Power Competition Lessons from Tibet

by Steve Ferenzi

Asponsor may disrupt or coerce an adversary with only a small investment in a proxy force without crossing the threshold to traditional armed conflict. Proxy employment represented a significant component of U.S. policy during the Cold War. As the United States once again relies on this tool to compete with peer state adversaries, it is beneficial to examine past engagements that may inform better ways to outsource national security objectives to proxy forces. Central Intelligence Agency support to anti-Chinese resistance forces in Tibet, the "Roof of the World," from 1956 to 1974 accomplished the limited objective of disrupting Chinese regional ambitions as part of the global effort to contain Communist expansion. However, success came at the expense of Tibetan casualties and failure to achieve the resistance's objective of an independent Tibet. This case study offers lessons for future proxy engagements in establishing mechanisms that facilitate proper proxy selection, mitigate deviation from sponsor goals, and optimize proxy capabilities.

Surrogates and Proxies—Then and Now

President Eisenhower characterized proxy warfare as the "cheapest insurance in the world."[1] He recognized the potential to accomplish national security objectives without direct U.S. military involvement by making relatively small investments in surrogate forces. Proxy employment therefore became a significant plank of U.S. national security policy during the Cold War against both the Soviet Union and China. Today, proxy warfare again provides the United States a way to compete below the level of armed conflict by expanding options to compel adversary behavior change and deter undesirable actions.[2] Central Intelligence Agency support to the Tibetan resistance against China from 1956 to 1974 represents a crucial Cold War proxy engagement that may inform better ways to outsource national security objectives to proxy forces.

Major Steve Ferenzi is an Army Strategist and Special Forces officer in the U.S. Army Special Operations Command's G-5 Strategic Planning Division. He has served previously with the 3rd and 5th Special Forces Groups (Airborne) and the 82nd Airborne Division and holds a Master of International Affairs degree from Columbia University's School of International and Public Affairs.

Lack of embedded advisors reduces control over the proxy.
A sponsor's direct advisory presence on the ground signals commitment to the proxy engagement and affords increased opportunity to effect favorable outcomes, but it increases the risk of sponsor exposure.
Using intermediaries reduces sponsor control.
A sponsor's attempt to further distance itself from the conflict and/or spread cost burdens by working through intermediaries will reduce its control over the proxy in proportion to the divergence between their operational objectives. Intermediate proxies often have different goals than the primary sponsor. This imposes significant constraints on a sponsor's ability to optimize proxy effectiveness.
Sponsor control based on resource provision is proportional to the value a proxy places on material support.
Making resources contingent on battlefield effectiveness, equipment accountability, and human rights compliance is not a surefire mechanism to ensure proxy obedience if other cost/benefit calculations dominate the proxy's decision-making process.
Political considerations directly impact both the strategic and tactical aspects of proxy employment.
Divorcing the larger political and strategic considerations that prompted the initial proxy engagement from actual proxy employment on the ground may significantly reduce its effectiveness. Proxy warfare requires an integrated policy approach.

Figure 1. Lessons from CIA support to the Tibetan resistance against China

This case study addresses two key aspects of proxy warfare: 1) force generation and "enabler" efforts without embedded advisors accompanying the proxy, and 2) the advantages and disadvantages of conducting proxy warfare through regional intermediaries.[3] This case also demonstrates adverse proxy selection and agency slack, where constraints on the ability to select the optimal proxy and induce it to perform as intended enabled the Tibetans to act contrary to U.S. preferences.[4] American successes and failures in its support to the Tibetan resistance provide a number of valuable lessons to consider for future proxy employment, both overt and covert. These lessons may apply throughout an entire generic proxy life cycle regardless of the specific temporal and political circumstances; the most significant are summarized in Figure 1 and expanded upon in the final section.

Overview

The U.S. Central Intelligence Agency (CIA) conducted a covert action campaign against China in Tibet from 1956 to 1974 by providing support to the indigenous resistance movement that formed in response to the Chinese Communists' invasion. The CIA's objective was to disrupt China within the framework of the larger policy of containing global Communist expansion. The CIA specifically aimed to reduce China's influence and capabilities by supporting a viable resistance inside Tibet and an autonomous Tibet under the Dalai Lama's leadership.[5] This proxy engagement, code-named "ST CIRCUS," achieved moderate success by disrupting Chinese regional plans, tying up the People's Liberation Army occupation force, and shaping the political discussion concerning Tibet that continues to this day.

Cold War political dynamics caused the United States to withdraw material support in 1969,
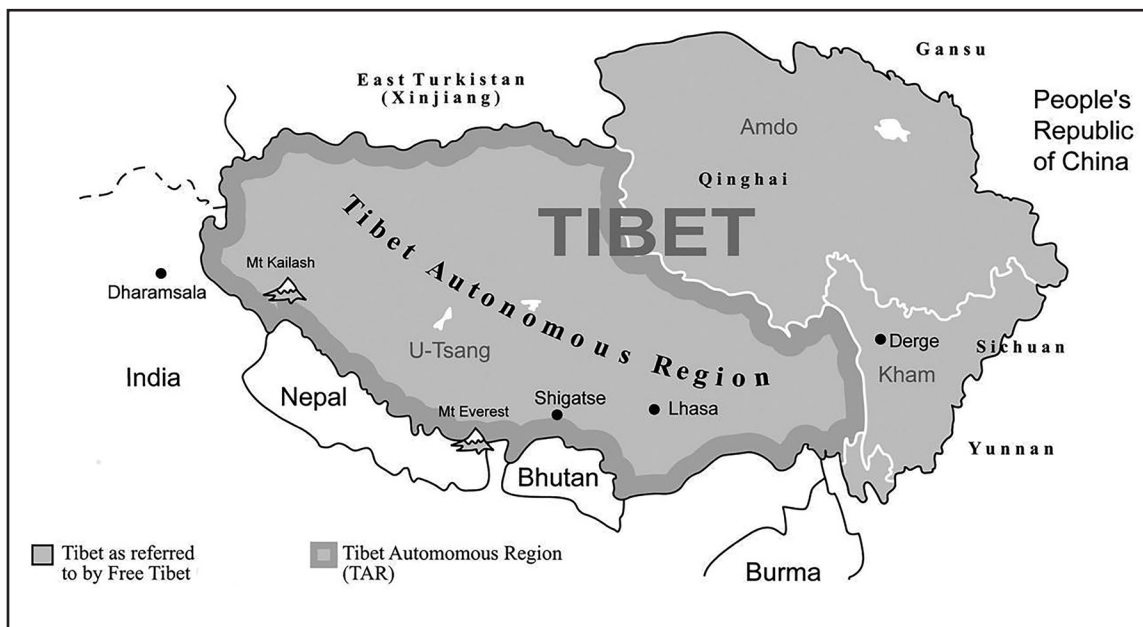
Figure 2. Map of Tibet (Source: Free Tibet)

demonstrating that sponsorship of the Tibetan proxy had fit into America's larger policy of destabilizing Communist regimes at the expense of the indigenous movement's political aspirations. The United States officially severed ties in 1974 by cutting the covert subsidy it had been paying to the Dalai Lama to support the government-in-exile, as rapprochement with China became the Nixon administration's priority.

Background

Nearly three miles above sea level, the Tibetan Plateau is known as the "Roof of the World."[6] Tibetans have historically maintained their independence through geographic separation afforded by harsh terrain and a priest-patron relationship whereby spiritual mentorship held the power of mainland China at bay. This association became a formalized power structure in the 16th century when Mongol chieftain Altan Khan bestowed the honorific title of "Dalai Lama" on a prominent Buddhist monk, establishing the religious and temporal authority of subsequent Dalai Lamas.[7]

The Qing Dynasty took control of the Ambo and Kham regions of Tibet between 1724 and 1728. Tibet declared its autonomy in 1913 following the overthrow of the Qing Dynasty, a situation that lasted until the Chinese Communist Party seized power in 1949. Intent on consolidating what it considered Chinese territory, the People's Liberation Army dispatched 20,000 troops to "realize the peaceful liberation of Tibet" and defeated the Tibetan army in Kham in 1950.[8]

The Chinese Communist Party subsequently established administrative control of villages throughout the eastern region of Kham and eventually all of Tibet. Extensive reforms based on Chinese revolutionary ideology stripped local leaders of power and disrupted traditional Tibetan life, causing villagers across the social spectrum to rise in protest. The armed Tibetan resistance began as a series of independent uprisings in opposition to Chinese policy in Kham, which turned into a widespread revolt in 1956 when Chinese forces bombed four monasteries and killed thousands of monks and civilians.[9]

The Dalai Lama's failure to achieve an acceptable peace with China and the growing popular resistance encouraged the Dalai Lama's elder brother, Gyalo Thondup, to contact the CIA in Calcutta in 1956.[10] The first phase of U.S. sponsorship of Tibetan proxies against the Chinese consisted of only six Tibetan refugees selected by the CIA and Gyalo Thondup to receive training and serve as its initial agents.[11] The official armed Tibetan resistance movement formed in June 1958 after local leaders decided to unite their formerly separate elements into a unified army of roughly 5,000 volunteers, taking the name *Chushi Gangdruk* in reference to the "four rivers and six ranges" of Kham.[12] The last façade of Tibetan autonomy evaporated after the Dalai Lama fled from Lhasa to India in March 1959.

Sponsor and Proxy Goals

Sponsor-proxy engagements took the form of a complex relationship between the United States, India, and the Tibetan resistance. The United States served as the primary sponsor, using the Tibetan proxy as a tool in the global fight against Communism. India served as a regional sponsor and intermediate U.S. proxy, providing sanctuary for the Tibetan government-in-exile, a joint operations center, and guerrilla training areas, and it ultimately siphoned off Tibetans meant for the resistance to use as a means to protect India's vulnerable northern border with China.

The United States

The United States took little interest in Tibet until Chinese Communist forces invaded in 1950. Previous interaction consisted of a secret reconnaissance mission executed by the Office of Strategic Services in 1942 to assess the feasibility of using Tibet as a resupply route to China after Japanese forces cut the Burma Road. This expedition laid the groundwork for future U.S. involvement, but also foreshadowed

the complex relationship that would develop throughout the Tibetan resistance period.[13]

As a plank in the global effort to contain Communist expansion, U.S. sponsorship of the Tibetan resistance was a perfect opportunity to confront Communism by means other than direct and costly military intervention.[14] Consistent with NSC 5429/5, the United States had an interest in "keep(ing) the rebellion going as long as possible."[15] A memorandum to the 303 Committee for covert actions oversight defined the program objectives as:

> "toward lessening the influence and capabilities of the Chinese regime through support, among Tibetans and among foreign nations, of the concept of an autonomous Tibet under the leadership of the Dalai Lama; toward the creation of a capability for resistance against possible political developments inside Tibet; and the containment of Chinese Communist expansion"[16]

U.S. ideological commitment to freedom and the resistance's practical utility as a disruptive mechanism kept U.S. interest in Tibet relatively static until President Nixon's rapprochement with China in 1972. In light of this political shift, support to the Tibetan resistance undermined efforts to establish China as a counterbalance to the Soviet threat, and the United States subsequently phased out its support completely in 1974.[17]

India

Indian support to the Tibetan resistance fluctuated based its regional position vis-à-vis China and Pakistan. India initially recognized China's sovereignty over Tibet, attempting to maintain cordial relations in order to cultivate Beijing as an offset to Pakistan, but it also built relations with Tibet in order to improve border security after China's invasion of Kham in 1950.[18] India reversed its position in 1959 by

granting the Dalai Lama asylum and hosting a Tibetan government-in-exile after the brutal Chinese shelling of unarmed Tibetans forced him to flee.[19] The 1962 Sino-Indian War, in which China seized 14,500 square kilometers of Indian Kashmir, created an alignment of interests between the United States and India in using the Tibetans as a proxy against China.[20] The Tibetans represented a means of guarding India's vulnerable northern border and a potential force for attaining an independent Tibet that would facilitate long-term security in the Himalayas.[21]

> **The establishment of the Combined Operations Center in New Delhi in 1964 formalized U.S.-Indian-Tibetan cooperation...**

The establishment of the Combined Operations Center in New Delhi in 1964 formalized U.S.-Indian-Tibetan cooperation, but India subsequently attained more influence over operations as the joint command was based on their soil.[22] U.S.-Indian relations deteriorated in the mid-1960s as India aligned itself with the Soviet Union in response to the increased threat embodied in Mao's Cultural Revolution and China's successful test of a medium-range nuclear ballistic missile in 1966. This new relationship adversely affected cooperation between the United States and India concerning guerrilla operations and assistance to the Tibetan government-in-exile. Coupled with drawdown of U.S. covert support and perception of the guerrillas' ineffectiveness, India decreased most of its joint paramilitary operations by the spring of 1967.[23]

Tibetan Resistance

The Tibetan resistance sought to achieve territorial independence from a Communist China that posed an existential threat to the Tibetan way of life. Mao's declaration to the

Dalai Lama that "religion is poison" was confirmed as early as 1955 when the People's Liberation Army implemented an atheist education system to supplant Buddhism, private and monastic property confiscation, and public humiliations and executions that incited the initial local protests.[24] The 1966 Cultural Revolution carried this to its completion as the Red Guards set about destroying the last vestiges of Tibetan identity.[25]

According to the Dalai Lama, "The CIA was pursuing a global policy against Communist China, while we were opposing Communist aggression in our country; our basic aims did not clash, so we accepted it (assistance from the CIA)."[26] Gompo Tashi, the leader of the *Chushi Gangdruk*, stated in a letter requesting support from President Eisenhower in 1959:

> "We Tibetans have determined to fight to the last against the Chinese Communists... as there is no alternative left for us except to fight. We see no other Powers other than the United States which is capable of giving us help in every respect to free Tibet from the domination of Red China."[27]

Recruitment through Employment

CIA support to the Tibetan resistance began as a pilot program in 1957 to train small teams in guerrilla tactics and intelligence collection outside of Tibet. The CIA inserted these elements back into Tibet and logistically supported them with covert U.S. air assets. This effort expanded to train resistance fighters on a larger scale in the United States prior to insertion back into Tibet to conduct operations. In the early 1960s, the CIA switched from parachuting agents into Tibet to supporting the resistance at the Mustang base in Nepal. By 1968 the United States began to phase out its support as Chinese military control became so great that further guerrilla operations would be futile. In the summer of 1974 the United States officially severed ties with the resistance by cutting the covert subsidy it had

been paying to the Dalai Lama in support of the government-in-exile.[28]

The CIA also executed a parallel effort with the Indian Intelligence Bureau to train and equip Tibetans for service in the Indian Special Frontier Force, a unit designed to conduct intelligence gathering and commando operations against China following the Sino-Indian War of 1962. Other efforts included the education of Tibetans at Cornell University and the establishment of Tibetan advocacy groups in the United States, India, and Europe.

