



INSTITUTE FOR DEFENSE ANALYSES

## **Building Partner Nation Capabilities with Commercial Technology**

Jarrett M. Lane  
Abdullah Naimzadeh  
EunRae Oh  
Matthew J. Reed  
Jennifer M. Taylor  
Mallory B. Thompson

September 2024

Distribution A; Approved for  
public release: distribution is  
unlimited.

IDA Product 3003307

INSTITUTE FOR DEFENSE ANALYSES  
730 East Glebe Road  
Alexandria, Virginia 22305-3086



The Institute for Defense Analyses is a nonprofit corporation that operates three Federally Funded Research and Development Centers. Its mission is to answer the most challenging U.S. security and science policy questions with objective analysis, leveraging extraordinary scientific, technical, and analytic expertise.

### **About This Publication**

This work was conducted by the IDA Systems and Analyses Center under contract HQ0034-19-D-0001, project DF-8-5313 “Security Cooperation Technical Trends Analysis for DSCA,” for the Defense Security Cooperation Agency. The views, opinions, and findings should not be construed as representing the official position of either the Department of Defense or the sponsoring organization.

### **Acknowledgments**

The authors would like to thank Leslie A. Hunter, Geoffrey M. Koretsky, Claudia T. Munoz, Laura A. Odell, Carlos Pesquera, and Kristian E. Smith of the IDA Systems and Analyses Center for their technical review of this report.

### **For More Information**

Jennifer M. Taylor, Project Leader  
jtaylor@ida.org, 703-845-2107

Daniel Y. Chiu, Director, Joint Advanced Warfighting Division  
dchiu@ida.org, 703-845-2439

### **Copyright Notice**

© 2024 Institute for Defense Analyses  
730 East Glebe Road, Alexandria, Virginia 22305-3086 • (703) 845-2000.

This material may be reproduced by or for the U.S. Government pursuant to the copyright license under the clause at DFARS 252.227-7013 (Feb. 2014).

INSTITUTE FOR DEFENSE ANALYSES

IDA Product 3003307

**Building Partner Nation Capabilities with  
Commercial Technology**

Jarrett M. Lane  
Abdullah Naimzadeh  
EunRae Oh  
Matthew J. Reed  
Jennifer M. Taylor  
Mallory B. Thompson



## Executive Summary

---

Commercial technologies are changing national defense and how wars are fought. The *2022 National Defense Strategy of the United States of America* highlights the importance of leveraging commercial technologies and innovation to maintain U.S. warfighting advantages.<sup>1</sup> Further, the use of commercial technologies in the Ukraine war demonstrates their utility and impact in modern conflict. While the Department of Defense (DoD) is increasingly investing in commercial technologies to enhance its capabilities, there is no established lead, strategy, or formal initiative to help partner nations understand use cases for commercial technologies, or to acquire, integrate, and deploy them for warfighting and critical task execution. The Defense Security Cooperation Agency (DSCA) requested that the Institute for Defense Analyses (IDA) consider how the defense system, from the security cooperation, acquisition, and defense innovation points of view, might be able to better support partners and increase partners' access to commercial technologies to solve operational challenges.

DoD's current approach to enhancing partner nations' capabilities leans heavily on sales and transfers of traditional hardware, platforms, and systems—legacy items and products covered by existing programs of record—developed for the U.S. military. This approach enables interoperability with U.S. forces, ensures sustainability and long-term supportability, and promotes the U.S. defense industrial base. However, these systems are often expensive and difficult to maintain, and they may take years to acquire and deliver. Many of these capabilities were developed in the context of U.S. military missions and the way in which the U.S. warfighter will operate in conflict, which may be different from the approach of a partner nation military. Furthermore, the hardware, platforms, and systems typically provided to partner nations often do not represent the latest available technology.

To help address this gap, the DSCA aims to develop new approaches for providing innovative commercial capabilities to partners. In support of this effort, DSCA asked IDA to assist in developing new approaches to providing capabilities to partner nations—particularly timely integration of new and emerging commercial technologies that could be used by partner nations to exercise self-defense and deterrence vis-à-vis the People's Republic of China and Russia.

---

<sup>1</sup> U.S. Department of Defense, *2022 National Defense Strategy of the United States of America*, October 27, 2022, <https://media.defense.gov/2022/Oct/27/2003103845/-1/-1/1/2022-NATIONAL-DEFENSE-STRATEGY-NPR-MDR.PDF>.

To complete this study, the IDA team interviewed representatives of fourteen Defense Innovation Organizations (DIOs) to understand their organizations' current engagement with partner nations. Interviews also served to evaluate how DSCA could leverage DIOs' insights into the commercial technology market to identify viable solutions for partner nations. The IDA team also conducted an extensive literature review to understand key trends across commercial technologies and evaluate their potential applicability to functional areas and tasks commonly executed by partner nation militaries. The team validated its literature review findings through interviews with IDA technologists and outside experts on military applications of commercial technologies.

This research surfaced four insights that can guide DSCA's efforts to incorporate commercial technology into security assistance activities. First, DIOs recognize the importance of supporting partner nations, but lack the resources and mandate to do so consistently. DIOs' ability to engage in helping solve partner nations' security challenges will likely be ad hoc and dictated by team (or individual) capacity at a given time.

Second, there are limitations to DIOs' ability to share information on commercial technology providers with DSCA. Some DIOs do not maintain well-structured datasets on companies with which they have engaged and commercial technologies they have explored. For those that do preserve data on commercial companies and technologies, policy blockers, contractual terms (e.g., non-disclosure agreements), and bandwidth constraints prevent DIOs from giving DSCA direct access to the data. As a result, DSCA will either need to submit ad hoc, targeted requests to DIOs for data or gather market data itself when scouting for potential solutions to partner nations' challenges.

Third, commercial technologies have the potential to deliver transformative effects across multiple functional areas and tasks for partner nations. Notably, four technology groupings can deliver significant impact across a multitude of tasks: compute, data, cyber, and artificial intelligence (AI)—specifically, multimodal AI and generative AI. This analysis suggests that investing in foundational commercial technologies like compute, data, cyber, and AI could create a flywheel effect, enabling partner nations to apply these capabilities to solve multiple problems across their enterprise and defense forces. Of the functional areas and tasks analyzed, intelligence, surveillance, and reconnaissance; measurement and signals intelligence; and maritime domain awareness can benefit greatly from commercial technologies. There is also great potential for commercial technologies to help modernize how partner nations execute command and control, manage enterprise-wide information technology, and conduct special operations (e.g., asymmetric warfare).

Fourth, there are multiple potential business strategies that DSCA could implement to incorporate commercial technology into security cooperation. In this report, IDA presents three potential strategies. The first is one in which DSCA advocates for the Defense Innovation Unit (DIU), which is a leading DIO, to own commercial technology-related efforts for the security cooperation community. The second strategy is one in which

DSCA and DIU co-own commercial technology-related efforts and create a division of labor based on technology or use cases (e.g., strategic versus tactical). The third potential strategy is one in which DSCA leads commercial technology-related activities and invests in building the team to do so.

Before pursuing any strategy over another, the following actions will arm DSCA with critical insights and learnings to make informed decisions about how to craft its business strategy going forward:

- engaging with key stakeholders (i.e., industry, partner nations, U.S. government) to understand their needs,
- working with the security cooperation community to introduce the concept of leveraging commercial technology to solve partner nations' challenges,
- focusing efforts on specific technologies or functional areas, and
- conducting pilot projects with DIOs, like the DIU.





# Contents

---

Executive Summary .....	iii
1. Introduction .....	1
A. Approach and Report Structure .....	2
2. Commercial Tech: Benefits and Drivers .....	5
A. Ukraine as a Case Study .....	5
B. PRC Use of Commercial Technology to Counter U.S. Influence .....	6
C. Security Cooperation as a Critical Enabler .....	8
3. Defense Innovation Organizations .....	11
A. DIO Data Sources and Availability to DSCA .....	12
B. Opportunities for Collaboration .....	12
C. Barriers and Challenges to Collaboration .....	14
4. Commercial Technologies and Capabilities .....	17
A. Heatmap Methodology .....	17
B. Commercial Technology Trends .....	20
C. Impacts on Functional Areas and Tasks .....	21
5. Business Strategies and Recommendations .....	25
A. Overarching Recommendations .....	25
B. Strategy #1: Implement a DIU-Led Approach .....	32
C. Strategy #2: Implement a Joint DSCA-DIU Approach .....	35
D. Strategy #3: Implement a DSCA-Led Approach .....	38
6. Additional Considerations and Research .....	47
7. Conclusion .....	51
Appendix A. DIOs Interviewed .....	A-1
Appendix B. Commercial Technology Heatmap .....	B-1
Appendix C. Definitions of Heatmap Task Areas .....	C-1
Appendix D. Resource Mock-Ups .....	D-1
Appendix E. Summary Table of Recommendations .....	E-1
References .....	F-1
Abbreviations .....	G-1



# 1. Introduction

---

The *2022 National Defense Strategy of the United States of America (NDS)* emphasizes the importance of innovation and commercial technologies to ensure the U.S. warfighting advantage—a point of emphasis that the *NDS* extends to partners, as well.<sup>2</sup> The strategy states, “The [Department of Defense] will support the innovation ecosystem both at home and in expanded partnerships with our Allies and partners.”<sup>3</sup> The *NDS* also notes that the Department of Defense (DoD) will “assist Allies and partners” in improving their resilience and ability to “fight through disruption” by improving, for example, cyber resilience through technologies such as modern encryption and zero-trust architectures.<sup>4</sup>

Notwithstanding recognition of commercial technologies’ potential impact on partner nations’ warfighting capabilities, there is no established lead, strategy, or formal initiative to help partner nations understand use cases for commercial technologies, or to acquire, integrate, and deploy them for warfighting and critical task execution. To help address this gap, the Defense Security Cooperation Agency (DSCA) is exploring new approaches for leveraging innovative commercial technologies to build partner nation capabilities—particularly commercial technologies that could be used by partner nations to exercise self-defense and deterrence vis-à-vis the People’s Republic of China (PRC) and Russia.

DoD’s current approach to enhancing partner nations’ capabilities leans heavily on sales and transfers of traditional hardware, platforms, and systems—legacy items and products covered by existing programs of record—developed for the U.S. military. The current approach has value. It enables interoperability with U.S. forces, ensures sustainability and long-term supportability of important platforms, and promotes the U.S. defense industrial base. However, traditional hardware, platforms, and systems are often expensive and difficult to maintain, and they may take years to acquire and deliver. Many of these capabilities were developed in the context of U.S. military missions and the way in which the U.S. warfighter will operate in conflict, which may be different from the approach of a partner nation military. Furthermore, the hardware, platforms, and systems typically provided to partner nations often do not represent the latest available technology.

---

<sup>2</sup> U.S. Department of Defense, *2022 National Defense Strategy of the United States of America.*”

<sup>3</sup> U.S. Department of Defense, *2022 National Defense Strategy*, 19.

<sup>4</sup> U.S. Department of Defense, *2022 National Defense Strategy*, 8.

## **A. Approach and Report Structure<sup>5</sup>**

This report offers a summary of the Institute for Defense Analyses' (IDA's) research, findings, and recommendations for how DSCA, other key stakeholders in the security cooperation community, and Defense Innovation Organizations (DIOs) can develop new approaches for incorporating commercially technology into security cooperation activities.

To complete this study, the IDA team interviewed representatives of fourteen DIOs (listed in Appendix A) to understand their organizations' current engagement with partner nations. Interviews also served to evaluate how DSCA could leverage DIOs' insights into the commercial technology market to identify viable solutions for partner nations. The project team focused on interviewing DIOs because these organizations are tasked with identifying commercial technologies and/or developing innovative commercially derived capabilities for the U.S. Department of Defense. Therefore, a core assumption in IDA's research is that DIOs are optimally positioned to help DSCA quickly identify innovative capabilities for partner nations.

The IDA team also conducted an extensive literature review to understand key trends across commercial technologies and evaluate their potential applicability to functional areas and tasks commonly executed by partner nation militaries. The team validated its literature review findings through interviews with IDA technologists and outside experts on military applications of commercial technologies.

This report starts by providing a high-level overview of the potential benefits and drivers of incorporating commercial technology into security cooperation activities. Given the importance of DIOs in enabling adoption of commercially available capabilities across the DoD, the report then outlines lessons learned into how DIOs gather data on commercially available capabilities, as well as insights into opportunities and barriers to DSCA collaborating with DIOs to facilitate adoption of commercially available capabilities among partner nations.

Next, the report evaluates which commercial technologies may be most impactful or relevant to partner nations. Because the universe of commercially available capabilities is vast, the IDA team developed a heatmap of commercial technologies and their potential impact on partner nation militaries' critical tasks and functional areas. The heatmap serves as a tool to help DSCA focus its efforts on specific commercial technologies.

---

<sup>5</sup> Consistent with the statement of work (task order HQ003423F0007), in addition to producing this report, the IDA team regularly briefed the sponsor to provide updates on the project's status and findings, provided accessible datasets (inclusive of the heatmap presented in this report), and produced short papers and analyses. The IDA team's research into datasets on technology trends yielded findings that, in coordination with the sponsor, required IDA to adjust the focus of its work, as articulated in this report. This report will also be complemented by a final briefing to DSCA leadership.

The report concludes by offering overarching recommendations for how DSCA can begin to incorporate commercial technologies into security cooperation activities, as well as three potential business strategies and recommended steps for how DSCA can implement and sustain coordinated efforts to leverage commercial technologies in building partner nation capabilities.

To help ensure clarity and readability of this paper, two critical terms used throughout this report need to first be defined: commercial technology and DIOs.

- **Commercial technology.** In the context of this paper, commercial technology refers to commercial-off-the-shelf technologies (COTS), as well as systems, tools, or weapons that are developed by private companies in partnership, under contract, or based on a demand signal from DIOs (i.e., “DIO-driven”). DIO-driven technologies are often derivative from COTS technology that have been hardened, modified or weaponized to address a capability gap. They can also represent the application of emergent science, computing, or engineering to improve an existing capability. These technologies, would not be readily available to partner nations without a deliberate effort by the DoD and DIOs to make them accessible.
- **Defense innovation organizations (DIOs).** DIOs are organizations that identify technologies and innovations (often produced by the private sector) and provide pathways for those technologies and innovations to be acquired and fielded by the DoD. DIOs are not exclusively DoD entities. The Undersecretary of Defense for Research and Engineering (USD R&E) identified over 250 DoD entities and partner organizations (e.g., federally funded research and development centers, labs, consortia, universities) as “innovation organizations.”<sup>6 7</sup> The Defense Innovation Unit (DIU) was tasked as the lead DIO responsible for organizing a core subset of DoD entities within the DIO community, called the Defense Innovation Community of Entities (DICE).<sup>8</sup>

---

<sup>6</sup> Office of the Undersecretary of Defense for Research and Engineering, “Innovation organizations,” Department of Defense, <https://www.ctoinnovation.mil/innovation-organizations/>.

<sup>7</sup> Not all of the “innovation organizations” identified by USD R&E focus on commercial technology. Some focus on basic research, technology assessments, or some other role in the innovation process.

<sup>8</sup> *Outpacing China: Expediting Innovation to the Warfighter, Before the United States House of Representatives Armed Services Committee*, 118<sup>th</sup> Cong. (2024) (statement of Douglas A. Beck, Director of Defense Innovation Unit).



## 2. Commercial Tech: Benefits and Drivers

---

### A. Ukraine as a Case Study

The ongoing conflict in Ukraine against Russian forces provides a relevant example of successful, rapid adaptation of commercial technology for military use. The first salvo in Russia's invasion was massive, widespread cyberattacks.<sup>9</sup> In response, the Ukrainian government worked with U.S. cloud companies to use edge computing devices to rapidly move terabytes of data and operations to commercial cloud infrastructure, which significantly improved the government's resilience against cyberattacks while preserving critical data and government services.<sup>10, 11</sup>

In the battlefield, commercial technologies are playing a pivotal role in Ukraine's ability to damage Russian forces. Ukrainian warfighters are innovating with commercial drones to improve reconnaissance, targeting, and delivery of small munitions. For example, Agile software development practices and tools used in commercial sectors enabled the Ukrainian army to develop Delta, a software platform that integrates satellite imagery, drone imagery, social media, and more to create a comprehensive view of the battlefield and derive actionable intelligence.<sup>12</sup> Commercial satellite communications, provided by Starlink, enabled Ukrainian forces to deploy Delta directly into the hands of warfighters, and maintain command and control (C2) after Russia disrupted Ukraine's military satellite communications.<sup>13</sup>

---

<sup>9</sup> James Pearson & Christopher Bing, "The Cyber War Between Ukraine and Russia: An Overview," Reuters, May 10, 2022, <https://www.reuters.com/world/europe/factbox-the-cyber-war-between-ukraine-russia-2022-05-10/>.

<sup>10</sup> Russ Mitchell, "How Amazon Put Ukraine's 'Government in a Box'—and Saved its Economy from Russia," *Los Angeles Times*, December 15, 2022, <https://www.latimes.com/business/story/2022-12-15/amazon-ukraine-war-cloud-data>. <sup>11</sup> Frank Konkel, "Ukraine Tech Chief: Cloud Migration 'Saved Ukrainian Government and Economy,'" Nextgov, December 1, 2022, <https://www.nextgov.com/digital-government/2022/12/ukraine-tech-chief-cloud-migration-saved-ukrainian-government-and-economy/380328/>

<sup>11</sup> Frank Konkel, "Ukraine Tech Chief: Cloud Migration 'Saved Ukrainian Government and Economy,'" Nextgov, December 1, 2022, <https://www.nextgov.com/digital-government/2022/12/ukraine-tech-chief-cloud-migration-saved-ukrainian-government-and-economy/380328/>

<sup>12</sup> Julian Borger, "Our Weapons Are Computers": Ukrainian Coders Aim to Gain Battlefield Edge," *The Guardian*, December 18, 2022, <https://www.theguardian.com/world/2022/dec/18/our-weapons-are-computers-ukrainian-coders-aim-to-gain-battlefield-edge>.