Pilot Team Operations

In February 1957 six Tibetan Khampas were selected from a pool of 27 refugees in India to serve as a "pilot team" that would be tasked with infiltrating Tibet and assessing the state of the resistance. Gyalo Thondup, the Dalai Lama's brother, chose these candidates, and the CIA flew them from East Pakistan (currently Bangladesh) to Saipan in the Northern Mariana Islands for training. Three CIA teams instructed the Khampas on espionage techniques, Morse code and radio communications, and guerrilla warfare, condensing a full year curriculum into approximately four months.

The CIA inserted the pilot team without U.S. advisors from East Pakistan via parachute, using covert air platforms with Polish pilots for deniability. This aerial delivery portion of ST CIRCUS was subsumed under the codename ST BARNUM. (ST was the CIA country code for East Asia, including Tibet.) Though it sustained three fatalities throughout the course of its activities, the pilot team linked up with the resistance and reported to the CIA. After determining that the resistance was operational, the CIA decided to proceed with material support and to train a second group of Tibetans.[29]

U.S.-Based Training Expansion

Training expansion began with a second contingent of Tibetans consisting of ten Khampa refugees that mirrored the ethnic composition of the first group. The training location moved from tropical Saipan to Camp Hale, Colorado, in order to better replicate the elevation of Tibet. The CIA implemented a ten-month pipeline to develop a trained Tibetan cadre that would have a multiplier effect for the resistance movement. While successive airborne teams succeeded in establishing a network among existing resistance elements and organizing resupply through the CIA, People's Liberation Army military operations and U.S. domestic political constraints resulted in significant guerrilla casualties. The United States prohibited overflights after the downing of a U-2 spy plane in Soviet airspace in 1960. This, coupled with the potential for political fall-out resulting from covert operations during the 1960 presidential elections, caused the United States to suspend resupply to the guerrillas for almost a year.[30]

> **The CIA also executed a parallel effort with the Indian Intelligence Bureau to train and equip Tibetans for service in the Indian Special Frontier Force...**

By late spring of 1960 all the airborne teams operating inside Tibet were non mission capable. Of the 49 agents dropped into Tibet since 1957, 37 had been killed, one was captured, and one surrendered. The remainder escaped back to India. Resistance leadership attributed the overall failure to several factors: the guerrillas would not listen to the cadres' advice to disperse, and continued to engage the Chinese in frontal assaults; the resistance could not sustain itself in the infertile countryside where it resided; and there was no communication between the different operational areas to synchronize their efforts. These losses forced the CIA to reevaluate its overall strategy for resistance support.[31]

From 1964 to 1967, the CIA inserted 25 additional elements classified as "radio teams"

Figure 3. Mustang Kingdom in Nepal (Source: Tibet Truth)

along the border primarily in central and western Tibet for the purpose of intelligence collection. Finding little support among the local population, most of the teams returned to India within weeks. By 1967 the CIA terminated this mission as it became evident that the risks were not worth the scattered intelligence the teams were delivering.[32]

Approximately 250 Tibetans received instruction under the U.S.-based training program until its termination in November 1964. The Fiscal Year 1964 budget allocated $585,000 (approximately $4.9 million in 2019 dollars)[33] for this program annually, with $400,000 for training expenses in Colorado and $185,000 for the covert air transportation from Colorado to India.[34]

External Sanctuary in Nepal

Gompo Tashi Andrugstsang, a successful trader from a reputable family who enjoyed support from Tibetan government leaders loyal to the Dalai Lama, began organizing a resistance in 1956 originally called *Chushi Gangdruk* (in reference to the "four rivers and six ranges" of Kham).[35] Gompo oversaw its reorganization into the unified resistance movement named

the National Volunteer Defense Army in 1958. Overwhelmingly composed of ethnic Khampas, this name change was an intentional effort to break from *Chushi Gangdruk's* regional overtones and appeal to all Tibetans. The National Volunteer Defense Army suffered from a Khampa brigand stereotype held by many central Tibetans due to Lhasa's and the Tibetan army's public opposition to anti-Chinese resistance, resulting in little local popular support in central Tibet.[36]

Initial CIA support to the National Volunteer Defense Army consisted of aerial resupply coordinated by the pilot teams and the paramilitary training imparted by the teams to the resistance elements. By mid-April 1959 Chinese troops and air power overwhelmed the National Volunteer Defense Army, forcing the leadership to seek sanctuary elsewhere while local resistance elements remained to disrupt Chinese supply routes along the Sichuan-Lhasa highway and the highway from Lhasa to Qinghai. In an effort to revive the resistance movement, Gompo proposed they regroup in the bordering Mustang kingdom of north-central Nepal, from which they could then operate inside Tibet. The CIA approved a plan to take 2,100 men from

the scattered National Volunteer Defense Army, reconsolidate them in Mustang as 300-man elements, and send them back across the border to conduct guerrilla attacks. The plan envisioned seven groups operating independently in Tibet with support in the form of aerial resupply and trained leaders.[37]

A major problem developed as word spread quickly of the newly established guerrilla base, drawing an immediate influx of 2,000 volunteers from local road construction gangs instead of the planned groups of 300. This overwhelmed the capacity to feed, supply, and train the men, and Indian newspapers began a series of articles about the exodus that exposed the intended covert nature of the operation. The Mustang operation eventually continued as the Kennedy administration took over and overflights resumed. The guerrillas achieved limited success by attacking isolated Chinese military camps and disrupting major highway supply routes, forcing China to post one division in the area and diverting traffic from western Tibet to the Qinghai-Xingjian highway 300 kilometers to the north. Captured documents also provided significant intelligence illustrating the serious Chinese governance problems that resulted from Mao's Great Leap Forward.[38]

Tension built as Washington vacillated between the utility of maintaining the Mustang force as a capability against China and the potential dangers it presented to ongoing diplomatic efforts to achieve Tibetan independence. As a result, the CIA did not fully resource the resistance to execute its intended operations, a situation further exacerbated by internal Tibetan leadership schisms and their lack of desire and inability to establish bases across the border as per the original plan. Failure to put CIA advisors on the ground and Mustang's geographical isolation ensured that the Mustang commander, Baba Gen Yeshi, "was free from scrutiny and, as such, a general who was accountable to no one."[39] By 1968 the

guerrilla force at Mustang consisted of 1,800 men, and no efforts had been made to recruit new members since the original 1961 influx.[40] Annual operating costs to support approximately 2,100 guerrillas at the Mustang base were budgeted at $500,000 dollars (approximately $4.2 million in 2019 dollars).[41]

Political will for continuing support to the guerrillas decreased as new U.S. government leadership began to consider the eight year Mustang project an outdated commitment. The CIA informed Gyalo Thondup in early 1969 that it was withdrawing support for the Mustang force. A number of resistance elements continued operations until Nepal began an anti-Khampa campaign denouncing the Mustang force. In 1974 Nepal forced the guerrillas to surrender their arms in response to the pressure on Nepal's king by Mao beginning in 1973.[42]

Special Frontier Force

The 1962 Sino-Indian War precipitated closer U.S.-Indian ties. The CIA and the Indian Intelligence Bureau collaborated in the creation of a Tibetan guerrilla force known officially as the Special Frontier Force, and more popularly as "Establishment 22." Gyalo Thondup was responsible for the initial recruitment of Tibetan exiles that would eventually number approximately 12,000, presuming that these men would only conduct resistance activities in Tibet. However, India intended to use the Special Frontier Force to protect India's borders if war with China were to break out again, and India did not authorize them to cross into Tibet for the purpose of confronting the Chinese. After six months of basic training identical to the Indian army's, the CIA supplemented their instruction with commando and guerrilla warfare tactics, sabotage, and explosives in the Indian town of Chakrata. The Indians sustained the Tibetans' motivation by maintaining the illusion that the troops were preparing for their own war of liberation.[43]

The United States, India, and the Tibetan resistance established the Combined Operations Center in New Delhi in 1964 to assume direction of the Camp Hale operations and the guerrilla operations at Mustang, but the Indians exercised sole command over the Special Frontier Force. Friction developed in trying to define the role of the Mustang force in relation to Special Frontier Force operations, as well as the overall objectives of the three member parties.[44]

> **The United States terminated its relationship with the resistance as it could no longer effectively accomplish U.S. objectives…**

By 1971 direct CIA contact with the Special Frontier Force had almost ceased. Against the backdrop of escalating Indian-Pakistani tensions, India employed 3,000 members of the Special Frontier Force in Operation EAGLE, participating in direct combat against Pakistani forces in East Pakistan as part of India's efforts to facilitate future Bangladesh's independence. As tensions with Pakistan eased by the late 1970s, the Special Frontier Force received a new internal counterterrorism mission, and it continues today as part of the Indian military establishment.[45]

Non-Combat Efforts

The United States led additional efforts to support the Tibetan resistance in a nonviolent capacity. The CIA selected twenty junior Tibetans to study at Cornell University from 1964 to 1967, believing it should make "educational investments in the future" to develop the human infrastructure necessary for the resistance to establish a governing body. [46] Graduates went on to serve within the Tibetan government-in-exile, as well as the Tibetan language section of All-India radio and the *Tibet Freedom* magazine. This program ceased in 1967 due to restrictions that prohibited the CIA from funding political programs in the United States.[47]

The CIA also supported the establishment of "Tibet Houses" in Geneva, New York City, and New Delhi. Their purpose was to unofficially represent the Dalai Lama and "to maintain the concept of a separate Tibetan political identity."[48] The Tibet House in New York City worked closely with Tibetan supporters in the United Nations to lobby for their cause and served as a coordinating point for resettling 500 Tibetan refugees throughout Europe.[49] The Tibet House in New Delhi, considered one of the more enduring tangible contributions to the Tibetans, remains a major attraction for scholars and tourists today.[50]

Relationship Termination

The United States terminated its relationship with the resistance as it could no longer effectively accomplish U.S. objectives, and the growing rapprochement with China necessitated political concessions that eschewed support to the insurgency. According to Gyalo Thondup, China conditioned the establishment of diplomatic relations with the United States on severing its connections and assistance to Tibet, including Mustang. Roger McCarthy, the CIA officer who created the Tibetan Task Force and who trained the first pilot team on Saipan, stated, "it still smarts that we pulled out in the manner we did… Granted, in many other operations, we did it even less gracefully and more abruptly."[51]

Gyalo Thondup delegated the execution of the CIA's withdrawal plan to his longtime companion Lhamo Tsering who initiated various programs to ease the Mustang guerrillas into new vocations. He devised a plan with the Combined Operations Center that resettled 500 of the Mustang force per year for three years, leaving 300 fighters to serve as a token resistance. One-hundred-twenty eventually joined the Special Frontier Force, but a number decided to carry on the resistance until they were defeated

and the Nepalese killed their leader. Lhamo started literacy programs and farming projects and developed projects in Nepal to employ former resistance members in carpet-weaving factories, hotel management, and transportation businesses, all of which succeeded, especially the carpet-weaving factory that is now one of Nepal's principle employers.[52] In the words of John Kenneth Knaus, the CIA officer in charge of the covert operation, the Tibetans became the "worthy but hapless orphans of the Cold War."[53]

Goal Accomplishment

U.S. sponsorship of the Tibetan proxy failed to achieve an independent Tibet, but ST CIRCUS achieved moderate success in accomplishing the limited objective of disrupting Chinese regional plans and also shaping the political discussion concerning Tibetan freedom that continues to this day. Guerrilla operations targeting Chinese military camps and disrupting major highway supply routes forced China to tie up one division in the area and divert traffic from western Tibet to 300 kilometers to the north. Pilot team members facilitated the Dalai Lama's escape to India, and guerrillas captured 1,600 classified Chinese documents that provided an intelligence windfall concerning Chinese internal assessments of the Great Leap forward, Chinese order of battle information, and internal political analysis discussing China's relations with Taiwan and the Soviet Union.

Blowback

Support to the Tibetan resistance did not produce classical blowback in the form of political embarrassment or turning its weapons and training on the United States. However, this proxy engagement exhibited both *adverse selection* and *agency slack*. The inability to select the optimal proxy and the failure to make it perform as intended often allowed the Tibetans to act contrary to the interests of the United States in pursuit of their own goals.

Adverse selection concerns choosing an appropriate proxy in a situation where the sponsor does not have a clear understanding of the proxy's capabilities or intent.[54] U.S. sponsorship of the Tibetan resistance suffered from selection of a group whose goals were not completely in sync with its own, and who lacked the capacity to completely fulfill its needs. The goal of the resistance was complete Tibetan independence from China, while the United States was primarily concerned with disrupting China in the greater scheme of global Communist containment.

> ## U.S. sponsorship of the Tibetan proxy failed to achieve an independent Tibet...

The CIA had to rely on specific personalities such as Gyalo Thondup and Gompo Tashi for proxy recruitment and operational management inside Tibet. While the Khampa refugees provided a convenient recruitment pool, the overwhelming Khampa composition prevented the resistance from becoming a truly national movement and relegated it to only the eastern region of Tibet where it could draw support from the local population. Furthermore, the CIA generally misunderstood the importance of regional allegiances and identities within the Tibetan community. U.S. intelligence based its analysis on British sources that focused mainly on the capital region of Lhasa, and only one of the CIA officers could speak Tibetan. Gyalo Thondup, the CIA's primary contact with the Tibetans, was from the northeastern region of Amdo and not always sympathetic to the Khampa authority systems. This adversely impacted the CIA's ability to advise the resistance, as demonstrated in the CIA veto of Tibetan suggestions to organize operations around alliances based on districts of origin, their attempt to impose merit-based, military-

style ranking on the Tibetans' social-power based system, and their efforts to organize battalions according to a place-neutral scheme which clashed with the district-based loyalties of the fighters.[55]

U.S. support to the Tibetan resistance provides a number of valuable lessons to consider for future proxy engagement.