<sup>13</sup> Grace Jones, Grace, Janet Egan, & Eric Rosenbach, "*Advancing in Adversity: Ukraine's Battlefield Technologies and Lessons for the U.S.*," Harvard University Belfer Center, July 31, 2023,

Ukraine’s use of commercial drones also serves as an example of the potential cost and speed advantages of commercial, dual-use technologies. For example, Ukraine is using commercial drones to develop loitering munitions that target armor, weapons systems, entrenched combatants, and more—effects traditionally delivered with systems and materiel like aircraft and artillery.<sup>14</sup> For reference, DJI drones (a Chinese product) commonly used by Ukrainian forces for surveillance, retail for roughly \$2,000.<sup>15</sup> Ukraine has also developed the ability to produce its own low-cost drones. One report indicates that for about \$400—about one-tenth the cost of a traditional projectile—Ukrainian drone teams can produce an exploding drone capable of destroying a Russian tank.<sup>16</sup>

Though commercially available capabilities may not always be a suitable replacement for traditional capabilities, they can be additive and may effectively augment how partner nations execute critical tasks. Creative applications of commercially available capabilities can also be useful in mitigating risks in supply shortages and augmenting partners’ warfighting plans, and tactics. Ukraine’s use of commercially available capabilities is not only cost-effective and agile, it is borne out of necessity. Bottlenecks and capacity constraints in the supply chain for materiel necessitate innovation. As of 2023, Ukraine’s monthly use of 155-millimeter shells outstripped one year of U.S. production capacity.<sup>17</sup> Though increasing production capacity and shoring-up the defense industrial base is a top priority, challenges such as hiring, raw material availability, and manufacturing equipment will remain a concern for the foreseeable future.<sup>18</sup>

## **B. PRC Use of Commercial Technology to Counter U.S. Influence**

IDA’s analysis indicates that the PRC recognizes the value of exporting commercial technology and that it is using this technology as a means to expand their influence around the globe and counter U.S. similar efforts. Over the last several decades, the PRC drastically strengthened its commercial and dual-use technology industries. The PRC’s civil-military fusion strategy, coupled with an increase in the country’s defense spending, led to tens of billions of dollars in funding to streamline PRC commercial research and

---

<https://www.belfercenter.org/publication/advancing-adversity-ukraines-battlefield-technologies-and-lessons-us>.

<sup>14</sup> Justin Ling, “To Beat Russia, Ukraine Needs a Major Tech Breakthrough,” WIRED, January 4, 2024, <https://www.wired.com/story/ukraine-russia-future-war-tech/>.

<sup>15</sup> Philip E. Ross, “Budget Drones in Ukraine Are Redefining Warfare: Small, Low-cost Tech Enables new Military Tactics,” IEEE Spectrum, May 17, 2023, <https://spectrum.ieee.org/drone-warfare-ukraine>.

<sup>16</sup> Samya Kullab, “How Ukraine Soldiers Use Inexpensive Commercial Drones on the Battlefield,” PBS News, September 26, 2023, <https://www.pbs.org/newshour/world/how-ukraine-soldiers-use-inexpensive-commercial-drones-on-the-battlefield>.

<sup>17</sup> Frank Morris, “*Slow Manufacturing and Price Gouging Threaten the New U.S. Military Arms Race*,” NPR, April 14, 2023, <https://www.npr.org/2023/04/07/1168725028/manufacturing-price-gauging-new-u-s-military-arms>.

<sup>18</sup> Morris, “*Slow Manufacturing*.”



development efforts and to advance dual-use technology projects.<sup>19 20 21 22</sup> The Chinese Communist Party even created the Central Commission for Integrated Military and Civilian Development to promote collaboration among Chinese universities, technology companies, and the military, making it difficult to bifurcate Chinese commercial activity from government and military activity.<sup>23</sup> Between 2022 and 2023, the U.S. Department of Commerce added over seventy Chinese technology companies to the Entity List after determining the companies have “close ties... to the Chinese military and the defense industry” and that they often specialize in dual-use technologies like artificial intelligence (AI) and software used for weapon life-cycle management.<sup>24 25 26</sup> In fact, according to a 2022 RAND report, almost half of the PRC’s manufacturing output is considered dual-use.<sup>27</sup>

The PRC’s civil-military fusion strategy enables its Belt and Road Initiative, which is a strategy for growing the PRC’s economic and political global influence.<sup>28</sup> The PRC leans on its ubiquitous availability of Chinese-produced technologies to foster partnerships and become a source of low-cost, quickly acquirable capabilities.<sup>29</sup> IDA’s analysis of open-source data indicates China may be incorporating commercial, dual-use technologies into

---

<sup>19</sup> Meia Nouwens, & Helena Legarda, “*China’s Pursuit of Advanced Dual-use Technologies*,” International Institute for Strategic Studies, December 18, 2018, <https://www.iiss.org/research-paper/2018/12/emerging-technology-dominance>.

<sup>20</sup> Evelyn Cheng, “China to Increase Defense Spending by 7.2%,” CNBC, March 4, 2023, <https://www.cnbc.com/2023/03/05/china-defense-budget-two-sessions.html>.

<sup>21</sup> China Power Team, “How Dominant Is China in the Global Arms Trade?,” CSIS, April 26, 2018, <https://chinapower.csis.org/china-global-arms-trade/>.

<sup>22</sup> U.S. Department of Defense, “Military and Security Developments Involving the People’s Republic of China,” 2023, <https://media.defense.gov/2023/Oct/19/2003323409/-1/-1/1/2023-MILITARY-AND-SECURITY-DEVELOPMENTS-INVOLVING-THE-PEOPLES-REPUBLIC-OF-CHINA.PDF>.

<sup>23</sup> Nouwens & Legarda, “*China’s Pursuit*.”

<sup>24</sup> The Entity List is a U.S. government list of foreign individuals, companies, and organizations deemed a national security concern, subjecting them to export restrictions and licensing requirements for certain technologies and goods.

<sup>25</sup> U.S. Department of Commerce, Bureau of Industry and Security, “Additions and Revisions to the Entity List and Conforming Removal from the Unverified List,” December 19, 2022, <https://public-inspection.federalregister.gov/2022-27151.pdf>.

<sup>26</sup> U. S. Department of Commerce, Industry and Security Bureau, “Additions of Entities to the Entity List and Removal of Entity from the Entity List,” Federal Register, June 14, 2023, <https://www.federalregister.gov/documents/2023/06/14/2023-12726/additions-of-entities-to-the-entity-list-and-removal-of-entity-from-the-entity-list>.

<sup>27</sup> Cortney Weinbaum et al. “China’s Defense Industrial Base,” RAND, February 11, 2022, [https://www.rand.org/pubs/research\\_briefs/RBA930-1.html](https://www.rand.org/pubs/research_briefs/RBA930-1.html).

<sup>28</sup> Ahmad Syamsudin & Chen Mei Hua, “Huawei’s Role in Indonesia Raises Digital Colonization Concerns,” Radio Free Asia, September 27, 2023, <https://www.rfa.org/english/news/china/china-bri-indonesia-09272023104442.html>

<sup>29</sup> Daniel R. Russel, & Blake H. Berger, “*Weaponizing the Belt and Road Initiative*,” Asia Society Policy Institute, September 2020, [https://asiasociety.org/sites/default/files/2020-09/Weaponizing%20the%20Belt%20and%20Road%20Initiative\\_0.pdf](https://asiasociety.org/sites/default/files/2020-09/Weaponizing%20the%20Belt%20and%20Road%20Initiative_0.pdf).

its security assistance packages. For example, Huawei (one of the world’s largest telecommunications companies and suspected to have deep ties with the Chinese Communist Party and Chinese military)<sup>30</sup> sold cybersecurity capabilities to Indonesia’s National Cyber and Crypto Agency—roughly equivalent to the U.S. National Security Agency.<sup>31</sup> Many export-restricted companies on the Entity List, like ZTE, Huawei, Tencent, Hikvision, Zhejiang Dahua, and Alibaba, have directly sold their dual-use technologies (e.g., cloud, AI, and surveillance technology) to foreign governments, militaries, and security forces on almost every continent.<sup>32 33 34</sup> Since 2009, Chinese technology companies signed contracts with over 140 countries to install automated “safe city” surveillance equipment (including facial recognition technology) that allows governments to monitor cities and towns.<sup>35</sup>

The PRC will continue to provide its commercially available capabilities faster and cheaper than the United States will, creating technological and economic dependencies that may provide the PRC with global influence among partner nations.<sup>36 37</sup> Without a strategy to include partner nations in United States’ fostering and adoption of commercial technology, the PRC may take advantage of its comparative strengths in commercial and dual-use technologies to counter U.S. security cooperation efforts. The DoD must therefore develop a strategy to compete with the PRC’s ability to rapidly export commercial technology, retain the U.S.’s status as the partner of choice, and assist partner nations with achieving United States’ global security objectives.

### C. Security Cooperation as a Critical Enabler

Helping partner nations incorporate commercial technologies into their operations presents an opportunity both to improve their ability to counter Chinese and Russian aggression and to improve the U.S.’s position as a partner of choice. The NDS specifically

---

<sup>30</sup> Noah Berman et al., “Is China’s Huawei a Threat to U.S. National Security?,” Council on Foreign Relations, February 8, 2023, <https://www.cfr.org/backgrounders/chinas-huawei-threat-us-national-security>.

<sup>31</sup> Syamsudin & Mei Hua, “Huawei’s Role.”

<sup>32</sup> Jennifer Bouey et al., “China’s AI Exports: Technology Distribution and Data Safety,” RAND, December 11, 2023, [https://www.rand.org/pubs/research\\_reports/RRA2696-2.html](https://www.rand.org/pubs/research_reports/RRA2696-2.html).

<sup>33</sup> Mark Montgomery & Eric Sayers, “Don’t Let China Take Over the Cloud—US National Security Depends on it,” *The Hill*, November 13, 2023, <https://thehill.com/opinion/national-security/4307002-dont-let-china-take-over-the-cloud-us-national-security-depends-on-it/>.

<sup>34</sup> Kaan Sahin, “*The West, China, and AI surveillance*,” Atlantic Council, December 18, 2020, <https://www.atlanticcouncil.org/blogs/geotech-cues/the-west-china-and-ai-surveillance/>.

<sup>35</sup> James Kynge, et al. “Exporting Chinese Surveillance: The Security Risks of ‘Smart Cities’,” *Financial Times*, June 9, 2021, <https://www.ft.com/content/76fdac7c-7076-47a4-bcb0-7e75af0aadab>.

<sup>36</sup> Sarosh Nagar, “ZTE’s Revenge: Russia’s Technological Power Vacuum in the Wake of the Ukraine War,” *Harvard International Review*, August 24, 2022, <https://hir.harvard.edu/ztes-revenge-russias-technological-power-vacuum-in-the-wake-of-the-ukraine-war/>

<sup>37</sup> Nouwens & Legarda, “*China’s Pursuit of advanced dual-use technologies.*”

highlights the importance of leveraging commercial technologies and innovation to maintain U.S. warfighting advantages.<sup>38</sup> Leveraging commercial technology is not only essential to defending American alliances and influence abroad, but may be key to helping U.S. partner nations deter and defend themselves against aggression in cost-effective and adaptable ways. Commercial technologies can improve partner nations' capabilities across functional areas and tasks critical to self-defense and deterrence. Though commercial technologies may not always be appropriate or optimal solutions to a partner nation's needs, they can offer some advantages and opportunities that traditional defense products and services cannot. Much like the DoD's own motivations to leverage commercial technologies, partner nations can benefit from the pace of innovation, adaptability, and quality of solutions available in the commercial market.

The tradeoffs of using commercial technology versus traditional military capabilities will need to be evaluated on a case-by-case basis. However, recent use cases suggest that commercial technologies can materially benefit partner nations' ability to deter and defend against aggression, and offer the DoD another effective tool for building partnerships and critical capabilities internationally. In some cases, commercial technologies may offer lower cost solutions than traditional military capabilities.<sup>39</sup> This technology might also be more relevant to the partner nation's needs and might better address interoperability and capability gaps that could serve as a force multiplier and further U.S. goals in a particular region.

---

<sup>38</sup> U.S. Department of Defense, *2022 National Defense Strategy*.

<sup>39</sup> Gregory C. Allen, "Across Drones, AI, and Space, Commercial Tech Is Flexing Military Muscle in Ukraine," CSIS, May 13, 2022, <https://www.csis.org/analysis/across-drones-ai-and-space-commercial-tech-flexing-military-muscle-ukraine>.



### 3. Defense Innovation Organizations

---

IDA engaged with fourteen DIOs to understand how partner nations factor into their strategies. The IDA team also explored how DSCA can access DIOs' data and insights into commercially available capabilities. To inform potential strategies for how DSCA can best incorporate commercial technologies into security cooperation activities, IDA captured lessons learned about how DIOs interact with industry and explored opportunities and challenges to leveraging the DIOs' expertise and resources to support partner nations.

IDA found that DIOs generally recognize the importance and potential impact of helping partner nations acquire commercially available capabilities. In fact, the DIU 3.0 plan states, "We must connect the solutions created by U.S. tech companies to allied and partner acquisition organizations when appropriate ... especially in a conflict, when speed is critical."<sup>40</sup> However, IDA found that DIOs lack the mandate, resources, presence, and expertise required to help address partner nations' needs proactively and consistently. DIOs focus foremost on acquiring technologies for the DoD. In cases in which DIOs are engaging internationally, it is typically with allies and high-end partners and focused on international armaments cooperation in service of better capabilities for the U.S. warfighter.<sup>41</sup> There are periodic engagements with partner nations, though usually in response to an active conflict or acute, tactical problem (e.g., the war in Ukraine).<sup>42</sup> However, the DIOs do not currently have focused lines of effort or goals associated with helping partner nations leverage commercially available capabilities.

Some DIO representatives, including DIU, offered to query their datasets for targeted requests from DSCA and help DSCA run outreach events in support of specific partner nations. Working with willing leaders and individuals within DIOs may allow DSCA to tap the DIOs' networks, expertise, and capabilities for identifying, vetting, and sourcing commercially available capabilities. Connecting DIOs' knowledge of commercial

---

<sup>40</sup> Douglas A. Beck, "DIU 3.0: Scaling Defense Innovation for Strategic Impact," Center for a New American Security, February 7, 2024, <https://www.cnas.org/publications/reports/diu-3-0>.

<sup>41</sup> See, for example, DIU's collaboration with the trilateral partnership of Australia, the United Kingdom, and U.S. (AUKUS) to run a multinational electromagnetic warfare challenge. See also DIU's coordination with the Indian Ministry of Defense's Innovations for Defense Excellence organization on a joint challenge to develop maritime intelligence, surveillance, and reconnaissance (ISR) capabilities.

<sup>42</sup> See, for example, DIU's support to requirements generation and technology delivery for Ukraine. The DIU indicates it plans to increase its activity with international allies and partners as part of DIU 3.0—the organization's latest evolution—but is prioritizing engagement with allies and well-resourced partners like India.

capabilities with the expertise of DSCA and Security Cooperation Organizations (SCOs) has the potential to deliver value to partner nations.

## **A. DIO Data Sources and Availability to DSCA**

DIOs curate ecosystems of industry partners and gain visibility into the market, in part, by conducting a variety of industry outreach activities. Examples include open “office hours,” pitch events, and formal requests for proposal (RFPs) aimed at attracting non-traditional vendors and innovative solutions. One of these organizations, DIU, reported in FY 2022 that they received over 1,600 pitches from industry. These figures suggest DIOs have the reach and market visibility that could help DSCA accelerate and scale efforts to find commercially available capabilities relevant to partner nations.

Additionally, DIOs often work closely with trade associations. Working with trade associations (e.g., the Association for Uncrewed Vehicle Systems International (AUVSI)) could help DSCA scale outreach and engagement with industry, as well as access datasets maintained by the associations on members and their respective products. For example, AUVSI maintains a dataset that is accessible for a fee and regularly updated with technical specifications and contact information for specific drones.<sup>43</sup>

Finally, open-source researchers and reports can serve as a valuable source of intelligence on technology trends and applications. For example, some researchers spend significant time and effort tracking the models of drones and other technologies used in active conflicts (e.g., Ukraine).<sup>44</sup> Although not all of these technologies are going to be provided by the U.S. or by allies, DSCA can use open-source reporting and researcher datasets to find examples of technologies and products used by military and security forces globally. Additionally, DIOs leverage subscription services to specialized publications (e.g., *Jane’s*), industry analyst reports (e.g., Gartner), and market intelligence services (e.g., Crunchbase and Futurepedia.io). DSCA could acquire access to such databases, as well, to gain insights into key trends and potential solutions for partner nations.

## **B. Opportunities for Collaboration**

The DIOs representatives with whom the IDA team met recognize the importance and potential impact of helping partner nations acquire commercially available capabilities. Some DIO representatives offered to query their datasets for targeted requests from DSCA and help DSCA run outreach events in support of specific partner nations. Working with

---

<sup>43</sup> “Uncrewed Systems & Robotics Database,” AUVSI, accessed September 3, 2024, <https://www.auvsi.org/usrd>.

<sup>45</sup> National Urban Security Technology Laboratory, “*Saver Technote: Laser Protective Eyewear*,” U.S. Department of Homeland Security, January 2022, [https://www.dhs.gov/sites/default/files/2022-01/SAVER\\_Laser%20Protective%20Eyewear\\_TechNote\\_508%20final\\_18Jan2022.pdf](https://www.dhs.gov/sites/default/files/2022-01/SAVER_Laser%20Protective%20Eyewear_TechNote_508%20final_18Jan2022.pdf).

DIOs may allow DSCA to tap the DIOs' networks and expertise. Connecting DIOs' knowledge of commercial capabilities with the expertise of DSCA and SCOs has the potential to deliver value to partner nations.

Working with DIOs can also help DSCA identify vetted, proven capabilities critical to ensuring that partner nations acquire effective solutions and mitigating risks of deploying untrustworthy or unproven technologies. For example, the U.S. Department of Homeland Security's National Urban Security Technology Laboratory conducts market surveys and technological testing to inform local emergency response departments of the capabilities available in the commercial market. Though these are more focused on lower-end security forces, some of these capabilities could have applications for partner nations (e.g., unmanned aerial systems (UAS) for first responders, counter-UAS, counter-improvised explosive device, and protection against lasers).<sup>45</sup> The Department of Homeland Security indicates that they are willing to provide access to non-public documents for other federal agencies).<sup>46</sup>

In addition, some technology accelerators partner with DoD research organizations to technically vet members of their defense portfolios.<sup>47</sup> Because these organizations can have hundreds of companies in their programs, DSCA could identify vetted technologies more quickly by engaging with accelerator business development managers for lists of their programs.