Agency slack occurs when the proxy pursues its own ends contrary to the interests of the sponsor.[56] Lack of embedded CIA advisors on the ground caused this to manifest in three ways that significantly impacted the operation. The first concerned the pilot teams' inability to organize the resistance elements into dispersed units. Their concentration and conventional head-on engagements with the superior People's Liberation Army caused heavy casualties that quickly degraded the resistance. Despite emphasis on guerrilla warfare and creating underground resistance cells in the villages, the teams were unable to break the Khampa and Amdoan tradition of using large tribal forces of a hundred or more fighters.[57]

Second, the Mustang operation became a static base instead of the initial consolidation point to establish forward guerrilla elements for permanent operations in Tibet. Again, lack of direct supervision allowed leadership schisms to occur at Mustang that prevented execution of the original plan. Conditioning aerial resupply on resistance performance failed to achieve the requisite control. The base commander was even able to line his pockets with the money and material provided by the CIA without accountability.[58]

Finally, U.S. partnership with India as an intermediate regional proxy, and subsequent lack of direct operational engagement with the Special Frontier Force, allowed India to siphon off a substantial number of Tibetans for use in operations unrelated to the resistance. Diversion of these personnel and resources significantly degraded the CIA's ability to influence operations inside of Tibet and have a greater disruptive effect against China.

Lessons for Future Proxy Engagement

U.S. support to the Tibetan resistance provides a number of valuable lessons to consider for future proxy engagement. These apply throughout an entire generic proxy life cycle regardless of the specific temporal and political circumstances. It may be helpful to consider the process of developing and using a proxy as comparable to a value chain, the set of activities a firm performs to deliver a product or service to the market. This is a system that optimizes inputs, transformation processes, and outputs to eliminate waste and maximize performance.[59] Value is added to the product at each step in the chain. In proxy warfare, "value added" occurs by optimizing proxy capabilities and establishing mechanisms that both ensure proper selection and mitigate deviation from sponsor goals. A sponsor accomplishes this through the steps of recruitment, vetting, force generation, employment, and demobilization/integration.

Recruitment

The nature of the recruitment pool impacts proxy effectiveness. Recruiting from a restricted candidate pool may prohibit a mass-based, inclusive resistance movement, but it could increase effectiveness and sponsor control. Expanding the recruitment base may create a more inclusive movement, but it may create messy peripheral effects requiring the sponsor to balance the multiple competing interests of proxy diversification.

The CIA failed to develop an inclusive, broad-based movement in Tibet—it recruited

from refugee camps in India and relied on two key Tibetan individuals for selection. This provided a narrow situational perspective and favored one ethnic group that prevented formation of a national resistance movement. However, it afforded significant control over the proxy elements created for limited objectives such as intelligence collection and subversion.

Vetting

The amount of vetting required is proportional to the degree of ideological overlap between the sponsor and proxy. Corollary: reliance on individual proxy personalities for "mass vetting" may create significant control problems for a sponsor. Concern over the potential for a proxy to commit human rights abuses, associate itself with designated terrorist or criminal groups, or conduct insider attacks necessitates increased vetting for democratic sponsors. Using pre-vetted proxy leaders to mass vet individuals under their command may accelerate the force generation process, but it reduces the sponsor's ability to screen out undesirable candidates and may adversely affect choosing the right proxy and controlling its actions.

Ideological alignment and close personal relationships with two key Tibetan resistance figures eliminated the need for the CIA to conduct significant vetting. Alignment persisted throughout much of the proxy engagement, but leadership schisms at the Mustang base prevented the effective employment of guerrilla elements against the Chinese after one of the CIA's key partners passed away.

Force Generation

The relationship between the type of proxy force and the scope of the sponsor's objectives must be realistically assessed at the beginning of the engagement and consistently re-evaluated. A sponsor's need for its proxy to accomplish maximalist objectives during the early stages of engagement may clash with both its willingness to devote the material and political capital required to secure those objectives, and the actual capabilities of the proxy force. Neglecting to align these elements at any point during the proxy engagement may reduce effectiveness and ultimately result in failure.

The CIA created and supported scalable proxy forces based on different objectives. Small "pilot teams" were successfully used to assess the capabilities of the existing resistance movements inside Tibet, collect intelligence, conduct sabotage, and later serve as force multiplication elements by advising the Tibetan guerrilla units in place of actual CIA officers on the ground. The CIA later supported the mass organization of traditional guerrilla elements by reconsolidating fighters dispersed and degraded by Chinese military operations. This proved ineffective as the Tibetans were unwilling to maneuver on Chinese forces, forcing the United States to terminate the relationship.

> **...the Tibetans were unwilling to maneuver on Chinese forces, forcing the United States to terminate the relationship.**

Employment

Lack of embedded advisors reduces control over the proxy. A sponsor's direct advisory presence on the ground signals commitment to the proxy engagement and affords increased opportunity to affect favorable outcomes, but it increases the risk of sponsor exposure.

Reduced control resulted in losses of effectiveness against China. Inability to influence tactical engagements ultimately degraded resistance operations. The Tibetans failed to disperse against the People's Liberation Army and instead opted to fight in conventional, head-on engagements that resulted in heavy casualties. Operationally, guerrilla leadership

decided to remain in static bases in Nepal instead of establishing forward elements for permanent operations in Tibet. The United States was unable to apply sufficient leverage via resource provision/denial to force the resistance to comply with its directives.

Using intermediaries reduces sponsor control. A sponsor's attempt to further distance itself from the conflict and/or spread cost burdens by working through intermediaries will reduce its control over the proxy in proportion to the divergence between their operational objectives. Intermediate proxies often have different goals than the primary sponsor. This imposes significant constraints on a sponsor's ability to optimize proxy effectiveness.

> **Tibet illustrated an orderly withdrawal of sponsor support as the United States both demobilized and reintegrated its proxy forces.**

CIA partnership with India's Intelligence Bureau resulted in over 12,000 Tibetans siphoned off from the resistance for service in India's Special Frontier Force. The CIA was unable to use them in Tibet against the People's Liberation Army, and India employed them in an operation against Pakistan to facilitate Bangladesh's independence.

Sponsor control based on resource provision is proportional to the value a proxy places on material support. Making resources contingent on battlefield effectiveness, equipment accountability, and human rights compliance is not a reliable mechanism to ensure proxy obedience if other cost/benefit calculations dominate the proxy's decision-making process.

The CIA attempted to use supply as a control measure by manipulating air drops to the guerrillas. Air drops were conditioned on the guerrillas moving off of their bases into forward positions, but the Tibetans refused to depart unless they received the supplies first. This failed to achieve the intended effect and ultimately led to the guerrillas remaining in static positions until the CIA terminated the relationship.

Demobilization/Integration

The degree of planning for proxy demobilization/integration influences the post-conflict outcome. A proxy may be integrated into the post-conflict political order to establish enduring influence and leverage (as Iran did with Hezbollah in Lebanon and Syria), or demobilized to prevent potential blowback.[60] This must be a deliberate consideration and not an afterthought.

Tibet illustrated an orderly withdrawal of sponsor support as the United States both demobilized and reintegrated its proxy forces. The CIA, in conjunction with trusted Tibetan officials, executed a deliberate plan that resettled 500 guerrillas into civilian life per year for three years. A small number of guerrillas continued the resistance and were ultimately defeated, and some joined other security forces such as India's Special Frontier Force. The plan incorporated literacy programs and farming projects, and developed ventures in Nepal to employ former resistance members in carpet-weaving factories, hotel management, and transportation businesses

External political considerations directly impact both the strategic and tactical aspects of proxy employment. Divorcing the larger political and strategic considerations that prompted the initial proxy engagement from actual proxy employment on the ground may significantly reduce its effectiveness. Proxy warfare requires an integrated policy approach.

U.S. ideological commitment to containing Communism and the resistance's practical utility as a disruptive mechanism kept U.S. interest in Tibet relatively static until President Nixon's rapprochement with China in 1972. In light of this political shift, support to the Tibetan resistance undermined efforts to establish China

as a counterbalance to the Soviet threat and was subsequently phased out completely in 1974. In addition, domestic U.S. political constraints significantly decreased the resistance's operational effectiveness. Overflights were prohibited after the downing of a U-2 spy plane in Soviet airspace in 1960. Coupled with the potential for political fallout inherent in covert operations during the 1960 presidential elections, the CIA suspended resupply to the guerrillas for almost a year.

Conclusion

Proxy warfare in Tibet, despite significant indigenous personnel losses and failure to achieve the resistance's maximalist objective of an independent Tibet, accomplished the United States' limited objective of disrupting the Chinese occupation as part of the global effort to limit Communist expansion during the Cold War. This case provides one overarching lesson for future proxy employment by the United States: a sponsor may achieve *limited objectives* with only a small investment in a proxy force. However, a *democratic* sponsor must be willing to shoulder any resultant political fallout and explain the perception of "failure" to its constituency when the demand for maximalist objectives such as defeating or overthrowing an adversary is not satisfied by minimal resource expenditure.

By nature, strategic irregular warfare options employed *overtly* by a democratic sponsor in an era of increasing transparency can only be as effective as the political capital invested in their preparation and execution.[61] Avoiding integrated policy approaches in an effort to achieve quick fixes to national security dilemmas may result in embarrassment and diminished global influence. Proxy warfare should remain a tool in the U.S. national security arsenal, but it must not serve as a substitute for a comprehensive foreign policy approach. These lessons from U.S. support to the Tibetan resistance should inform future U.S. policy considerations when outsourcing national security objectives to proxies as part of an indirect approach to compete below the level of armed conflict or avoid prohibitive military intervention. *IAJ*

NOTES

1   Andrew Mumford, *Proxy Warfare* (Cambridge: Polity Press, 2013), 100.

2   Irregular warfare is a key element of great power competition, and adversaries are exploiting unconventional methodologies such as the use of proxies to advance their interests without crossing the threshold to traditional armed conflict. The United States possesses similar capabilities through its special operations forces (SOF) and intelligence services to shape adversary behavior, both through behavior reinforcement—*unconventional deterrence*, and behavior modification—*unconventional compellence.* See Keith Pritchard, Roy Kempf, and Steve Ferenzi, "How to Win an Asymmetric War in the Era of Special Forces," *The National Interest,* October 12, 2019, https://nationalinterest.org/feature/how-win-asymmetric-war-era-special-forces-87601; U.S. Army Special Operations Command, "Army Special Operations Forces Strategy," https://www.soc.mil/AssortedPages/ARSOF_Strategy.pdf; Claire Graja, "SOF and the Future of Global Competition," *CNA* (May 2019), https://www.cna.org/CNA_files/PDF/DCP-2019-U-020033-Final.pdf.

3   For how this case study applies to ongoing U.S. support to various Syrian resistance forces against the Islamic State, see: Steve Ferenzi, "Want to Build a Better Proxy in Syria? Lessons from Tibet," *War on the Rocks,* August 17, 2016, https://warontherocks.com/2016/08/want-to-build-a-better-proxy-in-syria-lessons-from-tibet.

4   These are components of Principal-Agent Theory known as "adverse selection" and "agency slack." David A. Patten, "Taking advantage of insurgencies: effective policies of state-sponsorship," *Small Wars & Insurgencies* 24, no. 5 (2013): 880.

5   "Memorandum for the 303 Committee, 26 January 1968," *Foreign Relations of the United States, 1964–1968,* Volume XXX, China, Document 342 (Washington, DC: US Government Printing Office, 1998), 739, https://history.state.gov/historicaldocuments/frus1964-68v30/d342.

6   Peter Hopkirk, *Trespassers on the Roof of the World: The Secret Exploration of Tibet* (New York: Kodansha America, Inc., 1995), 5.

7   Kenneth Conboy and James Morrison, *The CIA's Secret War in Tibet* (Lawrence: University Press of Kansas, 2002), 2, 9.

8   Ibid., 8.

9   Carole McGranahan, "Tibet's Cold War: The CIA and the Chushi Gangdrug Resistance, 1956-1974," *Journal of Cold War Studies* 8, no. 3 (2006): 109-111.

10   John Kenneth Knaus, *Orphans of the Cold War: America and the Tibetan Struggle for Survival* (New York: PublicAffair, 1999), 136, 138.

11   Ibid., 138.

12   McGranahan, "Tibet's Cold War," 109.

13   Knaus, *Orphans of the Cold War,* 4-18.

14   Ibid., 137.

15   NSC 5429/5 stated: "We should be ready to exploit any opportunities which might occur as a result of inherent internal weaknesses of Communist China," and "Utilize all feasible overt and covert means, consistent with a policy of not being provocative of war, to create discontent and internal divisions within each of the Communist-dominated areas of the Far East." Colonel Edwin F. Black, Memorandum: "April 1 OCB (Operations Coordinating Board) Luncheon Discussion: Exploitation of Tibetan Revolt," March 31, 1959, http://www.chushigangdruk.ca/History%20docs/White%20house%20documents%20on-tibetan-revolt-various-1959.pdf.

16   "Memorandum for the 303 Committee," 739.

17   Mikel Dunham, *Buddha's Warriors: The Story of the CIA-Backed Tibetan Freedom Fighters, the Chinese Invasion, and the Ultimate Fall of Tibet* (New York: Penguin Group, 2004), 382.

18   Conboy and Morrison, *The CIA's Secret War in Tibet*, 27, 32, 34.

19   Knaus, *Orphans of the Cold War,* 169.

20   For more on deeper U.S.-Indian relations, India's "Forward Policy" of challenging China's territorial claims, and the influence of the Sino-Indian War on JFK's administration, see Bruce Riedel, *JFK's Forgotten Crisis: Tibet, the CIA, and the Sino-Indian War* (Washington, DC: The Brookings Institution, 2015).

21   Knaus, *Orphans of the Cold War,* 266.

22   Ibid., 276.

23   Conboy and Morrison, *The CIA's Secret War in Tibet*, 228-229.

24   Knaus, *Orphans of the Cold War,* 126.

25   Mao's Cultural Revolution sought to obliterate the "Four Olds:" Old Ideas, Old Culture, Old Traditions, and Old Customs. In addition to banning all aspects of Tibetan culture, by the end of the Cultural Revolution, only fifteen of the original 6,000 plus Tibetan monasteries remained. Tens of thousands of Tibetans were imprisoned on political grounds, and 1.2 million Tibetans died at the hands of the Chinese. Dunham, *Buddha's Warriors*, 371-372.

26   Knaus, *Orphans of the Cold War,* 312-313.

27   "Letter from Andruk Gompo Tashi to President Eisenhower, December 1959," 9. http://www.chushigangdruk.ca/History%20docs/Letter%20from%20Andruk%20Gompo%20Tashi%20to%20President%20Eisenhower,%20December%201959.pdf.

28   Knaus, *Orphans of the Cold War,* 294, 310.

29   Ibid., 55-74.

30   Ibid., 84-139.

31   Knaus, *Orphans of the Cold War,* 233.

32   Ibid., 281.

33   CPI Inflation Calculator, https://data.bls.gov/cgi-bin/cpicalc.pl?cost1=585%2C000&year1=196401&year2=201908.

34   "Memorandum for the Special Group, 9 January 1964," *Foreign Relations of the United States, 1964–1968,* Volume XXX, China, Document 337 (Washington, DC: US Government Printing Office, 1998), 732. https://history.state.gov/historicaldocuments/frus1964-68v30/d337.

35   Knaus, *Orphans of the Cold War,* 142.

36   Conboy and Morrison, *The CIA's Secret War in Tibet*, 72, 78.

37   Knaus, *Orphans of the Cold War,* 238-239.

38   Ibid., 241-249.

39   Dunham, *Buddha's Warriors*, 353.

40   Ibid., 292-294.

41   "Memorandum for the Special Group," 732.

42   Knaus, *Orphans of the Cold War,* 296-300.

43   Ibid., 272.

44   Ibid., 276.

45   Conboy and Morrison, *The CIA's Secret War in Tibet*, 242-246, 258.

46   "Memorandum for the 303 Committee, 26 January 1968," 741.

47   The Tibetan students participated in a year-long academic program combining anthropology, world history, politics, governmental organization, and English composition. Knaus, *Orphans of the Cold War*, 284-285.

48   "Memorandum for the Special Group, 9 January 1964," 732.

49   "Memorandum for the 303 Committee, 26 January 1968," 741.

50   Knaus, *Orphans of the Cold War*, 287.

51   Dunham, *Buddha's Warriors*, 382-383.

52   Knaus, *Orphans of the Cold War*, 298-302.

53   Ibid., 324.

54   Patten, "Taking advantage of insurgencies: effective policies of state-sponsorship," 880.

55   McGranahan, "Tibet's Cold War," 114-115.

56   Patten, "Taking advantage of insurgencies: effective policies of state-sponsorship," 880.

57   Dunham, *Buddha's Warriors*, 218, 242.

58   Ibid., 374-375.

59   Michael E. Porter, *Competitive Advantage* (New York: The Free Press, 1985), 11-15.

60   Steve Ferenzi, "Beyond Half-Measures: Influencing Syria's Political Order through Non-State Proxies," *Small Wars Journal*, May 23, 2016, http://smallwarsjournal.com/jrnl/art/beyond-half-measures-influencing-syria%E2%80%99s-political-order-through-non-state-proxies.

61   Steve Ferenzi, "Imposing Costs by Other Means: Strategic Irregular Warfare Options to Counter Russian Aggression," Small Wars Journal, May 18, 2016, http://smallwarsjournal.com/jrnl/art/imposing-costs-by-other-means-strategic-irregular-warfare-options-to-counter-russian-aggres.

Countering

Russian Hybrid Warfare

by Nicholas J. Stafford

Russia's recent operations in Crimea, Eastern Ukraine, and Georgia have disrupted a generation of relative peace and stability between Moscow and its Western neighbors. This, and China's growing challenge to U.S. interests, has caused a dramatic re-appraisal of priorities in the U.S. where "great power competition, not terrorism, is now the primary focus of U.S. national security."[1] In light of the return to great power competition, the U.S. Army has accelerated its efforts to incorporate the technological advancements of the Information Revolution in a new conceptual approach that will inform the development of U.S. military doctrine and capabilities—Multi Domain Operations (MDO).

The U.S. Army in Multi Domain Operations 2028 describes how U.S. ground forces, as an integral part of joint and combined forces, will compete, fight, and win in all domains—space, cyberspace, air, land, maritime—against peer adversaries between 2028 and 2040.[2] Army forces enable the Joint Force and interagency efforts to seize and maintain the initiative in competition by deterring conflict and adversaries' attempts to expand the competitive space below the threshold of armed conflict.[3] The concept envisions three main phases: competition, armed conflict, and a return to competition. Although the MDO concept accounts for both Chinese and Russian approaches, Russia is used as the pacing threat.

The MDO concept explains how great power competitors intend to fracture U.S. alliances and partnerships through a combination of diplomatic and economic actions: unconventional warfare; information warfare; exploitation of regional social, ethnic, or nationalistic tensions; and the actual or threatened employment of conventional forces. In essence, adversaries aim to expand the competitive space by generating instability and creating political separation between allies—notably the North Atlantic Treaty Organization (NATO). The desired result is strategic ambiguity which inhibits

Major Nick Stafford is a serving British Army officer currently attending the School of Advanced Military Studies (SAMS). He has operational experience in Afghanistan and Europe and has recently served as a Armor Battalion S3 and Divisional planner. This article is based on his Masters in Military Art and Science paper, which examined Russian Hybrid Warfare and the challenges it poses for the U.S. Army's Multi Domain Operations concept.

the speed and precision of friendly recognition, decision, and reaction to adversary activities.[4]

This article argues that, in the competition phase, the MDO concept neglects a key element of the operational environment, the human terrain that is a critical requirement and vulnerability of the Russian operational center of gravity. As a result of this neglect the MDO concept, in traditional "American Way of War" fashion, is focusing on deterring and fighting Large Scale Combat Operations and fails to properly consider the importance of this human terrain as a position of relative advantage.

This article recommends that the U.S. Army needs to escape from the traditional American Way of War and see its role as part of a broader, whole-of-government and comprehensive, approach.

> **...hybrid forces can only be deployed in Russian-speaking regions, where they are ethnically and culturally transparent and cannot be easily detected.**

Russian Hybrid Warfare

In the wake of Russia's annexation of Crimea and war in Georgia, many analysts, military services and intellectuals, including the former Secretary of Defense Robert Gates and former National Security Advisor Lieutenant General H.R. McMaster, used the term "hybrid warfare" to help describe the complex and evolving crisis in Ukraine. The crisis, pitting the national government against separatists, Russian ultra-nationalists, proxy fighters, and Russian Military Main Intelligence Directorate (*Glavnoye razvedyvatel'noye upravleniye* – GRU) personnel, did not fit neat Western categories of war.[5] General Barno referred to this crisis as an example of a "shadow war" which can threaten U.S. interests through "strategic

disruption" and where ambiguity is the defining characteristic.[6] In this sense, hybrid threats provide the "perfect" conundrum: the injection of so much uncertainty that NATO might collapses under its own principle of allied consensus.[7]

Despite having a similar view to the U.S. on the future of the operational environment, Russia is approaching the problem in a very different way. Russia is experimenting with unconventional means to counter hostile indirect and asymmetric attacks, but Russia also sees conventional military forces as being of the utmost importance in its hybrid strategy.[8] Despite the subtle differences, all the terms around hybrid warfare point to the same thing: Russia is using multiple instruments of power and influence to pursue its national interests outside its borders. The objectives of Russian hybrid warfare are best summarized as: 1) capturing territory without resorting to overt or conventional military force; 2) creating a pretext for overt, conventional military action; 3) using hybrid measures to influence the politics and policies of countries in the West and elsewhere.[9]

However, several conditions are necessary for Russian hybrid operations. The first condition is that hybrid forces can only be deployed in Russian-speaking regions, where they are ethnically and culturally transparent and cannot be easily detected. The second is that hybrid forces must arrive covertly, a condition that favors Russia's near-abroad. The third condition is that covert deployment presumes border controls are poor and state power is weak in the target country.[10] While the Baltic states are vulnerable to Russian covert violence, especially in the Ida-Viru County, Estonia or Daugavpils, Latvia, they will be far harder to destabilize than Ukraine as they have greater control over their territory, stronger internal security forces and, crucially, support from NATO.

A vulnerability of hybrid warfare is that it requires local escalation-dominance. War is "hybrid" in the sense it combines

aspects of insurgency-type irregular warfare and conventional force, where the threat of escalation, and use of conventional forces, deters forceful retaliation.[11] When operating close to its own borders, Russia can easily introduce additional force elements to a conflict. However, if Russia were forced to operate away from its borders, it would be significantly harder to rapidly and successfully combine the different irregular and conventional forces to achieve coherent effects. Russia has been able to exploit Western fear of direct military confrontation in Ukraine, Georgia, and Syria, but it may not be able to achieve the same effect in the Baltics where NATO's resolve is stronger.

Russian tactics, techniques, and procedures are supported by persistent, rather than plausible, denial of Russian operations, even in the face of photographic evidence and firsthand testimonials. Of interest is the use of unidentified Russian agents, usually SPETSNAZ, to organize and lead protests and paramilitary operations, as well as the use of armed civilian proxies (Night Wolves motorcycle club), self-defense militias, and Russian paramilitary "volunteers" (Cossack, Chechen, Serbian and Russian Bns) instead of, or in advance of, regular troops.[12]

The MDO concept identifies the operational center of gravity for Russian actions in the competition phase as "the close integration of information warfare, unconventional warfare, and conventional forces."[13] Interestingly, these three elements of Russian hybrid warfare closely parallel the three phases often associated with Mao Tse Tung's Concept of Revolutionary Warfare: the political phase (organization, consolidation, and preservation); the unconventional warfare phase (progressive expansion); and the conventional phase (decision, or destruction of the enemy).[14]

Like Mao, who demonstrated the ability to switch between these phases as circumstances required, Russian hybrid warfare can combine these elements, at any stage, to achieve objectives. As recent events in Eastern Ukraine demonstrate, Russian actions below the level of armed conflict share many characteristics with an insurgency.

However, the MDO concept's description of the Russian operational center of gravity fails to capture the critical requirements and vulnerabilities of Russian hybrid warfare. Critically, it omits the requirements for Russian hybrid operations to be conducted in Russian-speaking regions, where Russian forces are ethnically and culturally transparent, cannot be easily detected, and can arrive covertly.

> **Russian tactics, techniques, and procedures are supported by persistent, rather than plausible, denial of Russian operations...**

The American Way of War

A classic "American Way of War" approach to problem-solving seems to influence the MDO concept heavily. In his seminal work, *The American Way of War*, Russell Weigley established the paradigm that many scholars use to explain the American military tradition. Hans Delbrück suggested that there are two kinds of military strategy: annihilation and attrition. Weigley argues that most modern U.S. military strategies preferred wars of annihilation and closing with the enemy for a "decisive battle" over wars of attrition.[15] Colin Gray's characteristics of American warfare augment the idea that U.S. military thinkers tend to focus on large, conventional, symmetrical battles:

1. Apolitical—often lacking a clear political objective.

2. Astrategic—military objectives do not necessarily achieve political objectives.

3. Ahistorical—the U.S. is still future-orientated.

4. Problem-solving and optimistic approach.

5. Cultural ignorance continues to hamper U.S. strategic performance.

6. Technologically dependent.

7. Firepower focused.

8. Large-scale—Huntingdon, "bigness not brains is our advantage, and we should exploit it." It is not a problem; it is a condition.

9. Profoundly regular—the U.S. is better at regular warfare.

10. Impatience.

11. Logistically excellent.

12. Sensitive to casualties.[16]

These values are prevalent in the MDO concept, which focuses on building the capability to "penetrate" adversary anti-access/area denial systems in order to demonstrate a credible deterrence, and, if necessary, win a decisive war through the rapid annihilation of enemy military forces.

By contrast, Russia is focusing on achieving political objectives without fighting, and only escalating to armed conflict when they have a decisive advantage. Russia has exploited the absence of U.S. global presence to secure objectives without requiring large-scale combat. The Russian approach more closely resembles Sun Tzu's theories of war as opposed to the Clausewitzian approach favored by the U.S. military. There is a danger that the MDO concept focuses on the kind of armed conflict the U.S. military traditionally wants to fight and overlooks the myriad of problems inherent in competition. Far more likely is that other powers echo Sun Tzu and Mao and avoid the U.S.'s

strengths and instead attack its weaknesses by continuing to conduct their hybrid warfare operations below the level of armed conflict. As Mao wrote: "In guerrilla warfare, there is no such thing as a decisive battle."[17]

Given Russian preferences for achieving objectives below the threshold of armed conflict, this paper argues that the MDO concept focuses too heavily on preparing the U.S. for confronting the most dangerous scenario—armed conflict against a near-peer enemy—as opposed to the most likely scenario of continued attritional competition in the "gray zone" of conflict. While the U.S., and its allies, must be prepared to conduct Large Scale Combat Operations, they also need to be able to defend their interests in competition.

The MDO concepts description of the threats seems to be at odds with its recommendation for how to best to counter them. This article will now examine how this gap stems from the failure to the MDO concept to recognize the importance of the human terrain to Russian's hybrid warfare operations, and how the concepts may fail to contest this terrain as part of a U.S. response.