The U. S. Department of Commerce offered to contact trade associations to discuss technology solutions on DSCA's behalf. However, due to staffing limitations and competing priorities, Commerce-driven outreach would likely need to be planned far in advance, limited in scope and frequency, and conducted in response to a clear demand from partner nations.<sup>48</sup> The Department of Commerce regularly hosts webinars and in-person events with partner governments and U.S. industry to help connect U.S. corporations to active RFPs from partner governments,<sup>49</sup> but Commerce does not collect data on U.S. corporate participation, nor does Commerce vet technologies.

---

<sup>45</sup> National Urban Security Technology Laboratory, "*Saver Technote: Laser Protective Eyewear*," U.S. Department of Homeland Security, January 2022, [https://www.dhs.gov/sites/default/files/2022-01/SAVER\\_Laser%20Protective%20Eyewear\\_TechNote\\_508%20final\\_18Jan2022.pdf](https://www.dhs.gov/sites/default/files/2022-01/SAVER_Laser%20Protective%20Eyewear_TechNote_508%20final_18Jan2022.pdf).

<sup>46</sup> U.S. Department of Homeland Security, Science and Technology, "National Urban Security Technology Laboratory," <https://www.dhs.gov/science-and-technology/national-urban-security-technology-laboratory>.

<sup>47</sup> Stakeholder at TechStars, "Interview on November 8, 2023," in-person interview by Abdullah Naimzadeh with email follow-up, November 8, 2023.

<sup>48</sup> Stakeholder at U.S. Department of Commerce, "Interview on September 13, 2023," interview by Abdullah Naimzadeh, EunRae Oh, and Matthew Reed.

<sup>49</sup> See, for example, a March 2024 webinar organized by the U.S. Department of Commerce regarding defense export opportunities in the Philippines. (Source: International Trade Administration,

### C. Barriers and Challenges to Collaboration

Scaling and sustaining collaboration between DSCA and DIOs will be difficult. The DIOs are not appropriately resourced, nor do they have a mandate, to support partner nations, most particularly those that are not part of major alliances (e.g., the North Atlantic Treaty Organization (NATO)) or partnerships (e.g., AUKUS). Individuals within DIOs expressed willingness to collaborate with DSCA on a case-by-case basis. Unless resourced and directed to support partner nations, DSCA’s collaboration with DIOs to solve problems for partner nations may be reliant on the goodwill and bandwidth of DIO team members.

Further, IDA found that there are legal and policy roadblocks to data sharing between DIOs and DSCA. For example, contractual and policy restrictions designed to safeguard proprietary and competitive industry data inhibit the transfer of technical data to other DoD organizations, creating a hesitance or inability for DIOs to provide unlimited data access to DSCA.<sup>50</sup> IDA’s research found that DIOs can instead query data sources in response to specific requests from DSCA and respond with information on capabilities that may be of interest. Relying on DIO staffs to respond to data query requests from DSCA presents limitations. Because organizations are limited in staffing and bandwidth, they may be unable to respond to individual or ad hoc requests for data, and thus there is a limit to the pace, complexity, and scale of requests. This hurdle can be mitigated by creating more targeted, specific requests to individual program managers for data. Scaling data requests is a challenge as the sheer number of DIOs may necessitate dozens, if not hundreds, of requests for DSCA to identify viable solutions for partner nations.

It is possible, however, that DIU could provide a pathway for streamlining data requests as DIU takes on responsibility for coordinating activities across DIOs and the DICE. In February 2024, DIU Director Doug Beck wrote,

Going forward, DIU will work with partners across the Department’s community of defense innovation entities—as well as with the Chief Data and Artificial Intelligence Officer (CDAO)—to take advantage of opportunities to generate impact through shared best practices, talent management, shared systems and processes, and enhanced teamwork. DIU has been charged by the Secretary and Deputy Secretary of Defense with ensuring maximum synergy—and eliminating dyssynergy—across this team.<sup>51</sup>

Outside of DIU, other organizations are reacting to the data challenge. The USD R&E developed a Transition Tracking Outcome Group to “improve the visibility and

---

“Aerospace and Defense Exporter Alert, February 2024,” U.S. Department of Commerce, February 26, 2024, <https://content.govdelivery.com/accounts/USITATRADE/bulletins/38a8c39>.)

<sup>50</sup> Stakeholder at SOF Vulcan, “Interview on September 29, 2023,” interview by Abdullah Naimzadeh, EunRae, and Matthew Reed.

<sup>51</sup> Beck, “DIU 3.0.”



management of the Department’s technology transition efforts and to enhance capability delivery to military users in the field.”<sup>52</sup> This effort, if successful, should lead to greater data access for organizations like DSCA on Departmental efforts to develop technology generally—providing insights into commercial technologies that have successfully transitioned to operational use by DoD organizations.

Finally, there are some limitations to relying exclusively on DoD sources of data on commercial technologies. Focusing data collection efforts exclusively on commercial entities who have previously worked with DoD organizations narrows the aperture and potentially overlooks more optimal solutions for partner nations. Furthermore, while there is substantially lower technical risk by focusing on DoD-vetted commercial technology, it is possible that a higher adherence to stringent DoD requirements leads to a higher cost and complexity than could be achieved from buying off-the-shelf technology. In addition, many DIOs are focused on developing technologies that may not result in prototypes (much less exportable capabilities) in the short term, thus limiting immediate relevance to partners.

---

<sup>52</sup> U.S. Department of Defense, “Transition Tracking Action Group (TTAG) Charter,” March 13, 2024, accessed September 3, 2024, <https://media.defense.gov/2024/Apr/10/2003435539/-1/-1/0/ESTABLISHMENT-OF-THE-TRANSITION-TRACKING-ACTION-GROUP-TTAG-CHARTER.PDF>.



## 4. Commercial Technologies and Capabilities

---

Stemming from its findings that DIOs are willing to assist DSCA but lack the mission and capacity to scale activities supporting partner nations today, the IDA team recalibrated its efforts to helping DSCA determine additional ways it could lead, scale, and sustain helping partner nations use commercial technologies to improve military capabilities.

Because DSCA focuses on sales and transfers of traditional materiel and systems today, the IDA team determined that a first critical step is providing DSCA a comprehensive view of commercially available capabilities that may be relevant to partners. However, commercially available capabilities will not be appropriate for all missions and tasks, and some capabilities may not be relevant to partners. Additionally, it is not feasible for DSCA to pay attention to all commercially available capabilities.

To help DSCA focus on commercially available capabilities that may be most impactful for partner nations, the IDA team developed a heatmap that shows the interplay between technologies and critical tasks (e.g., targeting, joint fires.) (see Appendix B). A heatmap is a data visualization method that offers a simple visual representation of the value or magnitude of one element's effect on another.<sup>53</sup> The heatmap developed for this project was designed to serve as a heuristic tool and framework for helping DSCA prioritize technologies and task areas for further investigation and potential development of tailored business strategies.

### A. Heatmap Methodology

To build the heatmap, the research team first created a technology taxonomy. The taxonomy draws from DoD documentation, industry reports, and academic publications to ensure inclusion of commercial technologies with military applications (i.e., dual-use). The taxonomy was reviewed by technical subject matter experts within IDA and from outside research organizations. The project team further refined the technology taxonomy by excluding technologies that failed to meet the following criteria in the context of partners:

1. **Applicability.** Technologies must be relevant to measurably improving and/or enabling a partner nations' defense and deterrence of larger aggressors.

---

<sup>53</sup> Leland Wilkinson & Michael Friendly, "The History of the Cluster Heat Map," *The American Statistician*, 63 no. 2, <https://doi.org/10.1198/tas.2009.0033>, 174–84.

2. **Sustainability.** There must be a robust or rapidly growing commercial market for the technology. For defense-unique technologies that have little to no commercial market, there must be a viable path to ensuring its continued production and sustainability. Examples include significant adoption and/or use by allied forces and/or plans by the DoD to acquire and scale the technology.
3. **Maturity.** Technologies must be technology readiness level (TRL) 7 or higher.<sup>54</sup> This indicates the technologies are no longer experimental and have, at a minimum, been successfully prototyped in a test reflective of expected operational conditions. The technology is generally ready for sale or transfer.
4. **Absorbability.** Those using the technology do not require specialized or advanced education (e.g., doctoral-level training). Training, certifications, and education on how to use the technology must be readily available (e.g., industry-provided) and generally consistent with what is commonly provided by the U.S. government to partner nations (e.g., via International Military Education and Training).<sup>55</sup>

Note, the taxonomy does not include technologies generally considered to be part of national infrastructure (e.g., telecommunications infrastructure such as fiber and 5G networks).

Next, the project team derived functional areas and associated tasks from the DoD's Universal Joint Task List (UJTL).<sup>56</sup> The project team reviewed all strategic national-level UJTJs. By process of elimination, the project team included in the heatmap only the UJTJs that could be considered applicable, or basic requirements, for any capable military (e.g., command and control, ISR, and medical care). The UJTJs from which the functional areas and tasks in the heatmap were derived are not representative of either the DoD's or partner nations' priority functional areas and tasks. The IDA team used DoD's UJTJs to help provide an organizing framework to the heatmap because the terminology and organizational structure used in the UJTJs are generally understood across the DoD. UJTJs that included highly advanced or clearly U.S.-unique tasks were excluded. Examples of excluded functional areas and tasks are those pertaining to nuclear capabilities

---

<sup>54</sup> Note that TRLs are not always used by commercial technology companies. The IDA team applied the TRL nomenclature because it is commonly used in and understood by the DoD and other government agencies. TRL 7 means that there has been a system prototype demonstration in an operational environment. (Source: U. S. Department of Defense, Office of the Executive Director for Systems Engineering and Architecture, Office of the Under Secretary of Defense for Research and Engineering, "Technology Readiness Assessment Guidebook," U.S. Department of Defense, June 2023, from <https://www.cto.mil/wp-content/uploads/2023/07/TRA-Guide-Jun2023.pdf>.)



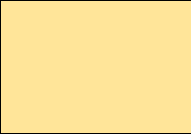

<sup>55</sup> International Military Education and Training is a program that provides U.S. government funds for international military personnel to attend educational programs and training at U.S. military facilities.

<sup>56</sup> U.S. Department of Defense, Joint Chiefs of Staff, *Universal Joint Task List*, 2024, [https://www.jcs.mil/Portals/36/Documents/Doctrine/training/ujtl\\_tasks.pdf?ver=C-PWxKHQGWo00CB3IQBhTg%3d%3d](https://www.jcs.mil/Portals/36/Documents/Doctrine/training/ujtl_tasks.pdf?ver=C-PWxKHQGWo00CB3IQBhTg%3d%3d)

and classified communications networks (e.g., the Joint Worldwide Intelligence Communications System). Appendix C provides a description of all task areas included in the heatmap.

Finally, the project team coded the impact of every technology included on the taxonomy vis-à-vis functional areas and tasks. Impact was rated on a scale of high, moderate, low, or none:

**Table 1. Impact Levels of Technologies in Taxonomy**

Impact Level	Heatmap Color	Definition	Examples & Explanation
High Impact		The technology has a proven or expected ability to provide transformational capabilities and deliver outsized returns.	The technology can render an enemy capability obsolete and/or unlock or power the ability to use additional capabilities.
Moderate Impact		The technology has a proven or expected ability to improve or optimize how a task is executed.	The technology can improve important functions in task execution. However, the technology alone may not unlock the ability to leverage additional capabilities.
Low Impact		The technology has a proven or potential utility in supporting execution of a task.	The technology may be useful to how a task is executed, but may not be required or essential.
No Impact		The technology has no discernable application or direct relevance to a task.	N/A

Evaluating impact is inherently subjective. However, to mitigate bias in the impact analysis and ensure the validity of the impact scores, the IDA team conducted literature reviews, sought input from subject matter experts, and completed multiple internal reviews of the impact scores to ensure consistency and accuracy in scoring. Literature reviews included reviewing publications such as industry analyst reports (e.g., Gartner), scientific articles and journals, and open-sourced reporting on military use of commercial technologies. (A complete list of sources consulted is provided in the bibliography.) The IDA team also collaborated with technical experts, functional experts, and former industry executives within and external to IDA to validate and adjust impact scores.

Notwithstanding the use of multiple sources to determine impact, there will always be some degree of subjectivity in the heatmap. Further, drawing hard boundaries and distinctions between technologies is difficult as they often bleed together (e.g., AI is often a core component of modern software). For these reasons, the heatmap should not be interpreted as authoritative. However, it does provide a well-formed directional view of

which technologies have the greatest potential to substantively improve or transform a partner nation's capabilities and thus informs DSCA's decisions on where to focus as it further develops strategies for delivering commercially available capabilities to partners.

## **B. Commercial Technology Trends**

One approach to evaluating which technologies can yield the highest impact is to aggregate the impact scores of each technology (e.g., numerical scoring of 3, 2, 1, and 0 for high, moderate, low, and no impact). This approach points to four technology groupings with potential to deliver significant impact across a multitude of functional areas and tasks:

1. **Compute.** This includes cloud and edge computing. The heatmap indicates cloud computing has the greatest potential impact, including high impact on multiple command, control, communications, and computer systems (C4S) and intelligence tasks.
2. **Data.** All sub-categories of data (collection, processing, analytics, visualization, and management and storage) have the potential to deliver significant impact across a multitude of functional areas and tasks.
3. **Cyber.** Security of enterprise infrastructure, as well as applications, has relevance and impact on every task included in the heatmap.
4. **AI.** The two subsets of AI that can yield the highest impact are multimodal AI and generative AI. Multimodal AI refers to AI and machine learning capabilities that can intake, process, and derive information from multiple types of data and from multiple sources (e.g., images and video ingested from different platforms). It can impact a variety of tasks, most notably ISR. Generative AI refers to AI and machine learning capabilities that can produce new data and content (e.g., text, images, or software code) in response to a prompt or tasking from a user. Generative AI is a fast-developing technology that has the potential to deliver impact across the vast majority of functional areas and tasks in the near future. Beyond the top-four technology groupings, software-defined networking may also have significant impact on some tasks, particularly C4S-related tasks. In addition, computer vision can have a large impact on intelligence-related tasks such as geospatial intelligence and ISR, and a moderate impact on a multitude of tasks pertaining to force employment, sustainment, and C4S.

There are some technologies that may not impact on or be useful to many task areas but can deliver outsized returns on specific capability areas and tasks. Not surprisingly, commercial satellite communications and commercial drones serve as useful examples. Commercial communications satellites have a proven ability to produce high impacts for C4S tasks and employment of joint fires and forces. Similarly, commercial UAVs are a

high-impact technology for targeting, ISR, and special operations (e.g., asymmetric warfare)—a finding amply demonstrated by commercial UAV use in Ukraine.<sup>57</sup>

### C. Impacts on Functional Areas and Tasks

In addition to understanding which technologies can produce the greatest impact, the heatmap offers a view into which functional areas and tasks could most benefit from using multiple commercial technologies. One task in particular has the greatest potential to benefit from integrating multiple commercial technologies together: ISR.

Multiple functional areas that can be classified as subsets or extensions of ISR also rate highly in terms of their potential to benefit from commercial technologies. Notably, measurement and signals intelligence (MASINT) and maritime warning (i.e., maritime domain awareness) can benefit significantly from commercial cloud and edge computing, data-related capabilities, cyber, and AI and machine learning. Benefits of each for ISR and ISR-related task areas follow:

- **Cloud Computing:** The ability to fuse and analyze different datasets quickly (e.g., geospatial, sensor, and open source) is essential to intelligence analysis and developing holistic operating pictures in a given domain or environment. Cloud computing’s scalability unlocks the ability to leverage significant compute power and quickly access and connect large quantities of disparate data, including by multiple dispersed teams. Finally, cloud computing enables optimal use of other commercial technologies designed within and for cloud computing environments (e.g., machine learning models, software).
- **Edge Computing:** Pushing computational power to the tactical edge can allow for faster decision-making. It also enables deployment of additional technologies into the field, such as machine learning (e.g., computer vision), including in bandwidth-constrained environments and without the need for connectivity to capital infrastructure (e.g., datacenters).
- **Cyber:** Security of ISR systems, platforms, infrastructure, and applications will be critical for resilience and data protection. Commercial cyber capabilities may not rise to the level of delivering high impact (i.e., it won’t render an enemy capability obsolete or unlock the use of additional technologies) but will be important and have applicability across virtually all ISR-related task areas.
- **AI and Machine Learning:** Most notably, computer vision and multimodal AI can deliver high impact (i.e., transformational applications) within ISR. For example, computer vision’s ability to process satellite and drone imagery enables more efficient use of human capital and (in many cases) more accurate

---

<sup>57</sup> Allen, “Across Drones, AI, and Space.”

and complete analyses of images. Multi-modal AI can intake and process multiple types and sources of data (e.g., text, image, and audio). It subsequently can produce more holistic outputs, as well as multiple types of outputs. For example, a multimodal AI that processes imagery and audio could glean insights from both, and produce text output describing what it found in both inputs.

Cloud, data, cyber, and AI can also deliver significant impact for joint C2 and information technology (IT) infrastructure. This finding highlights another angle for applying the heatmap: identifying commercially available capabilities that can be applied to multiple functional areas and therefore present the greatest potential to generate a fly-wheel effect for partner nations. For example, cloud computing acquired by a partner nation to improve Joint C2 could subsequently be applied to ISR, maintaining IT infrastructure, enterprise business systems, and more.

Commercial satellite communications, software, and integrated systems (e.g., software-defined networking) also have significant applicability and potential impact on Joint C2 and enterprise IT infrastructure. Commercial satellite constellations and communications, for example, can help provide resilience in C2 infrastructure and provide secure, reliable communications.<sup>58</sup> Integrated systems, such as software-defined networking, enable organizations to optimize their IT networks and more effectively deploy modern enterprise capabilities like cyber security, software-as-a-service, and cloud services.<sup>59 60</sup>

Finally, there's opportunity to leverage commercially available capabilities for special operations—particularly kinetic subsets of special operations, such as direct action and unconventional warfare. The greatest potential impact comes through commercial technologies that can be deployed to the tactical edge and in contested environments. Notable examples include commercial UAVs, edge computing, renewable energy, energy storage, commercial satellite communications, and sensors (e.g., biometric, infrared, and optical).