The Center Of Gravity in Competition

The MDO concept states that the military fulfills three roles in the competition phase: 1) the conduct of intelligence gathering, deception, and counter-reconnaissance; 2) the defeat of enemy information and unconventional warfare, principally through the support of partners; and 3) the maintenance of credible deterrence.[18]

The MDO concept self-defines the role of the military in competition. In doing so, the concept assumes that partners and agencies will deal with Russian and Chinese exploitation of social, ethnic, or nationalist tensions. The concept places competition in these areas on the periphery of military responsibility, resulting in an unbalanced focus on solving conventional military problems in the future operating environment. This bias toward conventional
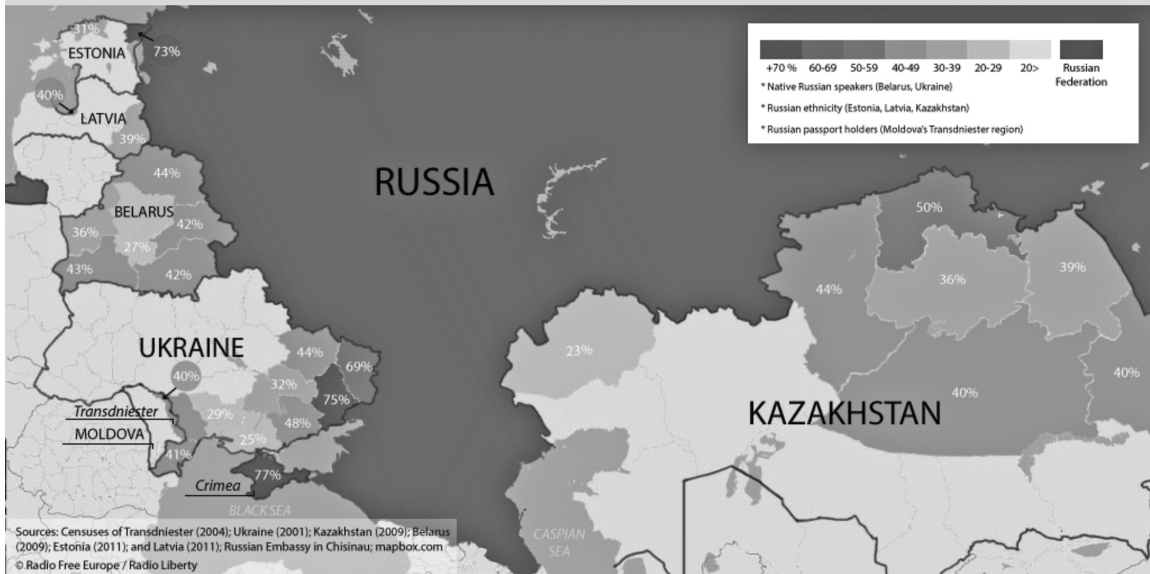
Figure 1. Ties to Russia
Source: Radio Free Europe / Radio Liberty. Copyright Radio Free Europe / Radio Liberty.
Re-printed with permission of Radio Free Europe / Radio Liberty, Prague, Czech Republic

warfare may inadvertently expose a gap in the responsibilities and capabilities between the roles of the U.S. military and those of other U.S. agencies.

The U.S. military is arguably as uncomfortable and unwilling to get involved with political activities before conflict as they are after conflict (Dr. Nadia Schadlow outlines the possible causes of the U.S. military's post-conflict hesitation in her "American Denial Syndrome" theory).[19] Often, this results in military organizations not considering the political aspects of an enemy's center of gravity. Despite considerable successes during large-scale combat, Antulio Echevarria II observes that "the new American way of war appears to have misidentified the center of gravity in [Operation IRAQI FREEDOM and Operation ENDURING FREEDOM], placing more emphasis on destroying enemy forces than securing population centers and critical infrastructure and

maintaining order."[20] This sentiment emphasizes the need to develop those capabilities required during competition as well as those needed in armed conflict. To appropriately understand competition requirements, the U.S. military must critically analyze the competitive environment.

Identifying a center of gravity during competition allows the U.S. to focus its efforts against that center. However, as Celestino Perez argues in *Addressing the Fog of the COG*, defining a center of gravity can be difficult.[21] This paper argues that the MDO concept characterization of the Russian operational center of gravity overlooks the critical requirement of Russian-speaking (or ethnic Russian populations) within the target country.

In regions where Russia conducts "gray zone" strategies, such as Ukraine and the Baltics, one of the critical requirements of Russian power is the target nation's Russian-speaking population. These populations, whom

the Russians have historically vowed to protect and advance, constitute "vital ground" that offers "positions of relative advantage" to the competitors in the human terrain. Russia cannot effectively execute its hybrid warfare approach without support from Russian-speaking populations in states close to its borders. The Russian-speaking populations are also, therefore, a critical vulnerability of the Russian operational center of gravity.

> **In many ways, the Russian threat below the threshold of armed conflict resembles a state-directed or state-sponsored insurgency...**

Russian forces operate where they are ethnically and culturally transparent and cannot be easily detected. This provides Russia with a significant advantage in the conduct of unconventional warfare. For example, Russian-speaking populations within the Baltic states represent the most fertile recruiting demographic for separatist movements and covert violent action.[22] Russia uses information to enable this political fragmentation. Most of the Russian-speaking populations in Estonia and Latvia get their views on history and current events from Russian television channels that are directly subordinate to the Kremlin and used as a mechanism of propaganda. As a result, Russian-speakers, exist in a "separate information space"[23] that remains unchallenged by the U.S. and its NATO allies.

In order to succeed in the competition phase, NATO and the U.S. must compete to win the support of these key demographics. Success in competition then, if viewed in business terms, is providing the best value proposition. The MDO concept must take steps to expand the competitive space and provide a greater value proposition to target populations than Russia. By avoiding focusing on competition in this light,

the MDO concept risks ceding these "positions of advantage" to Russia and failing to deny enemy actors key points of leverage. Not only could this prove unhelpful for the pursuit of U.S. interests in the competition phase, but it may also result in the U.S. entering an avoidable conventional conflict.

In contrast, securing the key human terrain in competition can deny Russia, or any adversarial force or ideology for that matter, access to those vital demographics. This denial reduces a competitor's options for achieving objectives below the threshold of armed conflict. Therefore, winning over the local populations through unified action with partner nations and agencies is the most effective way to achieve one of the MDO aims in competition: "seize and sustain the initiative in competition by deterring conflict on terms favorable to the U.S. and defeating an adversary's efforts to expand the competitive space below the threshold of conflict."[24]

In many ways, the Russian threat below the threshold of armed conflict resembles a state-directed or state-sponsored insurgency, meaning that the U.S. and its allies should conduct stability operations during the competition phase, lest it surrenders the initiative and influence to Russia. To address this need, the U.S. Army should add a fourth task to the MDO concept to frame what the Joint Force seeks to achieve during the competition phase: "conduct stability operations to win the support of key local populations." By doing so, the Joint Force can deny adversaries freedom of action and counter adversaries' efforts to expand the competitive space below the threshold of armed conflict. Stability operations enable the U.S. to promote its interests and access through presence and engagement, carefully tailored to the unique demographic realities in each state. Conducting stability operations, therefore, represents a logical approach in situations where the U.S. needs to rebalance power, expand the competitive space, and reduce the influence of competitors.

The U.S. and its allies already have many of the tools to compete for influence amongst local populations, having spent two decades engaged in counter-insurgency campaigns. Several approaches synonymous with effective counter-insurgency strategies are very relevant to countering adversaries' ability to compete in the current or future operating environments: separating the insurgency from their support base (the local population and external state), winning the local populations "hearts and minds," and assembling an effective intelligence apparatus to identify the grievances and requirements of the local populace and insurgent forces.

In basic terms, these all contribute to making needs-based assessments and emplacing the correct structures to compete and win. The U.S. Army needs to see its role in competition as part of a broader whole government approach and comprehensive approach. The long-term goal should be for the key demographic to support the host nation government while remaining actively hostile, or at least ambivalent, to the encroaching power.

Conclusions

The MDO concept seeks to solve five problems posed by China and Russia in competition and conflict. The first, and perhaps most fundamental problem extends from the question, "How does the Joint Force compete to enable the defeat of an adversary's operations to destabilize the region, deter the escalation of violence, and, should violence escalate, enable a rapid transition to armed conflict?"[25] This article proposes that the MDO concept must adopt a broader vision for competition, which looks beyond the traditional American Way of War and develops other "ways" of achieving U.S. strategic goals. Success in this realm, while requiring time and effort, offers an opportunity to enhance American interests and global order without the vast expense of blood and treasure that Large Scale Combat Operations against a peer competitor might entail. Local populations represent vital human terrain that must be secured to win in competition and to assure success in war, particularly in an operating environment characterized by dense urban terrain and democratized technology.

The author believes that part of the solution to this problem is making local populations a focus of a whole-of-government approach as well as Joint Force activity in multi domain competition. Identifying key populations, working with agencies and partners, and adapting existing U.S. stability doctrine to secure those demographics can enable success in competition. ***IAJ***

Notes

1   Secretary James N. Mattis, "Remarks by Secretary Mattis on the National Defense Strategy," (Department of Defense, 19 January 2018). Accessed 14 November 2018. https://dod.defense.gov/News/Transcripts/Transcript-View/Article/1420042/remarks-by-secretary-mattis-on-the-national-defense-strategy.

2   Training and Doctrine Command (TRADOC), Untied States Army, TRADOC Pamphlet 525-3-1, *The U.S. Army in Multi Domain Operations* (Fort Eustis, VA: TRADOC, 6 December, 2018), 1.

3   Ibid, viii.

4   Ibid, 7.

5   Frank Hoffman. "Not-so-new warfare: Political Warfare vs Hybrid Threats." *War on the Rocks*, (28 July 2014). Accessed 19 July 2018. https://warontherocks.com/2014/07/on-not-so-new-warfare-political-warfare-vs-hybrid-threats/.

6   General (Retd) David Barno and Nora Bensahel. "Fighting and Winning in the 'Grey Zone." *War on the Rocks*, (19 May 2015). Accessed 4 November 2018. https://warontherocks.com/2015/05/fighting-and-winning-in-the-gray-zone/.

7   Nadia Schadlow. "The Problem with Hybrid Warfare." *War on the Rocks*, (2 April 2015). Accessed 21 July 2018. https://warontherocks.com/2015/04/the-problem-with-hybrid-warfare/.

8   Charles K. Bartles. "Getting Gerasimov Right." *Military Review*, (January- February 2016): 36.

9   Christopher S. Chivvis. *Understanding Russian 'Hybrid Warfare': And what can be done about it*. Testimony presented before the House Armed Services Committee (Santa Monica, CA: RAND Corporation, 22 March 2017), 1.

10   Anton Shekhovtsov. "Who is afraid of the 'little green men'"? *The Intersection Project: Russia/Europe/World*, (21 September 2015). Accessed 4 November 2018. http://intersectionproject.eu/article/security/who-afraid-little-green-men.

11   Alexander Lanoszka. "Russian hybrid warfare and extended deterrence in eastern Europe." *International Affairs* 92, no. 1, (2016): 189.

12   United States Army Special Operations Command (U.S. SOCOM). *Little Green Men': A primer on Modern Russian Unconventional Warfare – Ukraine 2013-2014* (Fort Bragg, NC: U.S. SOCOM, 6 August 2016), 3.

13   TRADOC, Pamphlet 525-3-1, 11.

14   Samuel B. Griffith, "Introduction", in *Fleet Marine Force Reference Publication 12-18: Mao Tse-tung On Guerrilla Warfare* (Washington D.C: Headquarters United States Marine Corps, 5 April 1989), 20-21.

15   Russell F. Weigley, *The American Way of War* (Bloomington, University of Indiana, IN, 1973), 18-39, 124-163.

16   Colin S. Colin, "The American Way of War," in *Rethinking the Principles of War* by Anthony McIvor, (Annapolis, MD: Naval Institute Press, 2005), 13-40.

17   Griffiths, *Mao Tse-tung On Guerrilla Warfare*, 52.

18   TRADOC, Pamphlet 525-3-1, 27-31.

19   Nadia Schadlow, "American Denial Syndrome," In *War and the Art of Governance: Consolidating Combat Success into Political Victory* (Washington, D.C: Georgetown University Press, 2017).

20   Antulio J. Echevarria II, *Toward an American Way of War* (Carlisle, PA: Strategic Studies Institute, March, 2004), 13.

21   Celestino, Perez, *Addressing the Fog of COG: Perspectives on the Center of Gravity in US Military Doctrine* (Fort Leavenworth, Kansas: Combat Studies Institute Press, 2012).

22   Andrew Radin, *Hybrid Warfare in the Baltics – Threats and Potential Responses* (Santa Monica, CA: RAND Corporation, 19 October 2015), 24.

23   Mike Winnerstig, *Tools of Destabilization: Russian Soft Power and Non-Military Influence in the Baltic States* (Stockholm, Sweden: *FOI Swedish* Defense Research Agency, December, 2014), 53.

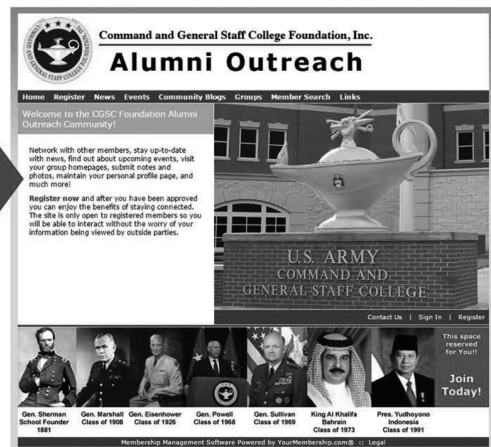24   TRADOC, Pamphlet 525-3-1, viii.

25   TRADOC, Pamphlet 525-3-1, 16.

Celebrating
15 Years of Service

It is with great excitement that we kick off our 15th year of service to the U.S. Army Command and General Staff College, its students, alumni and their families. Fifteen years of doing good things for good people.

2020 will be an impressive year. We have some exciting new programs for our alumni beginning this year, including a competitive scholarship program for children and grandchildren of CGSC Foundation Alumni Association Life Members. For our National Security Round Table Alumni we will offer a National Security Forum, which will allow for the discussion of current issues and challenges and continued involvement with the College.