Deep dives into each task area to understand how commercial technologies can be integrated into end-to-end solutions can offer partner nations and DSCA a clear roadmap for how to build transformative capabilities using commercial technology. The heatmap looks to illustrate that although some technologies have the potential to deliver higher impacts, realizing their transformational potential within a functional area or task often

---

<sup>58</sup> See, for example, the U.S. Air Force Research Laboratory's Defense Experimentation Using Commercial Space Internet program.

<sup>59</sup> IBM, "What Is Software-defined Networking (SDN)?," accessed August 13, 2024, <https://www.ibm.com/topics/sdn>.

<sup>60</sup> Chris Christou & Michael Lundberg, "Automating Cybersecurity Using Software-Defined Networking," *United States Cybersecurity Magazine*, 2016, <https://www.uscybersecurity.net/csmag/automating-cybersecurity-using-software-defined-networking/>.



requires integrating multiple technologies and designing end-to-end solutions. For example, although commercial UAVs can highly impact ISR, the heatmap indicates that integrating commercial UAVs with cloud and edge computing; data collection, processing, and analytics; commercial communications and observation satellites; multi-modal AI and computer vision; and open-sourced software presents an opportunity to develop a truly transformational ISR capability for partner nations—evidenced by Ukraine’s own experience integrating commercial drones with mobile apps, commercial satellite communications, and more to develop ISR, targeting, and joint fires capabilities.

The right commercial technology addressing the right operational problem could offer outsized returns for partners’ militaries. However, finding that match, and executing on the procurement of a commercial technology, will take creativity, innovation, and collaboration among DSCA and multiple stakeholders. Implementing new approaches is crucial to realizing the potential outsized returns commercially available capabilities can yield for partner nations. The next chapter outlines potential new business strategies and recommendations that DSCA could adopt to incorporate commercial technology into the DoD’s security cooperation strategy.



## 5. Business Strategies and Recommendations

---

This chapter is organized as follows. First, overarching recommendations that DSCA should implement to help incorporate commercial technology into security cooperation efforts are presented in Section A (beginning on this page). The overarching recommendations are designed to have applicability regardless of which business strategy on commercially available capabilities DSCA ultimately pursues.

Next, three potential business strategies for DSCA to improve the DoD's ability to deliver commercially available capabilities to partner nations are presented. At a high level, the business strategies are:

- **Strategy #1: DIU Leads.** DSCA can champion DIU as the lead organization for receiving partner nations' requirements, identifying viable solutions from across the defense innovation community, facilitating industry engagement, and enabling procurement and delivery of commercially available capabilities to partner nations.
- **Strategy #2: DSCA-DIU Joint Model.** DIU and DSCA develop a shared strategy and delineate roles and responsibilities tailored to each organization's strengths.
- **Strategy #3: DSCA Leads.** DSCA can invest in building an internal team charged with cultivating an ecosystem of partners (government and industry), including current security cooperation implementing partners, receiving partner nations' requirements, and identifying commercially available capabilities that can address partner nations' needs. DSCA can partner with DIU and other DIOs on an ad hoc basis to identify viable solutions and deliver commercially available capabilities to partner nations.

Beginning in Section B (page 32), a description of each strategy and its strengths and weaknesses are presented. Each strategy is accompanied by recommended steps for how to implement that strategy.

### A. Overarching Recommendations

The following recommendations should be considered irrespective of the business strategy DSCA opts to pursue.

## **1. Recommendation 1: Leverage the Heatmap to Focus DSCA’s Efforts on the Technologies and/or Capability Areas of Greatest Value and Feasibility**

The heatmap highlights the wide array of commercial technologies that may have utility for a partner nation. Focusing efforts on a small number of technologies or partner nation capability areas is important for two key reasons. First, it is not feasible for DSCA and the broader security cooperation community to understand the use cases and underlying requirements of all commercial technologies. Effectively advising and assisting partner nations on adopting and deploying commercial technologies requires deep expertise and well-defined strategies. Second, resource limitations (e.g., headcount, bandwidth, technical expertise) within DSCA and other DoD stakeholders, such as the DIOs, render it impractical to develop the depth of expertise required to engage on all potential commercial technologies.

A selection of the technologies and functional areas outlined in Chapter 4 may represent the best starting point for DSCA and other stakeholders in the security cooperation community to test introducing commercial technology to partner nations and developing the learnings necessary to codify and scale the effort.

## **2. Recommendation 2: Develop a Framework for Assessing When It Is or Is not in U.S. Interests to Consider Commercial Technologies as a Solution to a Partner Nation’s Challenge**

A framework to guide decision-making and make informed tradeoffs on whether to pursue commercial technologies as a solution for partner nations will be important to ensuring alignment with U.S. strategic interests. DSCA should consider developing the framework collaboratively across the security cooperation community (e.g., military department (MILDEP) Implementing Agencies, Office of the Secretary of Defense for Policy) and with input from interagency stakeholders (e.g., Department of State, Department of Commerce).

This framework should be applied at the strategic level, but should also inform engagements at the country level. For example, SCOs will need to understand ideal conditions and non-starters for exploring commercial technology solutions with partner nations.

Critical issues and questions to examine when determining if commercial technologies should be considered include:

- status as partner of choice
  - Will acquiring U.S. commercial technology meaningfully improve or reinforce the U.S.’s status as partner of choice with a partner nation?
  - Will an acquisition of a U.S. technology replace or mitigate against usage of a PRC- or Russian-provided technology?

- urgency and speed of delivery
  - Is there an urgent requirement? If so, can a commercial solution be delivered more quickly than a military solution?
- interoperability
  - Will deploying a commercial solution enhance, undermine, or have no effect on interoperability with U.S. forces?
- cost and economics
  - Will deploying a commercial solution forego an opportunity to reduce per-unit costs of a given defense article or service for U.S. forces?
  - Will the costs of a commercial solution provide the partner nation and/or U.S. government flexibility to invest in addressing other priorities?
- proven applicability and efficacy
  - Has the DoD acquired commercial solutions to solve a similar problem?
  - Have allied nations acquired commercial solutions to solve a similar problem?
  - Will commercial solutions be used to build the partner’s conventional or asymmetric capabilities?
  - Are commercial solutions demonstrated to have greater effect vis-à-vis defense articles in a given context or use case?
  - Are there analogous use cases in the commercial sector?

### **3. Recommendation 3: Open the Aperture for Commercial Technologies to Be Considered During the Case-shaping Phase of the Security Cooperation Sales Cycle**

Prevailing guidance to partner nations (and U.S. SCOs) encourages—if not requires—countries to look for traditional solutions. Per the Security Assistance Management Manual, Letters of Request (LORs) should specify which *defense articles* or *defense services* are being requested.<sup>61</sup> A requirement that the LOR defines specific defense articles and services is reinforced in DSCA’s Foreign Customer Guide.<sup>62</sup>

Granted, LORs are required to initiate the Title 22 Foreign Military Sales (FMS) or Foreign Military Financing (FMF) grant process, which may not have applicability to

---

<sup>61</sup> Defense Security Cooperation Agency, “Figure C5.F14. Standard Letter of Request Advisory,” Accessed August 13, 2024, <https://samm.dscamilitary.com/figure/figure-c5f14>.

<sup>62</sup> DSCA, “Appendix 1—Letter of Request (LOR) Guide,” accessed August 13, 2024, <https://www.dscamilitary.com/foreign-customer-guide/appendix-1-letter-request-lor-guide>.

acquiring commercial technologies. The FMS process, however, is core to DSCA’s business and ingrained in how the security cooperation community operates. For example, it is common practice to create “pseudo cases” that apply FMS and FMF infrastructure and processes to initiate Title 10 Building Partner Capacity cases.<sup>63</sup> Further indicating how deeply rooted FMS is as the standard, during interviews with a Geographic Combatant Command (GCC), interviewees expressed concern that partner nations turning to commercial-off-the-shelf technologies was indicative of a failure of the FMS process.<sup>64</sup> Without explicit guidance and institutional knowledge on how to explore commercial technologies to solve a partner nation’s problems, the DoD is effectively closing pathways for engaging the commercial market to identify innovative solutions to problems and optimize how it builds partner capacity.

SCOs, often the first line of contact with partners, will need additional guidance, training, and resources to effectively introduce commercial technology into case-shaping activities. Though SCOs cannot favor one vendor over another, they can help partner nations analyze, understand, and document their requirements. Per the Green Book (a textbook on security cooperation activities that is published by the Defense Security Cooperation University (DSCU)), “Normally, there should be ongoing consultations between the international partner and U.S. representatives, especially the in-country U.S. Security Cooperation Organization (SCO), to assist with defining and refining requirements.”<sup>65</sup> Through this consultative process, SCOs could encourage partner nations to consider commercially available capabilities in an analysis of alternatives and be prepared to provide information on commercial technologies if of interest to the partner nation.

DSCU could provide awareness, training, or materials to SCOs regarding priority commercial technologies (e.g., those highlighted as highest impact on the heatmap). Though SCOs will not become experts in those technologies, by providing them with a baseline understanding of the technologies and their use cases, they can identify partner nation requirements and use cases for which commercially available capabilities may be an effective solution. Appendix D provides a mock-up of simple resources that could be provided to SCOs.<sup>66</sup>

---

<sup>63</sup> Derek Gilman, et al, “Foreign Military Sales & Direct Commercial Sales,” September 30, 2014, [https://www.dsca.mil/sites/default/files/final-fms-dcs\\_30\\_sep.pdf](https://www.dsca.mil/sites/default/files/final-fms-dcs_30_sep.pdf).

<sup>64</sup> Stakeholder at a Geographic Combatant Command, “Interview on August 28, 2024,” in-person interview by Jarrett Lane, August 28, 2024.

<sup>65</sup> DSCU, *The Greenbook*, chap. 5, <https://www.dscu.edu/sites/default/files/2024-08/05-chapter.pdf>.

<sup>66</sup> Note, the mock-ups include insights into non-US vendors—including Chinese—who are market leaders in a given technology. These vendors are shown only for the purposes of giving a complete picture of the commercial marketplace, including potential competitive offerings to U.S.-made technologies.

Leveraging Assessment, Monitoring, and Evaluation authorities and funds<sup>67</sup> to deploy assessment teams and Expeditionary Requirements Generation Teams (ERGTs) can provide on-the-ground support from technical experts who can inform and guide exploration of potential commercial technology solutions. For example, per DoD Directive (DoDD) 5105.65, ERGTs can be staffed with representatives of any federal agency, thereby giving DSCA the ability to deploy commercial technology experts from across the entire U.S. government for the purposes of assisting partner nations in determining requirements.<sup>68</sup>

#### **4. Recommendation 4: Use Existing Procurement Methods to Test Delivery of Commercial Technologies and Pressure-test the Need for Additional Authorities to Facilitate Timely Procurements**

Procurements must be timely, as commercial technology evolves rapidly. Laying the foundations to ensure that the procurement of commercially available capabilities is as streamlined as possible will be critical to delivering capabilities on time, and in a manner that encourages industry and partner nations alike to engage in this effort. Using existing procurement mechanisms—and thoroughly documenting suboptimal outcomes that may arise from using them to help partner nations acquire commercially available capabilities—will be essential to identifying necessary legislative, policy, and process changes.

Direct commercial sales (DCS) may be an effective mechanism for partner nations to procure commercially available capabilities. In cases where DCS is likely the procurement method of choice, the most impactful role that DoD can play—be it DSCA, DIU, or SCOs—is helping commercial industry understand partner nations’ needs and facilitating well-curated connections. Though DoD advises industry on partner nation requirements today, most companies involved in DCS are well-established defense contractors. These companies often already have significant experience in-country, as well as deep expertise in security assistance programs, FMS, and DCS processes (e.g., obtaining export licenses). Facilitating partner nations’ procurement of commercially available capabilities may require “white glove” support to companies inexperienced in this space, as well as to partner nations unaccustomed to procuring capabilities other than traditional materiel. DSCA can learn from other organizations that have adopted and scaled similar “white glove” approaches, and should engage with nontraditional industry and partner nations to understand what support would be most useful.<sup>69</sup>

---

<sup>67</sup> *Assessment, monitoring, and evaluation of programs and activities, U.S. Code 10, § 383.*

<sup>68</sup> U.S. DoD, Office of the Secretary of Defense. *DoD Directive 5105.65.*

<sup>69</sup> The Department D is experimenting with this kind of approach with nontraditional industry via a “transition concierge” which acts as “the translator between non-traditional companies and the weapons system developers.” It’s possible that DSCA could draw from lessons learned and best practices from these organizations to bridge gaps between nontraditional industry and partners. For example, see Mikayla Easley, “Pentagon Creating New Role to Break Down ‘Language Barrier’ between Non-

However, DCS are used to acquire defense articles and defense services.<sup>70</sup> By extension, the products and services acquired via the DCS process typically require export licenses.<sup>71</sup> Many commercial technologies, including those in the heatmap above, are not subject to export controls (i.e., they are classified under the Export Administration Regulations 99 category).<sup>72</sup> Therefore, even the DCS process may not be appropriate or required to help partner nations acquire commercial technologies; instead the partner nation could engage vendors and acquire technologies on the open market.

In addition to DCS, FMF may present an option for facilitating procurements, particularly for commercially available capabilities that require military modifications. FMF may be used to acquire defense articles and services through either the FMS process or, in the case of some legislatively-authorized countries, the DCS process.<sup>73</sup> It is possible that partner nations could acquire commercially available capabilities, and subsequently leverage FMF to acquire the products or services needed to conduct military modifications. For example, a partner nation could acquire a commercial unmanned system, but subsequently leverage FMF to contract for products and services to modify the system for military-unique use cases (e.g., integrating it with ISR or C2 infrastructure, improving the system's resilience against electromagnetic spectrum threats).

Using multiple procurement methods in a “hybrid case” to develop a capability can be complex and risky. Successful hybrid cases require strong lines of communication among the partner nation, industry partners, DoD stakeholders; well-defined requirements and project plans; and synchronization of procurement actions and delivery dates.

There are also limitations to how FMF may be used to acquire commercially available capabilities. Only Israel, Egypt, Jordan, Morocco, Tunisia, Turkey, Portugal, Pakistan, Yemen, and Greece are authorized to use FMF for direct commercial contracts (DCCs).<sup>74</sup> If FMF is determined to be an essential component to helping partners acquire commercially available capabilities, legislative changes to existing authorities will be

---

traditional Vendors, DoD.” Defense Scoop, December 8, 2023, <https://defensescoop.com/2023/12/08/transition-concierge-pentagon/>.

<sup>70</sup> Per Section 47 of the Arms Export Control Act, defense articles include weapons, weapons systems, munition, aircraft, vessels, boats, and implements of war.

<sup>71</sup> Defense Acquisition University. *International Acquisition—Direct Commercial Sales (DCS)*. <https://www.dau.edu/acquikipedia-article/international-acquisition-direct-commercial-sales-dcs>.

<sup>72</sup> See, for example, the Department of Commerce's advisory opinion that cloud computing service providers do not need to acquire an export license. (U.S. Department of Commerce Bureau of Industry and Security. *Advisory Opinion Regarding Cloud Computing Service Providers*, by C. Randall Pratt, 2011, <https://www.bis.doc.gov/index.php/documents/advisory-opinions/533-cloud-computing-and-deemed-exports/file>.)

<sup>73</sup> Gilman et al., “Foreign Military Sales & Direct Commercial Sales.”

<sup>74</sup> DSCA, *Guidelines for Foreign Military Financing of Direct Commercial Contracts*, 2017, [https://www.dsca.mil/sites/default/files/dsca\\_guidelines\\_for\\_foreign\\_military\\_financing\\_of\\_direct\\_commercial\\_contracts\\_updatedfinal.pdf](https://www.dsca.mil/sites/default/files/dsca_guidelines_for_foreign_military_financing_of_direct_commercial_contracts_updatedfinal.pdf).



required (as well as alignment with the Department of State) to open the aperture for additional partner nations to leverage FMF for DCCs.

## **5. Recommendation 5: Develop a Total Package Approach and Map Technology Requirements**

Sales of military equipment, often include extensive analysis and documentation of the totality of what is required for a partner nation to effectively deploy, maintain, and sustain a capability. Ample documentation exists (e.g., checklists) to help partner nations articulate the full scope of support, ancillary equipment, etc. they will need as part of a given acquisition. For example, the U.S. Air Force publishes a “Fighter FMS Checklist” to guide LOR development. The checklist includes entries ranging from mission profiles (e.g., aerial refueling, targeting, air-to-air), to training requirements, to testing and certification.<sup>75</sup>

Helping partner nations effectively deploy and maximize the impact of commercial technologies on their ability to execute critical tasks will require a similarly holistic approach to mapping-out requirements. For example, if a partner nation aims to leverage commercial data analytics products, it is critical to understand whether the partner has the underlying compute infrastructure, data collection, data storage, and data management capabilities necessary to glean value out of an analytics capability in the first place. Building a repository of collateral such as discovery questions, checklists, and exemplar systems architectures will help all stakeholders—both partner nation and U.S.—identify gaps and develop a comprehensive strategy to ensure effective deployment of commercial technologies.

## **6. Recommendation 6: Conduct Pilot Projects with DIU.**

To help DSCA determine the optimal business strategy, IDA recommends first conducting a pilot project (or series of pilot projects) with DIU. This will enable DSCA to get insights into how it can best partner with DIU to deliver high-impact results for partner nations and ultimately determine the best business strategy going forward. A pilot project will also allow DSCA to test how engagement and procurement models typically employed by DIU could be used to address partner nation needs.

Scoping the pilot project to a proactive use case rather than a response to acute needs in conflict will enable DSCA to pressure-test how to best incorporate commercially available capabilities into security assistance packages and long-term security cooperation strategies. The pilot project could be structured into two parts: the first being requirements generation (e.g., needs discovery, problem statement development, solicitation release) in

---

<sup>75</sup> Air Force Security Assistance & Cooperation Directorate, *Foreign Military Sales (FMS) Checklist for Developing Acquisition of Fighter Aircraft Letter of Request (LOR)*, <https://afsac.wpafb.af.mil/resources/lor/USAF-Fighter-Aircraft-Checklist.pdf>.

partnership with DIU, and the second (pending successful outcomes from the first) being identification of viable solutions for a partner nation.<sup>76</sup>

Assessment, Monitoring, and Evaluation funds could be used during the first phase of the pilot project to field ERGTs to work with the partner nation to assess requirements and viable opportunities to leverage commercial technologies. The ERGTs should include DIU and, if additive, experts from other offices and federal agencies with expertise in commercial technology. Fielding an ERGT may not only help ensure the success of the pilot project, but will allow DSCA to test whether and how ERGTs could be fielded post-pilot project as a resource to partner nations and SCOs in identifying ways commercial technologies can address critical needs.