Join us for anniversary celebrations and events throughout the year, and as we continue to enhance scholarship, reward excellence, improve the quality of life, and connect CGSC and America's Army with the general public.

Our History

2005 December 22, 2005 – CGSC Foundation established.

2006 Issue #1 of the *Foundation News* goes to print.

2007 Foundation hosts first National Security Roundtable program at the College Nov. 27-28, 2007.

2008 First Distinguished Leadership Award presented to Gen. Colin L. Powell April 28, 2008. Powell also delivers first lecture in the Powell Lecture Series earlier that day.

First DACOR (Diplomatic and Consular Officers Retired) Distinguished Visiting Professor of Diplomacy presentation to the CGSC class conducted by Ambassador (Ret.) Ronald Neumann on March 8, 2008.

2009 Perot Foundation provides $6.1 million to stand up two programs – the Simons Center and the Gen. Hugh Shelton Chair in Ethics.

Inaugural Fort Leavenworth Ethics Symposium conducted Nov. 16-18, 2009. – Gen. (Ret.) Jack Keane, former Vice Chief of Staff of the Army, and Foundation President Hyrum W. Smith were key speakers.

2010 Grand opening of the Simons Center for Interagency Cooperation on April 21, 2010. Ross Perot performed the ribbon cutting.

President signs 5-Star General Commemorative Coin Act into law to honor CGSC.

First issue of the *InterAgency Journal* published in October 2010.

2014 Foundation conducts inaugural "Celebration of International Friendship" Aug. 22, 2014, at the Kauffman Center for the Performing Arts in downtown Kansas City.

First lecture in the "General of the Armies John J. Pershing Great War Centennial Series" presented Sept. 30, 2014 by Dr. Shawn Faulkner and Dr. Scott Stephenson from CGSC's Department of Military History.

2015 Army University established to coordinate education and training across the institutional Army. – CGSC is part of ArmyU.

2016 First lecture in the "Vietnam War Commemoration Lecture Series" presented March 23, 2016 by Dr. Jim Willbanks, director of CGSC's Department of Military History.

Inaugural lecture in the "Interagency Brown-Bag Lecture Series" presented Sept. 13, 2016 by Ambassador (Ret.) David Lambertson and Lt. Gen. (Ret.) Richard Keller.

2017 Foundation hosts first "Art of War" exhibit in Lenexa, Kansas. This exhibit marks the first time in history that items in the CGSC art and gift collection are curated and displayed for the general public.

2018 Foundation cohosts first "Leaders of Tomorrow Symposium" with Kansas State University to share leader development best practices between the military and the private sector.

2019 Foundation begins new capital campaign efforts to support programs and activities.

2020 Foundation celebrates 15 years of support to CGSC and military families.

New programs launched.

CGSC FOUNDATION – DOING GOOD THINGS FOR GOOD PEOPLE

Contributed
$9 million
in programs to the College, military families, and Fort Leavenworth

Contributed more than
125,000 hours
of labor to programs in support of the College

The Foundation supports **75% of CGSC graduation awards** and **100% of SAMS graduation awards**

The *Foundation News* magazine and the **Foundation's website** have won national awards

Supported more than **24 CGSC International Hall of Fame Ceremonies** recognizing and rewarding more than **55 international officers** inducted into the IHOF

NATIONAL SECURITY ROUNDTABLE

U.S. ARMY COMMAND AND GENERAL STAFF COLLEGE
FORT LEAVENWORTH, KANSAS
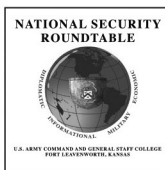
Conducted **22 National Security Roundtable Programs** educating and informing more than **300 civilian business and community leaders** from around the country about the College and their Army

Hosted five annual **Celebrations of International Friendship** bringing **national public attention to the international military student program at CGSC**

Celebration of International Friendship

Co-sponsored 10 annual **Fort Leavenworth Ethics Symposia** to enhance the professional military education on contemporary ethical and legal issues faced by military leaders

Fort Leavenworth Ethics Symposium
An intellectual forum co-sponsored by the U.S. Army Command and General Staff College and the CGSC Foundation, Inc.

The Foundation established the **Distinguished Leadership Award** in 2008 as a national level award that provides a prestigious and visible means of recognizing and honoring citizens, military and civilian, who distinguish themselves through outstanding achievement and leadership.

Created commemorative coin legislation signed into law by the President Oct. 8, 2010 as the **5-Star General Commemorative Coin Act**.

The U.S. Mint made $5 gold coins recognizing Douglas MacArthur; $1 silver coins recognizing George C. Marshall and Dwight D. Eisenhower; and the half-dollar clad, recognizing Henry Arnold and Omar N. Bradley – all graduates of CGSC.

Overall sales generated approximately **$2 million** for the Foundation's operational reserves in support of programs.

CGSC Foundation Press

The Foundation has six different routine publications published via the CGSC Foundation Press. In addition, the Foundation has published other special works, including books.

- **25 editions** of the *Foundation News* magazine
- **31 issues** of the *InterAgency Journal*
- **14** *InterAgency Essays*

- **18** *InterAgency Papers*
- **5** *Special Reports*
- **9 books** published or commissioned

• More than **2,100 articles published online** about Foundation and College events and activities

• More than **120 manuscripts** in Simons Center publications were **penned by CGSC students, graduates and faculty**

• More than **1,200 bibliography entries** in the Simons Center **online interagency bibliography**

Worth Noting

Simons Center plans for the future with CGSC faculty

Interagency faculty members from the U.S. Army Command and General Staff College met with CGSC Foundation leadership at the Simons Center for Interagency Cooperation on February 18. Attendees included Stephanie Chetraru, USAID; Ralph Erwin, National Geospatial-Intelligence Agency; Monique Guerrero, CGSC Interagency Fellowship Program; Roderic Jackson, Defense Intelligence Agency; and Kevin Rousseau, Central Intelligence Agency.

At the luncheon, the group discussed opportunities for further collaboration and new initiatives planned by the Simons Center. These initiatives, which include a new fellowship program, will be announced throughout the year as the Simons Center celebrates its 10th anniversary.

The largest and most extensive of the CGSC Foundation's programs, the Simons Center is committed to the development of interagency leaders and an interagency body of knowledge. Over the past 10 years, the Simons Center has produced several publication and lecture series, including the *InterAgency Journal* and InterAgency Brown-Bag Lecture Series.

- Simons Center

Senior NGA officer speaks at January brown-bag lecture

Mr. Ralph Erwin, Senior Geospatial Intelligence Officer, spoke on the roles and missions of the National Geospatial Intelligence Agency (NGA) on Jan. 28, 2020, in the Arnold Conference Room in the Lewis and Clark Center on Fort Leavenworth. His presentation was the sixth presentation of the InterAgency Brown-Bag Lecture Series for CGSC academic year 2020.

Erwin briefed those gathered on NGA's various responsibilities, from collaborating with the 15 other agencies that make up the U.S. intelligence community, to providing geospatial intelligence for national security, to deciding the "correct" spelling of foreign geographic locations when used by the U.S. government.

Erwin is the Senior Geospatial Intelligence Officer assigned by the Army NGA Support Team to be the NGA Liaison to the U.S. Army Training and Doctrine Command and the Combined Arms Center at Fort Leavenworth, Kansas. He is a Director of National Intelligence designated Intelligence Community Officer and served as a Senior Mentor to the Afghan Geodesy and Cartography Head Office in 2011.

The InterAgency Brown-Bag Lecture Series is co-hosted by the CGSC Foundation's Simons Center with the U.S. Army Command and General Staff School (CGSS). The series is an extracurricular, interagency topic-focused series that is intended to help enrich the CGSS curriculum. The presentations are scheduled each month. The CGSC Foundation and the Simons Center have received support for all brown-bag lectures in academic year 2020 from First Command in Leavenworth, Kansas.

- Simons Center

10 years ago: U.S. relief to Haiti following the 2010 earthquake

Ten years ago this January, a catastrophic magnitude 7.0 earthquake struck the country of Haiti, affecting an estimated three million people and taking over 200,000 lives. Originally aired in June 2018, Retired Ambassador Deborah McCarthy interviews Ambassador Ken Merten and Lieutenant General Ken Keen about the general devastation, the loss of team members, and the massive U.S. disaster relief effort to Haiti following the earthquake.

The interview is part of Ambassador McCarthy's podcast series "The General and the Ambassador: A Conversation." The podcast, produced by the American Academy of Diplomacy, promotes interagency cooperation and can be found at http://generalambassadorpodcast.org.

McCarthy was the 2018 DACOR Visiting Professor of Diplomacy for the U.S. Army Command and General Staff College (CGSC). The DACOR Visiting Professor of Diplomacy Program is conducted in partnership with the Diplomatic and Consular Officers, Retired, Inc. (DACOR) organization located in Washington, D.C., and the U.S. Army Command and General Staff College Foundation. Several times a year retired senior officials, usually Ambassadors with extensive diplomatic experience, come to Fort Leavenworth to interact with the U.S. Army Command and General Staff College students and faculty to provide a Department of State and Chief of Mission perspective to the curriculum. During their visit they also interact with area universities and civic organizations discussing policy, regional, and political expertise, as well as speaking about careers in the Foreign Service.

- Simons Center

Interagency faculty support Sergeants Major Course

CGSC interagency faculty members traveled to Fort Bliss, Texas, Dec. 6, 2019, to teach Sergeants Major Course students at the U.S. Army Sergeants Major Academy (USASMA).

The CGSC Interagency faculty representatives met individually with separate classrooms to discuss their respective organizations and listen to student briefings on some of the agencies that partner with the U.S. Army. The morning's classes were followed up with an afternoon panel for all the USASMA students currently studying interagency operations. After the panel, Mr. Ramzy Noel presented each of the CGSC faculty with framed USASMA Certificates of Appreciation.

This visit by the CGSC Interagency faculty highlights some of the many exchanges and support that CGSC offers to other elements within Army University.

The U.S. Army Sergeants Major Academy was founded in July 1972, as a special preparation source for the Army's senior enlisted leaders. Throughout its more than 46-year history, the Academy has taken on additional missions in the name of Noncommissioned Officer Professional Military Education. In recent years, with more than 24 missions under its roof, a need arose to better organize the institution to manage these missions and to refocus the Academy's efforts towards the Sergeants Major Course. On June 22, 2018, the Sergeants Major Academy was aligned under Army University and the Combined Arms Center, Fort Leavenworth, Kansas, (which is also CGSC's parent organization) with additional reporting to Training and Doctrine Command, Fort Eustis, Virginia. The result of these new changes created the NCO Leadership Center of Excellence (NCOL CoE), an accredited academic institution under which the Sergeants Major Academy now falls.

NCOL CoE is responsible for developing, maintaining, teaching, and distributing five levels of Enlisted Professional Military Education – Introductory, Primary, Intermediate, Senior and

Executive. Each level best prepares the soldier to fight and win in a complex world as adaptive and agile leaders and trusted professionals of Force 2025. It is also responsible for numerous other missions and programs including the Battle Staff NCO Course, Commandants Pre-Command Course, Spouse Leadership Development Course, USASMA Fellowship program, Staff and Faculty Development, the Soldier's Guide and NCO Guide.

The NCOL CoE-developed Professional Military Education courses are part of the career-long learning continuum and are an integral part of the Select, Train, Educate, Promote program of the Army Profession and affect more than 400,000 Soldiers annually. For more information visit https://ncolcoe.armylive.dodlive.mil.

- CGSC Foundation

Ambassador Canavan conducts first visit to CGSC

The Academic Year 2020 CGSC Foundation and DACOR Visiting Professor of Diplomacy, Career Minister (Ret.) Ambassador Katherine Canavan conducted her fall term visit Dec. 2-6, 2019. Her visit included meeting in a variety of forums with more than 300 students and faculty from the Command and General Staff School, the School of Advanced Military Studies, Park University, the University of St. Mary, Kansas University, and Leavenworth High School, as well as with dozens of business and community leaders.

On Dec. 2, Canavan met with CGSC's Dean of Academics, Dr. Jim Martin. She spent much of the day with the School of Advanced Military Studies (SAMS), first with seminar groups discussing diplomatic chief of mission perspectives, country team operations, interagency operations and expectations of ambassadors. In the afternoon she participated in a SAMS Interagency Panel, discussing interagency operations along with representatives from several government agencies. She closed her first day with a dinner with CGSC senior faculty and trustees of the CGSC Foundation.

On Tuesday, Dec. 3, Ambassador Canavan visited Leavenworth High School spending time in an AP Government class talking to students about her career as an ambassador and her time in the peace corp. She also explained how ambassadors work in relation to the president. Later in the day she visited with students in a human psychology class at the University of St. Mary discussing human rights violations in the South African region.

The following morning, Ambassador Canavan visited Park University and spoke with a group of the university faculty and staff about security issues in Europe and answered current events questions about NATO and her career in the Foreign Service. Prior to speaking with the group, Canavan met with Erik Bergrud, Associate Vice President for University Engagement.

In the afternoon of Dec. 4, Canavan spent time with the CGSC Foundation board of trustees at their quarterly board meeting in downtown Kansas City.

On the final day of her visit Ambassador Canavan traveled to the University of Kansas where she met with students in an undergraduate African Studies/Geography class speaking about her time in Botswana and later presenting to students and faculty in the African and African-American Studies Department speaking about current issues in Africa and her experiences in executing U.S. policy in that region. She also delivered a luncheon presentation at KU's Intelligence Community Center for Academic Excellence (ICCAE) discussing the current operational environment in Africa, including extremism issues and also how an ambassador works with the intelligence community in country.

The purpose of the CGSC Foundation's DACOR Distinguished Visiting Professor of Diplomacy

program is two-fold — to enhance the interagency education of the U.S. Army Command and General Staff College students and faculty and to connect the American public with senior U.S. government officials. The program is part of the CGSC Foundation's Distinguished Speaker Series and is the result of a partnership with the Diplomatic and Consular Officers, Retired, Inc. (DACOR) organization located in Washington, D.C. The program is sponsored locally by the Lawrence D. Starr Center for Peace and Justice at the University of St. Mary, Park University, and the University of Kansas.

Ambassador Canavan will return to Fort Leavenworth in mid-April for her spring term visit.

- Simons Center

DIA topic of December brown-bag lecture

The fifth presentation of the InterAgency Brown-Bag Lecture Series for CGSC academic year 2020 was conducted Dec. 10, 2019, in the Arnold Conference Room in the Lewis and Clark Center on Fort Leavenworth. Mr. Roderic C. Jackson, the Defense Intelligence Chair and Defense Intelligence Agency (DIA) Representative to the Combined Arms Center and Army University, led a discussion about the Defense Intelligence Agency, which is one of our nation's least understood intelligence organizations.

CGSC Foundation President/CEO Rod Cox provided the introduction.

Jackson provided an unclassified overview briefing of the DIA, discussing its organization and mission and provided insights with his own experiences in the field to a gathering of more than 40 CGSC students and faculty, along with senior representatives from Fort Leavenworth and community members from the region.

Roderic C. Jackson has more than 30 years of experience in national security affairs with long-term interest in African security. He has served with the DIA more than 16 years as a military and civilian employee. Among his numerous assignments and deployments, Jackson has worked as a Defense Attaché and as a policy advisor to leaders at U.S. Africa Command (AFRICOM), U.S. Central Command (CENTCOM), and U.S. European Command (EUCOM).

- Simons Center

Support the Foundation by shopping on Amazon Smile

Giving to the CGSC Foundation has never been easier. If you do any online shopping with the popular retailer Amazon, you can direct Amazon to donate to the Foundation at no extra cost to you. The way Amazon gives is through its charitable arm, AmazonSmile Foundation.

AmazonSmile is operated by Amazon and has the same products, prices and shopping features. When you shop on AmazonSmile .5 percent of the purchase price is donated to the charity of your choice, including the CGSC Foundation. AmazonSmile does not charge charitable organizations to participate and does not deduct any fees from the donation amount.

Shopping on AmazonSmile is simple. Instead of opening Amazon.com go to www.smile. amazon.com and log in using the same account information for the Amazon account you already have. On your first visit to AmazonSmile you will need to select a charitable organization. Search for "CGSC Foundation" or "Command and General Staff College Foundation" to select the Foundation and start shopping!

- CGSC Foundation

KC Federal Executive Board director presents at November 2019 InterAgency Brown-Bag Lecture

Mr. Larry A. Hisle, the executive director of the Greater Kansas City Federal Executive Board (FEB), spoke about the many programs of the Greater Kansas City FEB during the InterAgency Brown-Bag Lecture conducted Nov. 26, 2019, in the Lewis and Clark Center's Arnold Conference Room.

Hisle briefly touched on the FEB's history before diving into its purpose and three mission areas: 1) emergency preparedness, security, and employee safety; 2) workforce development; and 3) strategic partnerships. Hisle also highlighted how the FEB's programs help the federal government reduce expenditures, avoiding $2,276,814 in additional costs in 2018 alone.

According to Hisle, while all FEBs have the same general mission – to serve as a catalyst for communication, coordination and collaboration among federal offices in the metropolitan area in which the FEB is located – no two FEBs are alike. "Once you've seen one FEB, you've seen one FEB," said Hisle.

For example, Hisle stated that Kansas City is "the new Ellis Island" and is a hub for immigration. Also, while the Smithsonian – keepers of America's treasured history – is affectionately known as the Nation's "attic," Kansas City is the Nation's "storage pod." Kansas City is largest keeper of federal records outside of Washington, D.C.

During his presentation, Hisle also discussed the importance of recruiting new talent to the federal government. Hisle introduced the audience to FEB's Government to University (G2U) program, which aims to engage students and young adults in public service and introduce them to the wide range of careers available in the federal government. "Government has every job under the moon… and on the moon for that matter," said Hisle.

Hisle has served as the executive director of the Greater Kansas City Federal Executive Board since 2013. Hisle holds a bachelor's degree in Business Administration from Thomas Edison State University. He has previously served as a program manager in the U.S. Office of Personnel Management. Hisle is very active in the community volunteering with youth sports teams and scouting activities as well as serving on the board of directors of the Sherwood Center for the Exceptional Child and on the advisory council of the KCK Area Technical School.

Hisle's presentation was the fourth lecture in the series for academic year 2020.

The InterAgency Brown-Bag Lecture Series is co-hosted by the CGSC Foundation's Simons Center with the U.S. Army Command and General Staff School (CGSS). The series is an extracurricular, interagency topic-focused series that is intended to help enrich the CGSS curriculum. Unless otherwise announced, the presentations are scheduled each month from 12:30-1:30 p.m. in the Arnold Conference Room of the Lewis and Clark Center on Fort Leavenworth.

All lectures in the InterAgency Brown-Bag Lecture Series are free and open to the public. As the series moniker states, the lecture series is conducted in the traditional "brown-bag lunch" format. – Attendees are welcome to bring their own lunches into the conference room. Members of the public coming to the lectures from off-post will need to add extra time to check-in at the Fort Leavenworth visitor center. – For gate information, see the Fort Leavenworth homepage – https://garrison.leavenworth.army.mil.

- Simons Center

Area 51: Very Secret, Very Cool, but not Aliens

As part of the Foundation's Distinguished Speaker Series, Brent Geary, Ph.D., historian with the Central Intelligence Agency and the Center for the Study of Intelligence, presented a lecture titled, "Very Secret, Very Cool, but not Aliens: The U-2, the A-12 and Area 51," to more than 50 attendees at Park University on Wednesday, Oct. 30.

His presentation discussed several formally classified projects that led to much of the UFO speculation of the 1950s and 1960s. For decades, the aerial surveillance programs of the CIA were shrouded in mystery by both design and necessity. Unfortunately, according to Geary, their secrecy and spectacular technological achievements combined to add fuel to conspiracy theories related to extraterrestrials at a time when popular culture experienced a surge in interest in the topic.

Geary is a career leadership analyst who has worked primarily on Iran and the Middle East. In his role as an Iran expert, he briefed senior U.S. government and military leaders, including President Barack Obama in 2012, and foreign leaders. He spent one year as a president's daily briefer at the White House serving then Deputy National Security Adviser for Homeland Security and Counterterrorism John Brennan, and other members of the White House's National Security Council staff.

The Distinguished Speaker Series is designed to allow the Foundation to bring senior government experts to speak to area universities and the general public. Partners participate in the program to enrich the educational opportunities for their students, faculty, and university community. This event was produced in partnership with Park University and the National Archives. If your school or organization is interested in participating in the Speaker Series, contact the Foundation office – office@cgscf.org and (913) 651-0624.

- Simons Center
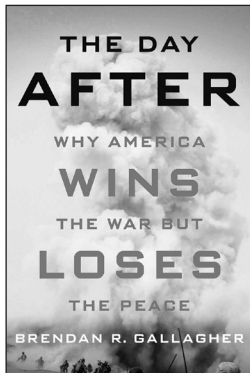
The Day After:
Why America Wins the War but Loses the Peace
by Brendan R. Gallagher

Ithaca, New York: Cornell University Press, 2019. 308 pp.

Reviewed by Lieutenant Commander Ryan Hilger
Navy Engineering Duty Officer, Strategic Systems Programs

The nation's entire cadre of junior and senior leaders have grown up in an era where the United States has enjoyed unequivocal military dominance on the battlefield, but failed to win the peace. In the three decades since the end of the Cold War, all four military services have known both sporadic low intensity conflicts and the nation's longest war in our history. As President George W. Bush declared "mission accomplished" for major combat operations in Iraq on May 1, 2003, aboard the USS Abraham Lincoln (CVN 72), the insurgency was just getting started. The Global War on Terrorism has been going on for eighteen years now, a victim of poor postwar planning, according to Army officer Brendan Gallagher. Bringing his experience on the ground in Afghanistan and Iraq to bear in a strategic level analysis of post-conflict outcomes, Gallagher proposes that the United States fails routinely in Phase IV operations due to poor efforts at three crucial tasks: 1) defining a clear, achievable political goal; 2) adequately anticipating and attempting to mitigate the foreseeable postwar obstacles; and 3) aligning the correct resources to achieve the desired end state.1 While there is no correct answer to these three questions, thorough consideration of these tasks, couched in historical precedents and outcomes, will significantly improve postwar outcomes.

Gallagher analyzes the three strategic questions through the lens of four case studies: Kosovo, Afghanistan, Iraq, and Libya, with Kosovo elevated to the benchmark against which the others are measured. While Kosovo was certainly not perfect, the political outcomes in the two decades since combat operations ceased show a high degree of stability, low rates of recidivism, and the eventual Kosovar declaration of independence from Serbia in 2008. Gallagher deftly weaves the narratives, interleaving personal experiences on the ground in two of the case studies, showing where the processes have broken down. Overall, Gallagher returns again and again to the tension between the Department of State, Department of Defense, and the National Security Council as the source of many of the problems. Their collective failure to work coherently and effectively together significantly undermined the definition of the desired political objectives in both Iraq and Afghanistan. In Libya, President Obama, Gallagher asserts, was well aware of the poor postwar planning for Iraq and Afghanistan and actively sought to repeat the same mistakes in Libya.

Yet similar issues at the senior levels of the Obama administration and the sudden, somewhat unintentional death of Muammar Gaddafi in 2011 resulted in very muddy objectives and rapid mission creep for which they were unprepared.

Gallagher spends the majority of his analysis looking at the interagency. The repeal of Clinton-era Presidential Decision Directive 56 by President Bush, he claims, shunted the National Security Council into a backwater power within the Cabinet. The National Security Council, having learned its lessons in the mid-1990s during Rwanda, Somalia, Haiti, and Bosnia, was a well-functioning organization going into the Kosovo operation in 1999. The acknowledgement of the administration's history and the willingness of the usually dominant Department of Defense to let Secretary of State Madeline Albright take the lead paved the way for a superior postwar outcome in Kosovo. Heavy reliance on the United Nations for a postwar solution was a key highlight that Iraq, Afghanistan, and Libya lacked. Even though partner nations were involved in all the conflicts that Gallagher surveys, the depth of support from UN member nations and the willingness to conduct sanctioned peacekeeping operations there was a key sign of effectiveness in Kosovo. Gallagher offers a basic quantitative analysis of each of the operations and shows that, per person, Kosovo commanded far higher dollars and peacekeepers per person than any of the other conflicts surveyed—by a wide margin. In Iraq, Army General Eric Shinseki's premonition of the conflict requiring half a million troops or more was born out by the time President Bush ordered the surge. Yet even at the peak of the surge, troop levels per Iraqi citizen we well below those in Kosovo. Gallagher's simple mathematical framework offers leaders an easy tool to examine postwar planning for future conflicts and think through how to overcome the obstacles they may encounter.

While Gallagher focuses at the Cabinet level of the administration as the perennial source of the problems, he offers implicit advice for junior and senior leaders in the military services: prepare whether your seniors are or not. Junior leaders may not have the resources to generate deep studies of potential postwar obstacles, but as former Secretary James Mattis notes in Call Sign Chaos, every leader has the ability to read books to prepare effectively for the assignments and challenges ahead. As Secretary Mattis relates, there is nothing new under the sun, and Xenophon's Anabasis, 2,500 years old, was the first book he picked up to begin preparing for combat operations in Iraq in 2003—he knew then that it would be a difficult, if not impossible, peace. Leaders at all levels have something to gain from The Day After as we enter an increasingly unstable world. Prepare wisely. *IAJ*

NOTES

1   Gallagher, pp. 19-23.
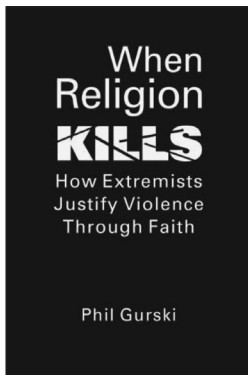
When Religion Kills:
How Extremists Justify Violence Through Faith
by Phil Gurski

Boulder, Colorado: Lynne Rienner Publishers, 2020. 181 pp.

Reviewed by Gary R. Hobin

Assistant Professor, Department of Joint, Interagency, and Multinational Operations
U.S. Army Command and General Staff College, Fort Leavenworth, Kansas

Coming to terms with threats from violent extremist groups requires the involvement of multiple agencies both inside and outside government. A broad approach to these threats would be enabled by a common understanding of how different groups justify the use of violence to advance their ideas.

Phil Gurski's recent book, *When Religion Kills: How Extremists Justify Violence Through Faith*, addresses one aspect of this understanding. Gurski, a former senior analyst in Canada's Security Intelligence Service, approaches his topic systematically, using skills developed over a lengthy career. Importantly, the book addresses six major religious traditions, rather than focusing on a single example. Gurski presents his analysis of each of the six using a common framework: first, he outlines the history of the religious tradition and its main concepts, which he identifies as the normative or mainstream tradition. Next, he provides an overview of the tradition as it relates to surrounding communities, both positively and negatively. Having identified these relationships, he explores the rhetoric of the tradition's extremist leaders who advocate violence, quoting from their speeches and writings. Finally, he draws conclusions from his case-study as to what the data implies. His analytical process of gathering data, assessing its accuracy, determining what it may indicate, and packaging the data in a useable form to enable readers to understand the issues involved is a well-established professional approach. This framework allows Gurski to present a massive amount of often conflicting information in a dispassionate and coherent manner.

This is not to imply that Mr. Gurski has no personal involvement in the topics he covers. He acknowledges that, as an intelligence professional, he has worked on several high-profile cases where violent religious extremists were responsible for massive loss of life; he cites the July 1985 Sikh extremists bombing of an Air India flight from Canada in which 329 passengers and crew aboard were killed. In another place, he refers to his own Catholic upbringing, his attending a Catholic school, and his school community in which sports teams from the neighboring non-religious school were considered to be the enemy. This, he writes, "might strike the reader as silly,"[1] but illustrates that religious-identity conflicts among Christians is neither a new nor a silly thing, and that religiously based violence affects all religious traditions.