DSCA should consider selecting a technology or task area that is low-risk and for which there is deep institutional knowledge—both within the DoD and industry—for how to design and implement solutions. For example, distribution and logistics may be a strong candidate. DSCA might also focus attention on an underdeveloped, but important, capability area that is expected to be a future priority for partners.

Finally, identifying ideal partners with whom to conduct a pilot project is important. Potential criteria for partners on which to focus include partners' expressed interest or demand for commercial technologies, partner nations' resourcing and ability to conduct a commercial acquisition, and technical competence and skills of the partner nation.

Informed by learnings from pilot projects, there are multiple strategies that DSCA could pursue from implementing and scaling new approaches to incorporating commercial technology into security cooperation with partners. The IDA team developed three potential strategies and recommended steps for implementing each. The strategies and associated steps for implementation are outlined in sections B, C, and D of this chapter.). A summary table of all recommendations is provided in Appendix E.

## **B. Strategy #1: Implement a DIU-Led Approach**

The first strategy presented is one in which DIU is the lead implementing agency on all commercial technology cases. In this model, DSCA would delegate responsibility to DIU for leading interaction with partner nations interested in acquiring commercially available capabilities, understanding partner nations' requirements, and serving as the primary interlocutor between partner nations and commercial industry to identify viable solutions. A DIU-led approach constitutes a formal expansion of DIU's mission and

---

<sup>76</sup> In some cases, DSCA and the larger security cooperation community may need to do some groundwork with certain partners so that they might understand the relevance of a class of technologies to the partner's security imperatives. Simply pointing out a set of solutions may not be effective for a partner who lacks an understanding of the potential opportunity space.

portfolio. DSCA would provide oversight to DIU's activities with partner nations akin to the MILDEPs.<sup>77</sup>

Benefits of leaning on DIU as the lead organization include leveraging its preexisting knowledge and expertise in cultivating ecosystems of commercial technology providers, identifying and vetting commercially available capabilities, and conducting business in a relatively expeditious manner.

Downsides of a DIU-led approach, however, are that DIU lacks resident expertise in security cooperation to include relevant authorities and approaches. DIU is also continuing to refine its approach to effectively serve U.S. warfighters; it is not clear whether DIU's model can effectively translate and scale to directly support partner nations, which come with varied strategic contexts, operational cultures, and technical levels of expertise.

Further, DIU is principally focused on solving operational and tactical problems. It is not well-versed in enterprise-level technology investments and infrastructure technologies, like cloud computing, that could have very high impact on partner nations' ability to leverage other technologies and execute critical tasks. Focusing on operational and tactical problems is a viable approach, but opting for this approach should be done cognizant of the tradeoff to leave other technologies and capability areas effectively unaddressed.

## **1. Steps for Implementing a DIU-Led Approach**

The following recommendations should be considered if DSCA opts to develop a DIU-led approach to incorporating commercially available capabilities into security cooperation activities.

### **a. Advocate for DIU to Receive a Mandate, Headcount, Resourcing, and Support to Build a Team and Portfolio Focused on Partner Nations**

Unless DIU receives a mandate and resources, DIU's ability to support partner nations will be limited to ad hoc activity based on bandwidth (and willingness) of their team to engage. Should DIU be provided additional personnel for this effort, it is critical that they are trained through DSCU on security cooperation authorities, policies, and procedures to help ensure DIU engages with partner nations appropriately. Sufficient personnel and resources will be required to support the full sales cycle, including activities typically considered "pre-LOR" (e.g., security cooperation assessments and collaborative engagements with partner nations to define requirements) through facilitating acquisition, delivery, and partner nation adoption of a given capability.

---

<sup>77</sup> DoD, Office of the Secretary of Defense. *DoD Directive 5105.65*.

**b. Update Policies to Establish DIU’s Role Akin to a MILDEP in the Security Cooperation Apparatus**

Policies such as DoDD 5105.65 and DoDD 5132.03 should be updated to formalize DIU’s role in the DoD’s security cooperation apparatus.<sup>78</sup> Like the MILDEPs, DIU’s role should be aligned to supporting Combatant Commanders and supporting security cooperation assessments to identify viable solutions for partner nations. Because DIU is not oriented around programs of record or procuring defense articles, policies should be updated to reflect DIU’s role in identifying and facilitating partner nation procurement of commercial technology.

**c. Incorporate DIU into the Security Cooperation Steering Group**

Per DoDD 5105.65, DSCA is responsible for providing oversight and direction to other DoD components regarding the execution of security cooperation programs.<sup>79</sup> Incorporating DIU into the Security Cooperation Steering Group would help align DIU’s activities with partner nations to strategic imperatives (e.g., prioritizing capability-building with certain countries or for certain missions).

**d. Establish a Framework and Mechanisms for how Partner Nations and/or SCOs Can Reach Directly to DIU to Explore the Applicability of Commercial Solutions for a Given Use Case and Define Requirements**

Consistent with the role of MILDEPs in supporting security cooperation assessments, DIU should serve as a resource to Combatant Commanders and, by extension, SCOs. In circumstances in which a partner nation expresses interest in commercial solutions, or in cases in which the Combatant Commander and/or SCO believe commercial solutions may be appropriate for a partner nation’s needs, DIU should be called on to support an assessment and/or engage with the partner nation to understand their problems and help define requirements.

DIU personnel in Combatant Commands could serve as the primary point of contact to provide reach-back support to SCOs and help evaluate the potential for commercial technology to solve a partner nations’ problem. By understanding partner nations’ problems, operational constraints, affordability targets, desired delivery schedule, training requirements, and other relevant considerations, DIU can most effectively engage commercial industry to identify viable solutions.

**e. Leverage DIU’s Existing Commercial Solutions Opening (CSO) Process to Post Problem Statements on Behalf of Partner Nations, Receive Proposals,**

---

<sup>78</sup> DoD, Office of the Secretary of Defense. *DoD Directive 5132.03*.

<sup>79</sup> DoD, Office of the Secretary of Defense. *DoD Directive 5105.65*.

## **Vet Potential Solutions, and Introduce Partner Nations to a Selection of Companies and Capabilities.**

When a partner nation is interested in acquiring commercially available capabilities, DIU should leverage its existing platform and processes for posting CSOs to solicit proposals and identify potential solutions available in the commercial market. The CSOs should be focused on identifying capabilities rated TRL7 or higher.

Pending the CSOs identifying viable solutions, DIU should coordinate with DSCA, Combatant Commander, SCOs, and the Defense Technology Security Administration to present solutions to partner nations. Except in cases in which only one company produces a given product, it is critical that neither DIU nor other DoD stakeholders advocate for a partner nation to acquire one solution over another. Instead, DIU should facilitate introductions between the commercial companies and partner nation; the partner nation can then initiate a DCC for their solution of choice.

### **C. Strategy #2: Implement a Joint DSCA-DIU Approach**

The second strategy IDA developed for DSCA's consideration is one in which DSCA and DIU create a joint strategy and framework for identifying and delivering commercially available capabilities to partner nations. This strategy would constitute DSCA owning some commercial technology cases with partner nations (e.g., largescale, enterprise-level commercial technology acquisitions), and DIU owning cases of a different nature—particularly tactical applications and fast-moving procurements.

Implementing this strategy would require (at a minimum) delineation of responsibilities, allocation and alignment of resources and personnel, and clarity on how to best leverage both organizations' respective strengths. A key benefit of a joint approach is that it allows DSCA to leverage DIU's existing ecosystem of commercial industry partners and expertise on commercially available capabilities. An anticipated challenge, however, is that DSCA and DIU operate with significantly different business models. Aligning processes and even team cultures may be difficult.

#### **1. Steps for Implementing a Joint DSCA-DIU Approach**

The following steps should be considered if DSCA opts to develop a joint approach with DIU to incorporating commercially available capabilities into security cooperation activities. The following steps offer just one potential way to implement a joint DSCA-DIU approach; multiple permutations of a joint approach may be possible.

**a. Develop a Framework that Leverages and Aligns DSCA and DIU’s Respective Strengths and Unique Capabilities**

DSCA’s expertise in security cooperation policies, programs, authorities, and strategies will be critical to delivering innovative solutions to partner nations. Additionally, DSCA’s network of SCOs have unique insights into partner nations’ problems, strengths, and limiting factors. DSCA also has experience navigating geopolitical complexities inherent in security cooperation, as well as implementing long-term strategic initiatives to build partner nation capabilities and capacity.

On the other hand, DIU has a significant network of innovative commercial companies and well-established visibility into the commercial market. DIU is also staffed by technical experts who understand commercial technologies and trade-offs that must be considered when making commercial technology acquisitions. Finally, DIU is purpose-built to quickly find viable solutions to U.S. warfighters’ challenges; it has begun sharing its approach for doing so with partner nations (e.g., Ukraine) through workshops and other forums.<sup>80</sup> However, as articulated in Section B (page 32), DIU lacks the experience, expertise, resources, and mandate to lead enduring activities supporting partner nations.

Given these factors, DSCA should consider a framework in which it serves as the primary coordinator when commercially available capabilities are of interest to a partner nation, and DIU serves in a support and/or advisory role when requested by DSCA.

Additionally, DSCA should lead on long-term, strategic engagements with partner nations, while DIU leads on tactical and urgent solutioning. For example, if a partner nation is interested in acquiring enterprise-level technologies (e.g., commercial cloud infrastructure) or undertaking a transformative initiative with commercial technology, DSCA would serve as the lead organization for helping the partner nation. Conversely, if a partner nation requires urgent assistance (e.g., in response to conflict or disaster) or needs solutions for a tactical-level challenge, DIU would serve as the lead organization for identifying viable solutions.

**b. Build a Small-footprint Team (2-3 Headcount) within DSCA Responsible for Cultivating and Facilitating Engagements Between Industry and Partner Nations Focused on Strategic or Long-term Commercial Technology Applications**

This team would focus exclusively on facilitating strategic or enterprise-level technology investments by partner nations, such as cloud acquisition or architecting systems and end-to-end solutions for critical mission areas (e.g., ISR). This team should

---

<sup>80</sup> Defense Innovation Unit, “DIU Hosts Ukraine and the Future of Unmanned Aerial Systems Forum in Warsaw,” accessed August 13, 2024, <https://www.diu.mil/latest/diu-hosts-ukraine-and-the-future-of-unmanned-aerial-systems-forum-in-warsaw>.

serve a convening role to pull in experts from across government and the DoD (e.g., DoD Chief Information Officer and DIU), industry, and partner nations to understand requirements, identify viable solutions, and craft strategies to help partner nations acquire necessary capabilities.

**c. Create a Process through Which DSCA Determines if and when to Request DIU's Assistance when Partner Nations Express Interest in Commercially Available Capabilities**

A joint DSCA-DIU could entail DSCA serving as the primary conduit for determining if and when a given use case or partner nation requirement necessitates DIU's involvement. For example, when a partner nation expresses an interest in commercially available capabilities, the SCO will relay that information to DSCA. DSCA, in coordination with relevant regional policy desks, the GCC, and other stakeholders as appropriate, can then assess whether it is in the DoD's strategic interests to explore solutions outside of programs of record and traditional materiel before bringing the case to DIU for assistance.

This arrangement offers two potential advantages over allowing SCOs to go directly to DIU. First, it can help ensure alignment with overarching strategic priorities. There is some risk that decentralization of decision-making on when it is appropriate to explore commercially available capabilities could result in disjointed approaches and a proliferation of fielded commercial capabilities that lack interoperability or operational cohesion. Second, positioning DSCA to receive demand signals for commercially available capabilities can help mitigate against both resistance to, and over-indexing toward, commercial technology.

**d. Leverage DIU's Existing CSO Process to Post Problem Statements on Behalf of Partner Nations, Receive Proposals, and Vet Potential Solutions**

When a partner nation is interested in acquiring commercially available capabilities, DSCA and DIU should leverage DIU's existing platform and processes for posting CSOs to solicit proposals and identify potential solutions available in the commercial market. The CSOs should be focused on identifying capabilities rated TRL7 or higher.

**e. Detail DSCA Employees and/or Experienced SCOs to DIU. Detailees Should Serve as Liaisons and Assist DIU in Developing New Portfolios and Processes**

Personnel detailed to DIU should possess expertise in security cooperation processes, best practices, and key policies and regulations (e.g., export controls). Detailees will coordinate closely with DSCA and tap DIU's technical expertise to help craft portfolios tailored to supporting certain partner nations and/or priority mission areas.

Though details are often viewed as a resource drain on the organization from which the detailee originated, in this case they present an opportunity for DSCA to learn and mature its own understanding of commercial industry. Detailees embedded at DIU can help DSCA learn best practices and strategies for engaging commercial industry to identify and deliver innovative solutions to international partners. Further, detailees may offer a pathway to DSCA leveraging DIU’s market intelligence capabilities and gaining insights into DIU’s ecosystem of commercial industry partners.<sup>81</sup>

**f. Coordinate with DIU to Leverage the Intergovernmental Personnel Act (IPA) to Embed Security Cooperation Experts within DIU**

DIU leverages IPA exchanges to attract technical talent and support DIU portfolios.<sup>82</sup> The IPA allows for exchanges of personnel from “other organizations” to a federal agency. “Other organizations” include nonprofits and federally funded research and development centers.<sup>83</sup> DSCA can coordinate with DIU to identify security cooperation experts from eligible organizations to augment the DIU team and help build portfolios tailored to delivering solutions for partner nations. This is not an enduring solution, but may be a way to augment the DIU team and alleviate personnel constraints on DSCA.

**D. Strategy #3: Implement a DSCA-Led Approach**

The third strategy IDA developed for DSCA’s consideration is one in which DSCA leads and drives the process of incorporating commercial technologies into security cooperation activities. This strategy would likely be the most resource-intensive because DSCA would need to build an organic capability from the ground-up. The benefit of this approach, however, is that DSCA can ensure there is alignment between its enterprise-level strategic imperatives and the approach of a newly created team focused on delivering commercially available capabilities to partner nations.

Should DSCA pursue this strategy, IDA recommends doing so over a three-phase approach:

1. Market Validation and Fit
2. Preparation and Launch
3. Execute and Scale

---

<sup>81</sup> For guidance and existing policy on detailing personnel, see DoDI 1100.23, "Detail of Personnel to OSD," September 26, 2012; Incorporating Change 1 on June 1, 2020 (whs.mil) and the Technology Transformation Services (TTS) Handbook’s instructions on “Details to Other Agencies” published by the U.S. General Services Administration.

<sup>82</sup> Defense Innovation Unit, “Careers,” accessed August 13, 2024, <https://www.diu.mil/careers>.

<sup>83</sup> *Temporary Assignments Under the Intergovernmental Personnel Act (IPA)*, U.S. Code 5 (1970), § 3371.



The following sections describe all three phases, as well as specific recommendations for steps DSCA should take in executing each.

## **1. Steps for Phase 1: Market Validation and Fit**

Engaging both industry and partner nations to understand their perspectives on strengths, weaknesses, opportunities, and threats associated with procuring commercially available capabilities will be critical to decision-making by DSCA's leadership, development of new strategies, and data-driven investments in new resources and capabilities within DSCA. For example, some industry partners may not be familiar with the arms export space and may need assistance to navigate U.S. and partner nation processes.

### **a. Define DSCA's Value Proposition in Enabling Sales of Commercially Available Capabilities to Partner Nations**

DIOs, like the DIU, attract companies into their ecosystem, in part, because of funding and authorities to make contractual awards, including under streamlined commercial terms (e.g., other transaction authorities). In short, they have capital, the ability to spend it, and the ability to do so quickly. This combination is attractive to innovative commercial companies that are unable or unwilling to enter contracts with Federal Acquisition Regulation (FAR) and Defense Federal Acquisition Regulation Supplement (DFARS) requirements, or navigate lengthy acquisition and procurement processes.

DSCA needs to clearly define and articulate the value it brings to commercial transactions between industry and partner nations. As a starting point, IDA identified three potential benefits DSCA can offer to industry and partner nations:

- 1. Customer discovery and requirements generation.** DSCA can leverage deep relationships with partner nations and help partner nations develop commercial technology procurement strategies and roadmaps, informed by known and anticipated challenges and requirements.
- 2. Convening power and network effects.** DSCA's deep relationships with partner nations and key interagency partners (e.g., Department of Commerce and Department of State) may be compelling to industry partners interested in international sales and military applications of their technologies.
- 3. Access to funding.** It is possible that FMF could be used to facilitate DCCs of in-scope technologies. As noted previously, only Israel, Egypt, Jordan, Morocco, Tunisia, Turkey, Portugal, Pakistan, Yemen, and Greece can use FMF for DCCs today. Expanding the list of countries will require new authorities. Because FMF funds are often limited, non-recurring, and unpredictable year-over-year, they are not always a good option for sustainment or scaling adoption

of a given technology. For example, FMF may not be a good solution for recurring annual costs of cloud services. FMF may be useful for developing proofs of concept and pilot projects or for acquiring items for which there is little to no sustainment cost. Further, companies paid via FMF for DCCs must meet eligibility criteria, including ensuring that subcontractors and suppliers are not “excluded from conducting business with federal programs” and have export privileges.<sup>84</sup>

**b. Validate Advantages and Willingness among Supply-side (Industry) and Demand-side (Partner Nation) Stakeholders for DSCA to Facilitate Procurements of Commercially Available Solutions**

DSCA should conduct private interviews and roundtable discussions to develop a holistic understanding of the concerns, objectives, and needs of potential supply-side stakeholders. Industry outreach should include a mix of companies by size, as well as experience in defense and international sales, to ensure DSCA develops a holistic understanding of potential supply-side stakeholders’ concerns, objectives, and needs. Some questions to explore with companies include:

- Are companies interested in selling to partners? Why or why not?
- Do companies have experience selling to partners? If so, what do they see as the greatest opportunities and challenges?
- What concerns do companies have about providing partner nations capabilities specifically for counter-PRC or counter-Russia strategies? (E.g., Are they concerned about other lines of business with PRC being impacted, or their company being targeted for cyberattacks and intellectual property theft by PRC and Russia?)
- What does industry need from DSCA for a new business strategy to be effective?
- What are companies’ preferred contracting and procurement mechanisms for delivering commercial capabilities to international partners?