In the book's introductory chapter, Mr. Gurski acknowledges the debt he owes to David Raoport, whose essay on "The Four Waves of Modern Terrorism"[2] first postulated the idea that modern terrorism, which Mr. Rapoport dated as originating in the latter years of the 19th century, has exhibited cycles of growth and decline, beginning with a core of "true believers," rising to a peak

of effectiveness, then subsiding as the first recruits to terrorism died off, to be replaced by less committed individuals. Rapoport identified four sequences of terrorism, hence the "four waves," which Gurski summarized as the anarchist wave, the anticolonial wave, the New Left wave, and the religious wave of terrorism. Gurski credits Rapoport with identifying the religious wave, but argues that Rapoport's projection that this wave, like its predecessors, would recede over time may be premature. He points out that the religious wave has already exceeded Rapoport's suggested longevity and shows no signs of diminishing.

One of the strengths of Gurski's book is its broad approach to the question of how some religious leaders use tenets of their faith to justify violence against others. Rather than focus, as other authors have, on one specific faith tradition, Gurski addresses six: each tradition in its own chapter, arranged alphabetically: Buddhist, Christian, Hindu, Islamic, Jewish, and Sikh. Gurski addresses each using the same framework detailed earlier, then, in his final chapter draws some broad conclusions regarding the use of religion as justification. Among his conclusions: extremist leaders from each tradition justify violence as a defensive reaction to those who would undermine that faith in its community, regardless of relative social power—the Rohingya Muslims are not about to replace or subvert Buddhists in Myanmar/Burma, regardless of the strident charges of some notable Buddhist monks. Muslim immigrants are not about to institute shariah law in the United States, regardless of the claims of some fundamentalist preachers. Gurski argues that, generally speaking, charismatic extremist leaders of many religious traditions preach that "the other" faith's adherents are actively seeking to supplant "our" religion or dilute "our" pure bloodline.

Another of his conclusions: violent religious extremists invariably argue that God allows, approves, or even commands violence against others in defense of the faith. Equally, these leaders use authoritative verses from scripture to "prove" that God supports their position. As an example, Christian religious extremists might use scriptural references to Jesus' driving the money-changers from the Temple, or the Psalmist's "Praise be to the Lord, my Rock, who trains my hands for war, my fingers for battle"[3] as proof of God's support for violence against those who differ from their interpretation. Interestingly enough, Gurski's chapter on Christian extremist violence is the longest in the book, in contrast to what he asserts is the government's downplaying of this type of threat.

Phil Gurski's book, *When Religion Kills*, is a valuable reference for anyone who struggles to understand how religions, whose formal doctrines emphasize peace and understanding, can be used to justify horrific violence against people of other faiths, even unto death. His bottom line: a recognized religious authority, using elements of the group's mainstream understanding of its faith, arguing that the faith is under attack from outsiders, provides a potent combination, potentially leading to religiously justified killing. A reader might disagree with some of his conclusions, but would find it difficult to dispute his evidence or his analysis. *IAJ*

NOTES

1   Phil Gurski, When Religion Kills: How Extremists Justify Violence Through Faith, Boulder, CO: Lynne Rienner Publishers, 2020, 66.

2 In Audrey Cronin and James Ludes, editors. Attacking Terrorism: Elements of a Grand Strategy, Washington, DC: Georgetown University Press, 2004, 46-73.

3 Gurski., 57.
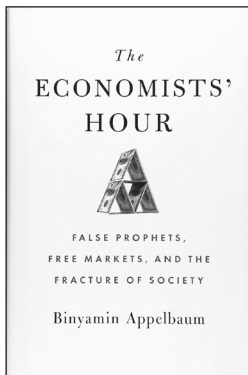
The Economist's Hour: False Prophets, Free Markets, and the Fracture of Society

by Binyamin Appelbaum

New York, New York: Little, Brown and Company, 2019. 440 pp.

Reviewed by Dr. David A. Anderson
Professor of Strategic Studies
U.S. Army Command and General Staff College, Fort Leavenworth, Kansas

Binyamin Appelbaum, an economics and business editorial page writer for the *New York Times*, writes an intriguing historical analysis of the evolving role and influence played by economists on U.S. political policy as well as its effect on the wellness and affluence of the U.S. economy from 1969-2008. He asserts that as economists gained prominence in politics they often advocated for free market policy to enhance economic prosperity for Americans. He believes these policies/policy reforms failed to provide income equality for Americans and only enhanced the financial standing of the elite because the market place favors those with money over those without. Economists focus too much on growth and not enough on income inequality. In essence, the book is a chronological reckoning of the U.S. placing too much emphasis on free and open market economic policy.

Appelbaum begins supporting his thesis by noting that throughout the 1960s the U.S. economy grew at a 3.13 percent annual rate, whereas it grew at a mere 0.94 percent annual rate during the 2000s. He maintains that during this time the U.S. went from producers of products to consumers of products. Throughout the past 45 years the top ten percent of total household income earnings rose from 31 percent to 48 percent. He highlights the stark impact Paul A. Volcker, Jr. the Federal Reserve chair under the Reagan Administration had on the economy when he aggressively attacked inflation by sharply raising interest rates. Appelbaum believes the "Volcker Shock" undermined employment levels and real wages. He emphasizes that inflation adjusted wages are approximately 2,250 dollars less in 2017 than in 1978. For a crescendo, he highlights that for the period 1980-2010 life expectancy rose for the top 20 percent of income earners and declined for the bottom 20 percent. Among women the gap widened from 3.6 years to 13.6 years.

Throughout the book Appelbaum clearly puts the income inequality blame on economists who advised for less government involvement in the economy (e.g. Martin Anderson, Walter Oi, Walt Heller, Milton Freidman, Michael Levine and others). He further blames the Chicago School of Economics for nurturing this economic philosophy over many years. Numerous renowned economists, both practitioners and academics, graduated from and/or taught at The Chicago School of Economics. These economists pushed forward policies that lowered: taxes, the size and scope of spending by government, industrial regulation and anti-trust law while promoting the benefits of globalization. The percentage of federal judges with economics experiences grew from 20 percent to 40 percent from 1980 to 1990 as did trust-the-market rulings. Milton Friedman advocated for smaller government and less government involvement in the economy.

Economist Walt E. Heller proposed to President Kennedy a cut in taxes while borrowing money to pump into the private sector to promote economic growth. Like Art Laffer who later proposed a similar policy to President Reagan, Heller believed lower taxes would actually raise government tax revenues in the long run through greater and repeated spending. Applebaum believes these policies failed to produce equitable results and burdened the country with debt. Later Heller advocated for more government involvement in the economy through monetary and fiscal policy while Freidman advocated for less.

Some U.S. Presidents have followed other economists' suggestions. Presidents Jimmy Carter and Ronald Reagan promoted industry deregulation based on the recommendations from economists such as Michael Levine. Deregulation and the revision of anti-trust law is how Federal Express got its start. Over the years economists Martin Anderson and Walter Oi battled to end military conscription believing it would produce a better military relative to the cost. President Nixon made that law in 1971. Nonetheless, defense spending has continuously grown.

Arguably the biggest contribution the author makes is his painstaking research covering the evolution of notable economists to prominence that has shaped U.S. economic policy over the years. He provides fascinating personal background stories of these economic heavyweights: their professional relationships, economic ideologies, and idiosyncrasies. He includes fascinating stories that bring alive the thought process behind major U.S. economic policy decisions. Appelbaum does a superb job detailing the rise in the ideology of free market capitalism and its influence on political policy both domestically and internationally—from the rise of international financial institutions led by the U.S. to the demise of the Gold Standard and the global embracement of the U.S. dollar as a reserve/vehicle currency. Finally, he defines the growth of the role of economists played in support of Federal government agencies (e.g. the Occupational Safety and Health Administration, and the Environmental Protection Agency).

There are some shortcomings of the book. Appelbaum falls short in recognizing the role of domestic and global economic factors that emerged during the 1970s such as the production of lower cost and high quality products produced in places like Japan and Taiwan, the quality/cost complacency of the U.S. industrial base/manufacturers, small research and development/modernization budgets, growing labor costs, energy/resource scarcity, inflation, technological innovation and others. He is also too quick to criticize without providing an alternative approach to what he argues has been consistently reckless economic policy that has caused the demise of the U.S. economy and exacerbated income equity among Americans. Further overstated is the policy consensus among economists. They did not all think alike and they fiercely debated the economic issues of their day.

In sum, Appelbaum does not provide a balanced prospective. He purposefully promotes his progressive political agenda. He professes inequality has risen because policy makers haven't decided to stop it. Income inequality needs to be addressed through greater government involvement in the economy (e.g. providing a stronger social safety net for working class people, and protecting workers, and their jobs, from foreign competition).

Regardless of these faults, the book is noteworthy in its articulation, research rigor, historical perspective, and its original blending of the minds/thought processes of economists and U.S. government administrations designing, debating, and implementing political economic policy. It is a particularly valuable read for senior military professionals, social science academics/scholars, public policy practitioners, and U.S. government interagency authorities. *IAJ*
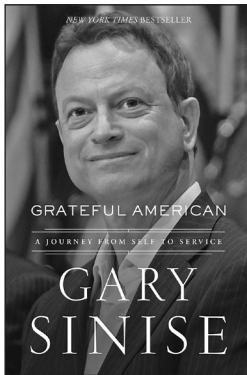
Grateful American:
A Journey from Self to Service
by Gary Sinise, with Marcus Brotherton

Nashville, Tennessee: Nelson Books, 2019. 280 pp.

Reviewed by Susan M. Rocha
Assistant Professor, Department of Joint, Interagency, and Multinational Operations
U.S. Army Command and General Staff College, Redstone Arsenal Satellite Campus

Grateful American tells the story of how Gary Sinise became a dedicated advocate for military service men/women and their families, both active duty and Veterans, as well as first responders—law enforcement and fire fighters. The book is an autobiography and a journal of reflection by the author. He provides an engaging and readable account of his journey to serve, as a grateful American.

Sinise uses many touchpoints in his life to weave his story, beginning with his great-grandparents immigration from Italy to Chicago in 1891; his grandfather's service in the U.S. Army during World War I; and his Uncle Jack's service in World War II as a U.S. Navy B-17 navigator. His father, Robert Sinise, also served in the U.S. Navy, 1951-1955, as a photographer/film developer at the Naval Support facility in Anacostia, D.C. Sinise was born in 1955 while his father was still in the Navy and refers to being a "Navy brat—just barely." Each of his reflections of his family members' military service speak to his ever-increasing understanding of the cost of freedom in our country, and to those who selflessly protect that freedom.

Grateful American includes how Sinise became interested in acting during high school in the suburbs of Chicago, and the drama teacher who opened his eyes to a world of opportunity. He admits he was not a great student—he had trouble reading. He played sports in high school, but was injured, so music and playing in a rock band became his main interest. Then he gets his first acting role in the West Side Story, "I had been baptized. My life of purpose had begun."

Interestingly, his movie career further inspired him to answer the call to serve, particularly his experience with Forest Gump. In making Forrest Gump in 1993 to1994, he discovered what it must be like for many Vietnam Veterans, and it led him to volunteer for the Disabled American Veterans. It also eventually led him to form the "Lt. Dan Band."

The two major events that greatly shaped Sinise's view on "his calling to act" were the Vietnam War and 9/11. Sinise's reflection on the Vietnam War started with his relatives who served in that war. Later when he met with Veteran organizations he realized they were never "Welcomed Home"—they were treated like the enemy, not heroes. Sinise's 9/11 reflection was even more visceral, as he recalled the horrors our nation endured that September day he stated, "…September 11 broke my heart and changed me forever."

In each of the chapters, Sinise focuses on his personal and professional development along life's journey, and his continued reflection on the "calling to serve" beyond himself, for the greater good of our country. He includes a section of pictures in the book, tying his reflections to personal

photos. There is also a "Called to Action" section which lists the organizations and/or efforts he supported over the years, to include the musicians in the "Lt. Dan Band." It is humbling to read how one American citizen has done so much to serve those protecting our way of life.

This is an inspiring read for any American—those who are already patriotic and grateful, as well as those who are confused by or indifferent to the positive focus on military/first responder's service to our country. This book highlights the importance of the civil-military connection as a two-way equation. The average American civilian may take for granted the freedom and security we enjoy, but there is a real cost—it is the military and first responders who pay the greatest price with their lives and health. If only all Americans were as grateful.

Grateful American will interest a general readership, including those interested in Gary Sinise's life as a celebrity, but especially for those who appreciate his many service projects over the past few decades, including the "Gary Sinise Foundation." *IAJ*

Editor's Note: Gary Sinise conducted a meet and greet at the Fort Leavenworth Post Exchange on February 25, 2019, to autograph copies of Grateful American. The event was co-hosted by the Exchange and the CGSC Foundation. In 2014, Sinise and his wife Moira endowed the "Lt. Col. Boyd McCanna 'Mac' Harris Leadership Award" at the U.S. Army Command and General Staff College in honor of his wife's late brother. Lt. Col. Harris was inducted in the Fort Leavenworth Hall of Fame in May 2016. Receiving the honor for Harris were his wife, Anne Harris, and his brother-in-law Gary Sinise.

For the full stories and photos see:

http://www.cgscfoundation.org/grateful-american-returns-to-fort-leavenworth

http://www.cgscfoundation.org/foundation-hosts-dinner-in-honor-of-sinise-family-new-leadership-award

http://www.cgscfoundation.org/they-were-soldiers

Programs of the CGSC Foundation and the Arthur D. Simons Center for Interagency Cooperation are sponsored in part by Armed Forces Insurance and other likeminded donors who support our mission to develop competent, committed leaders of character.

Thank you for your support.

The Simons Center
Fort Leavenworth, Kansas 66027
ph: 913-682-7244
www.TheSimonsCenter.org
facebook.com/TheSimonsCenter

CGSC Foundation, Inc.
100 Stimson Avenue, Suite 1149
Fort Leavenworth, Kansas 66027
ph: 913-651-0624
www.cgscfoundation.org
facebook.com/CGSCFoundation
twitter.com/CGSCFoundation
LinkedIn.com >>CGSC Foundation, Inc.