DSCA should also leverage in-house market analysis and lessons from ongoing engagements and work with partners to validate their interest and ability to procure, use, and sustain commercially available technologies.

- Are partner nations using commercially available capabilities today? If so, how? If not, why?

---

<sup>84</sup> DSCA, *Guidelines for Foreign Military Financing*.

- Are partner nations interested in acquiring and incorporating commercially available capabilities into their operations? Do they have a strategy and plan for doing so?
- Do partner nations' own interests and priorities for acquiring commercially available capabilities align with DSCA's perspective on which capabilities could yield the greatest impact?
- What are partner nations' preferred contracting and procurement mechanisms for commercially available capabilities (e.g., direct commercial contracts, FMF)?

Through these engagements, DSCA can evaluate potential market size and gather data needed to craft tailored business strategies for specific commercially-available capabilities.

## **2. Steps for Phase 2: Preparation and Launch**

If Phase 1 indicates strategic feasibility and demand for DSCA to provide commercially available capabilities, DSCA should invest in the foundational resources and capabilities needed to develop and execute new business and go-to-market strategies. This may require additional appropriation and authority from Congress.

### **a. Establish a Dedicated Team Focused on Cultivating and Facilitating Need-driven Engagements between Industry and Partner Nations**

This team should be responsible for cultivating strategic partnerships inside the DoD and with industry and for working with SCOs and partner nations to determine needs and facilitate targeted engagements between partner nations and potential sources of commercially available capabilities. The team should have technical expertise and competencies in priority technologies and/or capability areas. By staffing the team with technical experts, DSCA can more effectively:

- facilitate customer discovery with partner nations to ensure thorough evaluation of how commercially available capabilities may or may not be applied to a given use case,
- validate the relevance and efficacy of a technology to solving a given problem for partners,
- understand interdependencies and systems architecture requirements, and
- identify risks associated with the deployment of a given technology.

**b. Enhance DSCA’s Market Intelligence on Capabilities and/or Technologies of Greatest Potential Impact**

Current market intelligence is critical to staying abreast of key innovations and market trends, understanding companies’ offerings, and identifying new commercially available capabilities that may address partner nations’ needs. DSCA could take the following steps to develop market intelligence:

**1) Leverage DSCA’s Strategic Outreach Division to Coordinate and Execute a Campaign to Educate Commercial Technology Providers on DSCA’s Mission, Establish Relationships, and Build DSCA’s Brand Awareness**

Send demand signals to industry by publishing DSCA’s technology priorities, and create mechanisms through which industry can reach DSCA to share information on their products and offerings. This is analogous to a venture capital group’s investment thesis, a practice used by other organizations within the DoD like the DIU. The technologies priorities can be informed by the heatmap and refined through information gathered during pilot projects and Phase 1 of this strategy.

DSCA should also deploy leaders and a team focused on commercially available capabilities to industry events; coordinate briefings, roundtables, and webinars to educate industry on DSCA and its priorities; and develop resources and learning opportunities for both industry and partner nations to understand how they can work with DSCA to sell and procure commercially available capabilities.

**2) Establish an Advisory Board of Industry Partners Who Can Advise and Assist in Deployment of Commercially Available Capabilities to Partner Nations**

DSCA can serve as a convener between industry and partner nations to facilitate customer discovery, systems architecture design, and procurements. An advisory board would need to be conducted in accordance with appropriate laws and regulations, such as the Federal Advisory Committee Act and 5 C.F.R Sections 2635.101 and 2635.501-503.<sup>85</sup> Further, board members should have expertise and/or represent organizations that provide products and services within DSCA’s technology and functional areas of focus. Sustaining and extracting value out of this board will require consistent engagement and maintenance by DSCA. Doing so will require aligning personnel to owning and cultivating relationships with members, as well as ensuring the membership is kept “fresh” (i.e., the best possible companies are represented and actively participating).

---

<sup>85</sup> *Standards of Ethical Conduct for Employees of the Executive Branch, Code of Federal Regulations 5, (1992) Part 2635.*

By using a board to cultivate speculative relationships with U.S. companies and interested partner nations, DSCA will position itself to share the needs and potential market size of partner nations directly with U.S. companies. In turn, this information may influence companies' product roadmaps and ability to innovate on capabilities, features, and functionalities that maximize applicability of a given technology to partner nations' most pressing needs.

### **3) Subscribe to Publicly Available Market Intelligence Platforms and Databases**

Acquiring access to commercial market intelligence platforms and databases can accelerate DSCA's visibility into technologies, companies, and industry trends. Venture capital firms and companies frequently leverage Gartner, Pitchbook, Crunchbase, AlphaSights, and others to handle data collection, integration, analysis, and market intelligence report production.

### **4) Partner with DIOs and Interagency Offices that Have Established Market Intelligence Capabilities and Procurement Strategies Focused on Commercially Available Capabilities**

Establish relationships with DIOs and other interagency offices through which DSCA can submit targeted queries to identify commercially available capabilities that may meet partner nations' requirements. As noted earlier, DIU's interest in generating "impact through shared best practices, talent management, shared systems and processes, and enhanced teamwork" has potential to position DIU as an effective information aggregator and help streamline query requests for DSCA.<sup>86</sup>

### **5) Support and Engage with Broader DoD Efforts to Improve Data Visibility and Data Standards for Innovation Outreach and Transition Outcomes**

DSCA has the potential to benefit from new DoD-wide efforts like the Transition Tracking Action Group (TTAG)<sup>87</sup>, which aims to "improve the visibility and management of the Departments technology transition efforts"<sup>88</sup> DSCA, through USD Policy's involvement on the TTAG, could advocate for the creation of data sources releasable to select partner nations and, when advantageous or appropriate, grant partner nations greater visibility into existing DoD experiments with commercial technology. At a minimum,

---

<sup>86</sup> Beck, "DIU 3.0."

<sup>87</sup> U.S. Department of Defense, "Department of Defense Enhances Technology Transitions Through New Advisory Group," April 10, 2024, accessed August 13, 2014, <https://www.defense.gov/News/Releases/Release/Article/3736929/department-of-defense-enhances-technology-transitions-through-new-advisory-group/>.

<sup>88</sup> DoD, "Transition Tracking Action Group (TTAG) Charter."

Policy should advocate for data being sharable to DSCA could help ensure that Security Cooperation Officers understand the range of potential commercial technologies in search of transition partners.

### **3. Steps for Phase 3: Execute and Scale**

#### **a. Conduct Engagements with Partner Nations that Can Elucidate how They May Apply Commercial Technologies in New Ways**

The heatmap reflects a U.S.-centric perspective of technology impact. Further, constant technological evolution and innovation may result in unforeseen applications of commercially available capabilities. Incorporating commercial technologies into exercises and wargames with partner nations will stimulate new ideas on ways to apply technologies and illuminate how partner nations can best harness them to execute critical tasks. With additional training and guidance, SCOs should also be prepped to engage with partner nations on ways that commercially available technologies can meet their requirements and priorities.

#### **b. Proactively Field Assessment Teams to Apply the Heatmap Framework to Specific Partner Nations and/or Identify Opportunities for Commercially Available Capabilities to Improve Partner Nations' Abilities to Execute Critical Tasks**

The heatmap presented in this report was developed without grounding or insights into how specific partner nations are currently using commercial technologies or executing critical tasks. Fielding assessment teams with combined expertise in commercial technologies, systems architectures, and priority task areas can produce data-driven insights into opportunities and risks associated with incorporating commercially available technologies into how partners execute priority tasks. DSCA in-house foreign market intelligence capabilities may provide initial insights on current and likely future partner demands. Assessment, Monitoring and Evaluation funds could be used to field these teams.<sup>89</sup>

#### **c. Collaborate with Partner Nations and Industry to Develop Tailored Strategies and Roadmaps for Effective Commercial Technology Deployment, Including Building End-to-end Solutions and Transformative Capabilities**

Technologies are often reliant on one another; helping partner nations incorporate commercially available capabilities into their operations requires a holistic understanding of interplay and interdependencies of technologies. Additionally, the means by which one

---

<sup>89</sup> *Assessment, Monitoring, and Evaluation of Programs and Activities, U.S. Code 10, § 383.*

commercially available capability is best delivered may not be the same means by which another is delivered. Strategies should reflect unique timelines, contractual mechanisms, upfront costs, and long-term costs associated with acquiring a given technology or solution. As noted previously, some partners may need assistance in recognizing the opportunities through commercially available military capabilities and the demands of absorbing, applying, and sustaining procured solutions.





## 6. Additional Considerations and Research

---

Other factors not explored in this study warrant examination, as they may impact the viability and efficacy of DSCA helping partner nations acquire and incorporate commercially available capabilities into their operations. Potential areas of continued research include:

- **Resourcing.** Assuming direct commercial sales are the primary means through which a partner nation ultimately acquires commercial technologies (i.e., DSCA does not collect administrative fees), DoD Operations and Maintenance funds may be required to cover or augment the costs of dedicated teams and their activities.
- **Export controls.** Some technologies in the heatmap, including those that could significantly improve partner nations' capabilities, are subject to export controls.<sup>90</sup> It will be critical for DSCA to carefully study priority technologies to understand blockers, pathways, and requirements for helping partner nations acquire U.S.-produced technologies that fall under export control restrictions. Interagency coordination and collaboration will likely be a core component of overcoming export-related blockers (and more). Additionally, for solutions that require a military modification to a commercially available capability, DSCA should consider processes to facilitate partner nations acquiring the baseline product and subsequently completing military modifications locally.
- **Foreign Ownership, Control, or Influence (FOCI) vetting.** FOCI is a significant and growing concern.<sup>91</sup> Vetting commercial companies to determine if a foreign power—particularly adversarial actors—has the ability to influence or direct companies' performance will be important to ensuring partner nations acquire safe, secure, and reliable capabilities. Effectively vetting companies for FOCI and making informed judgements about the risks they pose will likely require expertise and support from agencies like the Defense Counterintelligence and Security Agency.

---

<sup>90</sup> U.S. Department of Commerce, Bureau of Industry and Security, *Export Administration Regulations*, <https://www.bis.gov/ear>

<sup>91</sup> U.S. Library of Congress, Congressional Research Service, *Department of Defense Contractors and Efforts to Mitigate Foreign Influence*, by Alexandra G. Neenan, R48110 (2024), 1.

- **Partner nations’ culture of innovation and absorptive capacity.** Further research should develop an assessment framework to understand partner nations’ culture of innovation and their ability to effectively and creatively use commercial technologies. This research should not necessarily be limited to partner nations’ militaries and security forces; it should look at civilian agencies, civil society, and native industry—all of which would be called upon for national defense in the event of conflict with PRC or Russia. An assessment framework can help mitigate against over indexing on lessons learned from Ukraine as DSCA develops strategies for helping partner nations acquire and use commercial technologies. Ukraine’s ability to innovate with commercial technologies may be due, in large part, to country’s robust IT industry and sizeable technical workforce.<sup>92</sup> The same may not be true for other partner nations.
- **Competitive market intelligence.** For many commercial technologies, comparable products and solutions are produced by adversarial actors and made readily available on the market. For example, Chinese companies figure prominently in the global market for commercial drones, cloud, and artificial intelligence. There is a risk that the DoD could help partner nations identify ways to use commercial technologies, only for the partner nation to subsequently acquire a comparable, better, or cheaper solution from an adversarial provider. Having deep insights into the competitive landscape such that requirements can be shaped and conditions set for U.S. technology providers to be favored will be important.
- **SCO capabilities and capacity.** This report highlights how SCOs will need to be trained and supported if they are to effectively introduce commercial capabilities for consideration among partner nations. It is possible that this task is too complex for most SCOs, at least near-term. Further research should go into understanding potential ways the GCCs and Combatant Commands may be

---

<sup>92</sup> By some estimates, Ukraine’s IT workforce totals 285,000 specialists who generate 4% of the national GDP (~\$6.8B). Of that population, many are in the armed forces or work in national cyber defense. (Boris Kontsevoi, “*The Ukrainian IT Industry Is Alive and Healthy*,” *Forbes*, October 12, 2022; <https://www.forbes.com/sites/forbestechcouncil/2022/10/12/the-ukrainian-it-industry-is-alive-and-healthy/?sh=5dd8f2d67f2c>; Huileng Tan, “Ukraine’s 285,000 IT Specialists Power Apps and Software Around the Globe, and Many of Them Are Still Working from Ukraine as the War Rages around Them,” *Business Insider*, April 8, 2022, <https://www.businessinsider.com/ukraine-it-specialists-still-working-through-war-2022-4>.)

able to minimize the burden on SCOs and help introduce commercially available capabilities to partner nations.

- **DSCA's and SCOs' culture of innovation.** The DoD is cultivating new approaches, mindsets, and human capital strategies for considering problems, engaging industry, innovating rapidly, attracting technical talent, and more. To help partner nations leverage commercially available capabilities, the cultural shifts the DoD is cultivating in the defense acquisition community will need to extend to DSCA and SCOs.
- **Risk mitigation.** Prior to encouraging or facilitating a sale, DSCA should have a well-informed understanding of how commercially available capabilities could be used by partner nations and the potential risks of such use.



## 7. Conclusion

---

Commercial technologies present significant opportunities for helping partner nations improve capabilities. Partner nations' execution of ISR, maritime domain awareness, Joint C2, and other critical missions can be modernized, if not transformed, by commercial technologies. The array of commercial technologies that may be beneficial to partner nations is vast. Leveraging tools and market intelligence, like the heatmap presented in this paper, can help DSCA and the broader security cooperation community focus efforts on the most impactful technologies for the highest priority tasks.

Though commercial technologies present great opportunity, multiple challenges will need to be overcome to effectively incorporate commercially -available capabilities into DoD's security cooperation strategy and ultimately deliver innovative capabilities to partners. Policies, personnel, and resources will need to be aligned to a new business strategy—one that introduces significant changes to how potential solutions to capability gaps are explored with partner nations. Doing so will take time, investment, focus, and dedication, but has the potential to yield significant strategic and operational benefits to the U.S. and partner nations.



## **Appendix A. DIOs Interviewed**

---

### Formal DIOs

- Air Force CyberWorx
- Big Safari
- Catalyst Accelerator\* (U.S. Air Force Sponsored)
- DEFENSEWERX
- Department of the Air Force AI Accelerator
- Griffiss Institute
- Irregular Warfare Technical Support Directorate
- Joint Artificial Intelligence Center (former)
- Joint Intermediate Force Capabilities Office
- National Security Innovation Network
- NATO DIANA
- SOFWERX
- Special Operations Forces (SOF) Acquisition, Technology, and Logistics
- TechStars Accelerator (U.S. Space Force Sponsored)

### Acquisition Stakeholders:

- Office of the Undersecretary of Defense for Acquisition & Sustainment (OUSD A&S), International Cooperation
- OUSD A&S, Industrial Base Policy
- Air Force Life Cycle Management Center, ISR & SOF
- DSCA Weapons
- Office of the Deputy Assistant Secretary of the Army for Defense Exports and Cooperation
- USD R&E Innovation Steering Group

### Additional Interviews:

- Department of Commerce
- Department of Commerce Aerospace Programs



**Appendix B.**  
**Commercial Technology Heatmap**

---

Functional Areas	Critical Tasks	Compute		Data				Cyber		Sensors & Optics						
		Cloud Computing	Edge Computing	Collection	Processing	Analytics	Visualization	Management & Storage	Enterprise & Infrastructure Security	Application Security	Acoustic	Biometric	Infrared	Optic & Visual	Radar	Seismic
Intelligence and Counterintelligence	Plan and Manage Intelligence Collection	Orange	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow
	Targeting	Orange	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow
	Geospatial Intelligence	Orange	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow
	Intelligence, Surveillance, and Reconnaissance (ISR)	Red	Red	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow
	Human Intelligence	Orange	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow
	Signals Intelligence	Orange	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow
	Measurement and Signature Intelligence	Orange	Yellow	Red	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow
	Processing & Exploitation	Orange	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow
	Collate & Integrate Intelligence	Orange	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow
	Early Warning & Strategic Indicators	Orange	Yellow	Red	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow
Disseminate Intelligence Products	Orange	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	
Produce Counterintelligence Products	Orange	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	
Employment of Forces	Coordinate and Employ Joint Fires and Forces	Orange	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow
	Non-lethal Capabilities	Orange	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow
	Counter Violent Extremist Organizations (VEOs) and Counterterrorism	Orange	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow
	Aerospace Control	Orange	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow
	Manned Aircraft Defense	Orange	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow
	Unmanned Aircraft Defense	Orange	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow
	Ballistic Missile Warning & Defense	Orange	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow
	Cruise Missile Warning & Defense	Orange	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow
	Counter-UAS	Orange	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow
	Protect Sea Frontiers	Orange	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow
	Provide Maritime Warning	Orange	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow
	Counter-IED	Orange	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow
	Manage Sensor Platforms	Orange	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow
Force Protection	Orange	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	
Special Operations Activities (e.g., DA, UW, IW, CT, Civil Affairs)	Orange	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	
Sustainment	Human Resources & Personnel Management	Orange	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow
	Force Mobilization and Readiness	Orange	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow
	Integrated Deployment Data	Orange	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow
	Contracting & Procurement	Orange	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow
	Distribution & Logistics	Orange	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow
	Provide Repair Parts, Materiel & Equipment	Orange	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow
	Base Operations & Support	Orange	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow
Coordinate Health Services	Orange	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	
Command & Control, Communications & Computer Systems	Maintain IT & C2 Infrastructure	Red	Orange	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow
	Cybersecurity & Defensive Cyberspace Operations	Red	Orange	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow
	Command, Control, Communications & Computer Systems (C4S)	Red	Orange	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow
	Enterprise Services & Business Systems	Orange	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow
	Conduct Military Deception Operations	Orange	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow
Joint C2 Capabilities	Red	Orange	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	
CBRN	CBRN Detection and Response	Orange	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow

Functional Areas	Critical Tasks	Energy				Commercial Space				Integrated Systems	
		Alternative Fuels	Renewables	Transmission	Storage	Communication Satellites	Observation Satellites	Terrestrial Systems	Launch	Software-Defined Networking	Internet of Things
Intelligence and Counterintelligence	Plan and Manage Intelligence Collection										
	Targeting										
	Geospatial Intelligence										
	Intelligence, Surveillance, and Reconnaissance (ISR)										
	Human Intelligence										
	Signals Intelligence										
	Measurement and Signature Intelligence										
	Processing & Exploitation										
	Collate & Integrate Intelligence										
	Early Warning & Strategic Indicators										
Employment of Forces	Disseminate Intelligence Products										
	Produce Counterintelligence Products										
	Coordinate and Employ Joint Fires and Forces										
	Non-lethal Capabilities										
	Counter Violent Extremist Organizations (VEOs) and Counterterrorism										
	Aerospace Control										
	Manned Aircraft Defense										
	Unmanned Aircraft Defense										
	Ballistic Missile Warning & Defense										
	Cruise Missile Warning & Defense										
	Counter-UAS										
	Protect Sea Frontiers										
	Provide Maritime Warning										
Counter-IED											
Manage Sensor Platforms											
Force Protection											
Special Operations Activities (e.g., DA, UW, IW, CT, Civil Affairs)											
Sustainment	Human Resources & Personnel Management										
	Force Mobilization and Readiness										
	Integrated Deployment Data										
	Contracting & Procurement										
	Distribution & Logistics										
	Provide Repair Parts, Materiel & Equipment										
Command & Control, Communications & Computer Systems	Base Operations & Support										
	Coordinate Health Services										
	Maintain IT & C2 Infrastructure										
	Cybersecurity & Defensive Cyberspace Operations										
	Command, Control, Communications & Computer Systems (C4S)										
	Enterprise Services & Business Systems										
CBRN	Conduct Military Deception Operations										
	Joint C2 Capabilities										
CBRN	CBRN Detection and Response										

Functional Areas	Critical Tasks	Logistics & Sustainment					Artificial Intelligence & Machine Learning					
		Supply Chain Planning Solutions	Warehouse & Inventory Management Systems	Fleet Management Systems	Last-Mile Delivery Systems	Transportation Mobility Systems	Natural Language Processing	Knowledge Graphs	Generative AI	Audio & Speech Recognition	Multi-Modal AI	Computer Vision
Intelligence and Counterintelligence	Plan and Manage Intelligence Collection											
	Targeting											
	Geospatial Intelligence											
	Intelligence, Surveillance, and Reconnaissance (ISR)											
	Human Intelligence											
	Signals Intelligence											
	Measurement and Signature Intelligence											
	Processing & Exploitation											
	Collate & Integrate Intelligence											
Employment of Forces	Early Warning & Strategic Indicators											
	Disseminate Intelligence Products											
	Produce Counterintelligence Products											
	Coordinate and Employ Joint Fires and Forces											
	Non-lethal Capabilities											
	Counter Violent Extremist Organizations (VEOs) and Counterterrorism											
	Aerospace Control											
	Manned Aircraft Defense											
	Unmanned Aircraft Defense											
	Ballistic Missile Warning & Defense											
	Cruise Missile Warning & Defense											
	Counter-UAS											
	Protect Sea Frontiers											
Provide Maritime Warning												
Counter-IED												
Manage Sensor Platforms												
Force Protection												
Special Operations Activities (e.g., DA, UW, IW, CT, Civil Affairs)												
Sustainment	Human Resources & Personnel Management											
	Force Mobilization and Readiness											
	Integrated Deployment Data											
	Contracting & Procurement											
	Distribution & Logistics											
	Provide Repair Parts, Materiel & Equipment											
Command & Control, Communications & Computer Systems	Base Operations & Support											
	Coordinate Health Services											
	Maintain IT & C2 Infrastructure											
	Cybersecurity & Defensive Cyberspace Operations											
	Command, Control, Communications & Computer Systems (C4S)											
	Enterprise Services & Business Systems											
CBRN	Conduct Military Deception Operations											
	Joint C2 Capabilities											
	CBRN Detection and Response											

Functional Areas	Critical Tasks	Unmanned Systems	Human-Machine Interfaces	Software						
		Commercial UAVs	Augmented Reality (AR) & Virtual Reality (VR)	Business Process Automation (BPA) & Robotic Process Automation (RPA)	Open Source Software (OSS)	DevSecOps	Low-Code & No-Code Tools	Software Engineering Tools	Platform Management	API Management
Intelligence and Counterintelligence	Plan and Manage Intelligence Collection	Orange	Grey	Orange	Orange	Orange	Orange	Orange	Orange	Orange
	Targeting	Red	Grey	Orange	Orange	Orange	Orange	Orange	Orange	Orange
	Geospatial Intelligence	Orange	Grey	Orange	Orange	Orange	Orange	Orange	Orange	Orange
	Intelligence, Surveillance, and Reconnaissance (ISR)	Red	Grey	Orange	Orange	Orange	Orange	Orange	Orange	Orange
	Human Intelligence	Orange	Grey	Orange	Orange	Orange	Orange	Orange	Orange	Orange
	Signals Intelligence	Orange	Grey	Orange	Orange	Orange	Orange	Orange	Orange	Orange
	Measurement and Signature Intelligence	Orange	Grey	Orange	Orange	Orange	Orange	Orange	Orange	Orange
	Processing & Exploitation	Orange	Grey	Orange	Orange	Orange	Orange	Orange	Orange	Orange
	Collate & Integrate Intelligence	Orange	Grey	Orange	Orange	Orange	Orange	Orange	Orange	Orange
	Early Warning & Strategic Indicators	Orange	Grey	Orange	Orange	Orange	Orange	Orange	Orange	Orange
Disseminate Intelligence Products	Orange	Grey	Orange	Orange	Orange	Orange	Orange	Orange	Orange	
Produce Counterintelligence Products	Orange	Grey	Orange	Orange	Orange	Orange	Orange	Orange	Orange	
Employment of Forces	Coordinate and Employ Joint Fires and Forces	Orange	Grey	Orange	Orange	Orange	Orange	Orange	Orange	Orange
	Non-lethal Capabilities	Orange	Grey	Orange	Orange	Orange	Orange	Orange	Orange	Orange
	Counter Violent Extremist Organizations (VEOs) and Counterterrorism	Orange	Grey	Orange	Orange	Orange	Orange	Orange	Orange	Orange
	Aerospace Control	Orange	Grey	Orange	Orange	Orange	Orange	Orange	Orange	Orange
	Manned Aircraft Defense	Orange	Grey	Orange	Orange	Orange	Orange	Orange	Orange	Orange
	Unmanned Aircraft Defense	Orange	Grey	Orange	Orange	Orange	Orange	Orange	Orange	Orange
	Ballistic Missile Warning & Defense	Orange	Grey	Orange	Orange	Orange	Orange	Orange	Orange	Orange
	Cruise Missile Warning & Defense	Orange	Grey	Orange	Orange	Orange	Orange	Orange	Orange	Orange
	Counter-UAS	Orange	Grey	Orange	Orange	Orange	Orange	Orange	Orange	Orange
	Protect Sea Frontiers	Orange	Grey	Orange	Orange	Orange	Orange	Orange	Orange	Orange
	Provide Maritime Warning	Orange	Grey	Orange	Orange	Orange	Orange	Orange	Orange	Orange
	Counter-IED	Orange	Grey	Orange	Orange	Orange	Orange	Orange	Orange	Orange
	Manage Sensor Platforms	Orange	Grey	Orange	Orange	Orange	Orange	Orange	Orange	Orange
Force Protection	Orange	Grey	Orange	Orange	Orange	Orange	Orange	Orange	Orange	
Special Operations Activities (e.g., DA, UW, IW, CT, Civil Affairs)	Red	Grey	Orange	Orange	Orange	Orange	Orange	Orange	Orange	
Sustainment	Human Resources & Personnel Management	Orange	Grey	Orange	Orange	Orange	Orange	Orange	Orange	Orange
	Force Mobilization and Readiness	Orange	Grey	Orange	Orange	Orange	Orange	Orange	Orange	Orange
	Integrated Deployment Data	Orange	Grey	Orange	Orange	Orange	Orange	Orange	Orange	Orange
	Contracting & Procurement	Orange	Grey	Orange	Orange	Orange	Orange	Orange	Orange	Orange
	Distribution & Logistics	Orange	Grey	Orange	Orange	Orange	Orange	Orange	Orange	Orange
	Provide Repair Parts, Materiel & Equipment	Orange	Grey	Orange	Orange	Orange	Orange	Orange	Orange	Orange
	Base Operations & Support	Orange	Grey	Orange	Orange	Orange	Orange	Orange	Orange	Orange
Coordinate Health Services	Orange	Grey	Orange	Orange	Orange	Orange	Orange	Orange	Orange	
Command & Control, Communications & Computer Systems	Maintain IT & C2 Infrastructure	Orange	Grey	Orange	Orange	Orange	Orange	Orange	Orange	Orange
	Cybersecurity & Defensive Cyberspace Operations	Orange	Grey	Orange	Orange	Orange	Orange	Orange	Orange	Orange
	Command, Control, Communications & Computer Systems (C4S)	Orange	Grey	Orange	Orange	Orange	Orange	Orange	Orange	Orange
	Enterprise Services & Business Systems	Orange	Grey	Orange	Orange	Orange	Orange	Orange	Orange	Orange
	Conduct Military Deception Operations	Orange	Grey	Orange	Orange	Orange	Orange	Orange	Orange	Orange
Joint C2 Capabilities	Orange	Grey	Orange	Orange	Orange	Orange	Orange	Orange	Orange	
CBRN	CBRN Detection and Response	Orange	Grey	Orange	Orange	Orange	Orange	Orange	Orange	Orange

Functional Areas	Critical Tasks	Additive Manufacturing			Medical							
		Printed Materials	Execution Systems	Design Systems	Medical Personal Protective Equipment (PPE)	Surgical and Laboratory Equipment	Medical Equipment	Imaging	Medical Software	Medical Devices	Diagnostics	Pharmaceuticals
Intelligence and Counterintelligence	Plan and Manage Intelligence Collection Targeting Geospatial Intelligence Intelligence, Surveillance, and Reconnaissance (ISR) Human Intelligence Signals Intelligence Measurement and Signature Intelligence Processing & Exploitation Collate & Integrate Intelligence Early Warning & Strategic Indicators Disseminate Intelligence Products Produce Counterintelligence Products											
Employment of Forces	Coordinate and Employ Joint Fires and Forces Non-lethal Capabilities Counter Violent Extremist Organizations (VEOs) and Counterterrorism Aerospace Control Manned Aircraft Defense Unmanned Aircraft Defense Ballistic Missile Warning & Defense Cruise Missile Warning & Defense Counter-UAS Protect Sea Frontiers Provide Maritime Warning Counter-IED Manage Sensor Platforms Force Protection Special Operations Activities (e.g., DA, UW, IW, CT, Civil Affairs)											
Sustainment	Human Resources & Personnel Management Force Mobilization and Readiness Integrated Deployment Data Contracting & Procurement Distribution & Logistics Provide Repair Parts, Materiel & Equipment Base Operations & Support Coordinate Health Services											
Command & Control, Communications & Computer Systems	Maintain IT & C2 Infrastructure Cybersecurity & Defensive Cyberspace Operations Command, Control, Communications & Computer Systems (C4S) Enterprise Services & Business Systems Conduct Military Deception Operations Joint C2 Capabilities											
CBRN	CBRN Detection and Response											

## **Appendix C.**

### **Definitions of Heatmap Task Areas**

---

This appendix presents a definition and examples for each task area included in the heatmap. The task areas are derived from the DoD's UJTLs—particularly those categorized as Strategic National-level UJTLs. The IDA project team modified the definitions of relevant UJTLs to ensure their applicability to partner nations.

The definitions are presented in the same order in which they are listed in the heatmap (i.e., not alphabetically), which is generally consistent with the order in which they are presented within DoD's own UJTL documentation.

#### **Intelligence and Counterintelligence**

- **Plan and Manage Intelligence Collection:** Coordinate intelligence gathering efforts ensuring efficient allocation of resources and alignment with strategic objectives. Includes Identifying strategic military intelligence requirements, planning strategic collection efforts, and managing intelligence analysis and activities responding to strategic requirements.
- **Targeting:** Identify, prioritize, and select targets by analyzing patterns to inform lethal or nonlethal military action, ensuring higher precision and reduced collateral damage. Includes actions to find, fix, track, target, engage, and assess time-sensitive targets; conduct target development including analysis, assessment, and documentation; provide intelligence input for the development and maintenance of target lists.
- **Geospatial Intelligence:** Intelligence derived from the mapping and analysis of ground, air, space, naval, and other geospatial domains to support operational planning and situational awareness. Produced through an integration of imagery, imagery intelligence, and geospatial information. Includes the collection and/or orchestration of geospatial imagery and data sources across the entire spectrum of providers (e.g., commercial and government systems) and analytical support (warning, targeting, and crisis), and baseline intelligence and products to enable national security priorities.
- **ISR:** Operations that involve fusing the collection and analysis of information across sensors, networks, and reconnaissance to support military decision-making and tactical planning. Involves collecting and integrating data gathered

through sensors, systems, platforms, human capital, and other assets to directly support current and future operations.

- **Human Intelligence:** Gathering intelligence through interpersonal contact, such as interviews and espionage, while ensuring the safety and anonymity of sources and means.
- **Signals Intelligence:** Gathering, analysis, and exploitation of intelligence from digital or electronic sources such as communications networks, radars, and weapons systems.
- **MASINT:** Gathering intelligence on the intrinsic characteristics and components of an object or activity using other intelligence disciplines, such as electro-optical, geophysical, radar, radio frequency, materials, and nuclear radiation. MASINT is produced by quantitative and qualitative analysis of physical attributes of targets and events to characterize, locate, and identify them.
- **Processing & Exploitation:** Analyzing and extracting useful information from collected intelligence from vast data sources.
- **Collate & Integrate Intelligence:** Managing and fusing data from multiple sources to improve the reliability and credibility of information; converting diverse forms of intelligence into formats that enable all-source analysis; and creating a comprehensive intelligence and operating picture.
- **Early Warning & Strategic Indicators:** Identifying potential threats or opportunities against entities, partners, or interests for timely and accurate early warnings. Includes identifying and reporting time-sensitive intelligence on foreign developments that could threaten national security and interests. “Warning” connotes distinct communication to decision-makers.
- **Disseminate Intelligence Products:** Secure and timely distribution of critical information and intelligence physically and/or virtually. Examples include personal contact, physical transfer, message traffic, portal pages, e-mail, collaborative software applications, secure voice/fax, video teleconferencing, newsgroups, broadcasts, and tactical radio circuits.
- **Produce Counterintelligence Products:** Creating materials to counter espionage and other intelligence threats, protecting sensitive information and operations. This task may include counterintelligence analysis and production to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, persons, their agents, or international terrorist organizations or activities.



## Employment of Forces

- **Coordinate and Employ Joint Fires and Forces:** Orchestrating the use of combined arms and joint fires allowing integrated operations across different military branches to create lethal or nonlethal effects on a target.
- **Non-lethal Capabilities:** Tactics and technologies designed to have reversible effects and deter or incapacitate personnel or material immediately without causing death or significant damage.
- **Counter Violent Extremist Organizations (VEOs) and Counterterrorism:** Operations aimed at preventing and combating VEOs' activities. This task includes integrating strategy, plans, and intelligence priorities for operations against VEOs and other threat networks, and executing operations against VEOs and other threat networks as directed.
- **Aerospace Control:** Identifying and sensing aircraft to ensure control and supremacy in airspace; managing both civilian and military air traffic to safeguard against threats. This involves monitoring, validating, warning of, and defending from threats posed by aircraft, missiles, and space vehicles.
- **Manned Aircraft Defense:** Employing capabilities, systems, etc. to counter and/or provide protection against threats posed by manned aircraft. Integrates offensive and defensive operations to control and protect airspace by deterring, mitigating, and/or destroying manned airborne threats.
- **Unmanned Aircraft Defense:** Employing capabilities, systems, etc. to counter and/or provide protection against threats posed by UAS.
- **Ballistic Missile Warning & Defense:** Detection and defense against ballistic missile threats.
- **Cruise Missile Warning & Defense:** Detection and defense against cruise missile threats.
- **Counter-Unmanned Aerial Systems:** Detection and defense against UAS to ensure security of airspace, personnel, critical infrastructure, and other assets.
- **Protect Sea Frontiers:** Safeguarding maritime borders and territorial waters against attacks and threats, including economic threats and ecological disasters.
- **Provide Maritime Warning:** Leveraging technologies, systems, human capital, and/or processes to gather, assess, and disseminate intelligence and other information regarding impending maritime-based threats as well as man-made and natural disasters.
- **Counter Improvised Explosive Devices (Counter-IED):** Thwart asymmetric threats posed by IEDs through attacking networks, detecting and defeating

devices, and training forces. Counter-IED activities should take a holistic approach that incorporates intelligence, information, training, operations, materiel, technology, protection, and policy.

- **Manage Sensor Platforms:** Oversee and direct the operation and utilization of sensor systems across optical, radar, acoustic, and other sensor types.
- **Force Protection:** Comprehensive security, including perimeter security, access control, and surveillance that provide measures to safeguard military personnel and assets, supervisory control and data acquisition systems, and critical infrastructure.
- **Special Operations Activities:** Full-spectrum special operations activities to include: direct action, special reconnaissance, countering weapons of mass destruction, counterterrorism, unconventional warfare, hostage rescue and recovery, counterinsurgency, and military information support operations.

## Sustainment

- **Human Resources & Personnel Management:** Assessing manpower needs and allocating human resources. Encompasses recruitment, training, role assignment, career development, and retention strategies, as well as separation and retirement processes.
- **Force Mobilization and Readiness:** Encompasses overall preparedness of military forces, which includes having sufficient numbers of personnel who are trained and equipped, supported by adequate reserves, war reserve materials, and pre-positioned stocks. Mobilization is the process of activating components of the military to reinforce the active forces in various scenarios, ranging from domestic emergencies to full-scale conflict.
- **Integrated Deployment Data:** Information about the personnel, equipment, and resources being moved during a deployment, ensuring that the precise items, in the right quantities, arrive at the designated locations in sync with operational timelines.
- **Contracting & Procurement:** This task includes providing acquisition planning and support, contract execution, and contract management functions necessary to ensure necessary supplies and services are provisioned to the enterprise and force.
- **Distribution & Logistics:** Management and utilization of personnel, systems, processes, infrastructure, data, and assets required to effectively store, distribute, and deliver materiel and critical supplies.

- **Provide Repair Parts, Materiel & Equipment:** Encompasses procurement, production, storage, maintenance, and delivery of spare parts, materiel, and other equipment necessary to sustain forces and ensure continued operation of critical systems, platforms, and other assets (e.g., vehicles).
- **Base Operations & Support:** Encompasses activities and services necessary to operate and maintain installations, such as construction, power supply, food storage and preparation.
- **Coordinate Health Services:** This task encompasses the provisioning of medical, dental, veterinary, optical, and ancillary services (e.g., patient care, patient movement). It also includes medical supplies and maintenance, as well as health-related preparedness (e.g., pandemic planning).

## Command & Control

- **Maintain IT & C2 Infrastructure:** Ensuring the continuous operation, security, and reliability of military information networks, including those critical to exercising command and control.
- **Cybersecurity & Defensive Cyberspace Operations:** Protection of military information networks and other designated cyber assets. This includes monitoring for threats, actively defending against attacks, and restoring systems after a breach to ensure the secure and reliable flow of information.
- **Command, Control, Communications & Computer Systems (C4S):** The systems and infrastructure providing secure communication, data processing, and decision-making tools that enable military commanders to effectively direct forces and coordinate operations. This includes everything from strategic-level networks to tactical communication systems used in the field.
- **Enterprise Services & Business Systems:** Software applications, services, and systems used manage business operations and critical enabling functions exercised across the military enterprise such as finance, human resources management, procurement, and planning.
- **Conduct Military Deception Operations:** Actions designed to influence adversaries' decision-making process or deliberately mislead enemy decision-makers, causing them to act in ways that benefit friendly forces and contribute to the success of the mission.
- **Joint C2 Capabilities:** Systems, applications, and communication networks used by commanders to effectively lead and coordinate forces. These capabilities enable planning, decision-making, situational awareness, and secure communication.

## **Chemical, Biological, Radiological, and Nuclear (CBRN)**

- **CBRN Detection and Response:** A comprehensive set of actions and capabilities (e.g., technologies, systems, etc.) aimed at detecting, preparing for, mitigating against, and recovering from incidents involving CBRN materials.

## **Appendix D. Resource Mock-Ups**

---

This appendix presents mock-ups of one approach to deep-diving priority task areas and/or technologies on the heatmap and providing SCOs basic insights needed to identify potential commercial technology solutions for partner nations’ needs. The mock-ups are *not intended to be used as a comprehensive market report on a task area/technology or to be interpreted as a suggestion of which vendors should be selected to support a particular initiative*. Rather, this is a simple overview of a task area relevant definitions, technologies, use cases, vendors, and resources that could be used as a starting point for discovering useful, task-specific commercial technologies.

The first slide describes a priority task area, while the second and third slides begin to dig deeper into high-impact technologies related to that task. This template could be similarly applied to the rest of the heatmap, where a “placemat”, slide, or similar resources are created for each task and for each technology. An SCO could read about a task area (e.g., maritime warning), see the high-impact technologies listed on the slide (e.g., cloud computing), and then navigate to the slide or other resources on that technology to learn more.

Alternatively, high impact technology slides could be made for and tailored to each task area slide. For example, while cloud computing could be useful across a wide variety of task areas, the cloud computing slide under “maritime warning” could just include information, resources, examples, etc. of cloud computing within the context of maritime warning

## TASK: MARITIME WARNING

Task Description	Exemplar Use Cases – Maritime Warning Technology	
<ul style="list-style-type: none"> <li>▪ <b>Task Definition:</b> <u>Integrated maritime communication networks and threat intelligence</u> to issue alerts and warning regarding impending <u>military threats or natural disasters</u></li>   <li>▪ <b>Maritime Warning Includes:</b> <ul style="list-style-type: none"> <li>▪ Monitoring unauthorized or hostile vessels, piracy activities, and other illegal activities;</li> <li>▪ Reporting on environmental hazards and marine pollution;</li> <li>▪ Supporting search and rescue operations;</li> <li>▪ Achieving all-domain maritime awareness by integrating sensors and intelligence information.</li> </ul> </li> </ul>	<div style="border: 1px solid #ccc; border-radius: 10px; padding: 10px; margin-bottom: 10px;"> <p><b>SeaWatch in the Philippines:</b> The Philippines is trialing the Sea Watch app, which integrates and geolocates photos/reports of illicit activities made by fisherman on their mobile phones.</p> </div> <div style="border: 1px solid #ccc; border-radius: 10px; padding: 10px; margin-bottom: 10px;"> <p><b>Sea Guardian in Japan:</b> Japan is trialing the MQ -9B UAV from General Atomics Aeronautics over the East China Sea to test if it could replace some manned surveillance missions in the area.</p> </div> <div style="border: 1px solid #ccc; border-radius: 10px; padding: 10px;"> <p><b>Underwater Tracking in Australia:</b> Australia contracted with L3 Harris to procure Maritime Underwater Tracking Ranges which connect a series of sensors to relay location and movement data and enable testing and evaluation of maritime platforms.</p> </div>	
Commercial Tech for Maritime Warning	Potential Sources of Market Intel and Contact Information	
<ul style="list-style-type: none"> <li>• <b>Commercial UAVs</b></li> <li>• <b>Cloud Computing</b></li> <li>• <b>Edge Computing</b></li> <li>• <b>Data Collection, Processing, Analysis, and Visualization</b></li> <li>• <b>Application Security</b></li> <li>• <b>Acoustic, Radar, and Optic Sensors</b></li> <li>• <b>Communication and Observation Satellites</b></li> <li>• <b>Terrestrial Systems</b></li> <li>• <b>Software Defined Networking</b></li> <li>• <b>Internet of Things</b></li> <li>• <b>Audio and Speech Recognition</b></li> <li>• <b>Multi-Modal AI</b></li> <li>• <b>Computer Vision</b></li> </ul>	<div style="border: 1px solid #ccc; border-radius: 15px; padding: 10px; margin-bottom: 10px;"> <p><b>NGA Challenge</b> In 2024, NGA is partnering with the National Security Innovation Network to launch the “Global Fishing Forecast Challenge” for commercial and academic communities to identify innovative solutions to forecasting IUU fishing.</p> <p><b>Contact <a href="mailto:media@nsin.mil">media@nsin.mil</a> for more information.</b></p> </div>	<div style="border: 1px solid #ccc; border-radius: 15px; padding: 10px; margin-bottom: 10px;"> <p><b>DIU to DoD Users</b> In 2022, DIU transitioned 17 commercial solutions - including autonomous maritime intelligence, surveillance, and reconnaissance technologies - to DoD users. One of the vendors they worked with is Sairdrone.</p> <p><b>Contact <a href="mailto:Sairdrone@diu.mil">Sairdrone@diu.mil</a> for more information.</b></p> </div> <div style="border: 1px solid #ccc; border-radius: 15px; padding: 10px;"> <p><b>Project Aegir</b> NGA opened its first commercial solutions opening. Selected vendors will pitch solutions to identifying, monitoring, and tracking illicit maritime activity in INDOPACOM’s AOR.</p> <p><b>Contact <a href="mailto:John.Doe@nga.mil">John Doe (john.e.doe@nga.mil)</a> for more information.</b></p> </div>

## TECH: CLOUD COMPUTING

Technology Description	Exemplar Use Cases																						
<ul style="list-style-type: none"> <li>▪ <b>NIST Definition:</b> Cloud computing is a model for enabling <u>ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources</u> (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with <u>minimal management effort</u> or service provider interaction.</li> <li>▪ <b>Types of Cloud:</b> Cloud computing infrastructure <u>varies in both scale</u> (from localized to distributed data centers) and <u>accessibility</u> (public, community, private, and hybrid cloud).</li> <li>▪ <b>Cloud Impact:</b> Helps businesses, governments, militaries, and intelligence agencies:               <ul style="list-style-type: none"> <li>▪ Deploy and access applications and services rapidly;</li> <li>▪ Build <u>interoperability</u> and <u>scale</u> information access;</li> <li>▪ <u>Reduce the cost and complexity</u> of IT management;</li> <li>▪ Improve <u>data security</u>;</li> <li>▪ Promote <u>innovation</u> with access to a broader array of capabilities.</li> </ul> </li> </ul>	<div style="background-color: #f0f0f0; padding: 10px; border-radius: 10px; margin-bottom: 10px;"> <p><b>Ukraine's Data Migration to the Cloud:</b> The Ukrainian government worked with U.S. cloud companies to move terabytes of data to commercial cloud infrastructure at the beginning of Russia's invasion. This decision enabled the Ukrainian government to preserve critical data and government services, and improve its resiliency against continued cyberattacks</p> </div> <div style="background-color: #f0f0f0; padding: 10px; border-radius: 10px; margin-bottom: 10px;"> <p><b>India's Economic Growth and Accessibility:</b> Esconet created an encrypted, cloud-based system called "Army Cloud," for the Indian Army, which has helped the organization to centralize data storage (and eliminate mobile servers), reduce costs, and enhance data accessibility and security.</p> </div> <div style="background-color: #f0f0f0; padding: 10px; border-radius: 10px;"> <p><b>CIA Cloud:</b> In 2013, the CIA radically signed a contract with a commercial cloud company, Amazon Web Services, to improve the agency's efficiency and innovation. In 2020, the CIA signed a new contract to also include services from Google, Microsoft, Oracle, and IBM.</p> </div>																						
Market Leaders	Potential Sources of Market Intel																						
<table style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left; border-bottom: 1px solid black;">Company &amp; Market Share</th> <th style="text-align: left; border-bottom: 1px solid black;">HQ Country</th> </tr> </thead> <tbody> <tr> <td>• Amazon Web Services (AWS): 32% Market Share</td> <td></td> </tr> <tr> <td>• Microsoft Azure: 23%</td> <td></td> </tr> <tr> <td>• Google Cloud: 11%</td> <td></td> </tr> <tr> <td>• Alibaba Cloud: 4%</td> <td></td> </tr> <tr> <td>• IBM Cloud: 3%</td> <td></td> </tr> <tr> <td>• Salesforce: 3%</td> <td></td> </tr> <tr> <td>• Oracle Cloud: 2%</td> <td></td> </tr> <tr> <td>• Dell: 2%</td> <td></td> </tr> <tr> <td>• Huawei: 2%</td> <td></td> </tr> <tr> <td>• Tencent: 2%</td> <td></td> </tr> </tbody> </table>	Company & Market Share	HQ Country	• Amazon Web Services (AWS): 32% Market Share		• Microsoft Azure: 23%		• Google Cloud: 11%		• Alibaba Cloud: 4%		• IBM Cloud: 3%		• Salesforce: 3%		• Oracle Cloud: 2%		• Dell: 2%		• Huawei: 2%		• Tencent: 2%		<div style="background-color: #f0f0f0; padding: 10px; border-radius: 10px; margin-bottom: 10px;"> <p style="text-align: center;"><b>U.S. Federal Cloud Computing Strategy</b></p> <p>A long-term, high-level strategy to drive cloud adoption in Federal agencies, focusing on the pillars of security, procurement, and workforce. Could be a tool to consider or others looking to adopt cloud-based solutions.</p> <p style="font-size: small;">Click on the link for more information: <a href="https://cloud.cio.gov/strategy/">https://cloud.cio.gov/strategy/</a></p> </div> <div style="background-color: #f0f0f0; padding: 10px; border-radius: 10px; margin-bottom: 10px;"> <p style="text-align: center;"><b>CJADC2</b></p> <p>Contracts awarded in 2022 to Amazon Web Services Inc. (AWS), Google Support Services LLC, Microsoft, and Oracle to establish an enterprise DoD cloud capability that can eventually also integrate international partners. Contact DISA for more information.</p> <p style="font-size: small;">For more information, click on the link to contact DISA: <a href="https://community.hacc.mil/s/contact">https://community.hacc.mil/s/contact</a></p> </div> <div style="background-color: #f0f0f0; padding: 10px; border-radius: 10px;"> <p style="text-align: center;"><b>Cloud Security Alliance</b></p> <p>The CSA STAR Registry is a publicly accessible registry that documents the security and privacy controls provided by popular cloud computing offerings. Could use as a tool for finding and vetting commercial companies.</p> <p style="font-size: small;">Click on the link for more information: <a href="https://cloudsecurityalliance.org/star/registry">https://cloudsecurityalliance.org/star/registry</a></p> </div>
Company & Market Share	HQ Country																						
• Amazon Web Services (AWS): 32% Market Share																							
• Microsoft Azure: 23%																							
• Google Cloud: 11%																							
• Alibaba Cloud: 4%																							
• IBM Cloud: 3%																							
• Salesforce: 3%																							
• Oracle Cloud: 2%																							
• Dell: 2%																							
• Huawei: 2%																							
• Tencent: 2%																							

## TECH: COMMERCIAL UAVs

Technology Description					Exemplar Use Cases and Tech Integration		
<ul style="list-style-type: none"> <li><b>DTIC Definition:</b> UAVs (or drones) are powered, aerial vehicles that <u>do not carry a human operator</u>, use <u>aerodynamic forces</u> to provide vehicle lift, can <u>fly autonomously or be piloted remotely</u>, can be <u> expendable or recoverable</u>, and can carry a <u>lethal or nonlethal payload</u>.</li> <li><b>Impact:</b> Military and dual-use drones can be used to <u>identify, survey, and strike/engage ground-based targets</u>. Heavy lift drones are also being adapted to <u>carry supplies for contested logistics</u>. Commercial UAVs have high utility for <u>special operations</u>. UAV's have even greater potential when combined with other tech.</li> <li><b>Types of UAVs:</b> UAV's <u>vary in wing type, size, payload capacity, range, uses, power sources/motors</u></li> </ul>					<div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> <b>Ukraine's AI Enabled Drones:</b> <i>Integrating AI and data from satellites and other sources with drones</i> has helped Ukrainian attack drone operators map out/locate Russian targets and have even carried out autonomous strikes.         </div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> <b>Gaza Conflict:</b> Israel is using small, quadcopter drones <i>with anti-collision sensors</i> to investigate Hamas' underground tunnel system.         </div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> <b>Post-Disaster Assistance:</b> Commercial drones are used to help assess damage and deliver aid after natural disasters. For example, in 2019, drones delivered food and supplies to isolated areas in Japan following Typhoon Hagibis.         </div> <div style="border: 1px solid #ccc; padding: 5px;"> <b>Border Security in Nigeria:</b> Nigeria uses commercial tethered drones <i>(paired with electro-optical sensors)</i> to bolster its border security by identifying potential threats. Terrorist groups like Boko Haram also commercial drones for intelligence gathering and creating IEDs.         </div>		
<b>Wing Type</b> Multi-rotor, fixed-wing, single-rotor, fixed-wing, hybrid VTOL	<b>Payload Capacity</b> Featherweight (<11 grams), lightweight, middleweight, heavy-lift (more than 100 kg)	<b>Range</b> Very close-range (5 km), close-range, short-range, mid-range, long-range (>644km)	<b>Uses</b> Military or recreational uses (photography, racing, GPS, delivery)	<b>Power Sources</b> Battery, gasoline, hydrogen fuel cell, solar			
Market Leaders				Potential Sources of Market Intel and Contact Information			
<b>Company &amp; Market Share</b>		<b>HQ Country</b>		<div style="border: 1px solid #ccc; padding: 10px; margin-bottom: 10px; border-radius: 10px;"> <b>DIU Blue UAS</b>            Since 2020, DIU has maintained a list of policy approved commercial UAS models for use by the DoD.   <b>Click here for the cleared list:</b>  <a href="https://www.diu.mil/blue-uas-cleared-list">https://www.diu.mil/blue-uas-cleared-list</a>             Contact <a href="mailto:blueuas@diu.mil">blueuas@diu.mil</a> for more information.         </div> <div style="border: 1px solid #ccc; padding: 10px; margin-bottom: 10px; border-radius: 10px;"> <b>REMA Program</b>            In February 2024, DARPA began working with contractors to adapt U.S. military drones to have autonomy capabilities. The companies selected for the first contract include Anduril, RTX, Leidos, Northrop Grumman, and SolarTech.             Contact <a href="mailto:outreach@DARPA.mil">outreach@DARPA.mil</a> or <a href="mailto:DARPA-PS-23-12@darpa.mil">DARPA-PS-23-12@darpa.mil</a> for more information.         </div> <div style="border: 1px solid #ccc; padding: 10px; border-radius: 10px;"> <b>UAV Market Reports</b>  <b>Drone Industry Insights:</b>  <a href="https://droneii.com/the-drone-industrys-journey-through-2023">https://droneii.com/the-drone-industrys-journey-through-2023</a>   <b>Fortune Business:</b>  <a href="https://www.fortunebusinessinsights.com/commercial-drone-market-102171">https://www.fortunebusinessinsights.com/commercial-drone-market-102171</a> </div>			
<b>DJI:</b> 70% market share							
<b>Autel Robotics:</b> 4.4% market share							
<b>Yuneec:</b> 2.5% market share							
<b>Skydio:</b> 1.5% market share							
<b>AeroVironment:</b> 0.5% market share							
<b>Parrot:</b> 0.1% market share							



**Appendix E.**  
**Summary Table of Recommendations**

---

Business Strategy	Recommendation
Overarching	Leverage the heatmap to focus DSCA's effort on the technologies and/or capability areas of greatest value and feasibility.
	Develop a framework for assessing when it is or is not in U.S. interests to consider commercial technologies as a solution to a partner nation challenge.
	Open the aperture for commercially-available capabilities to be considered during the case-shaping phase of the sales cycle.
	Use existing procurement methods to test delivery of commercially-available capabilities and pressure-test the need for additional authorities to facilitate timely procurements.
	Develop a total package approach and map technology requirements.
	Conduct pilots with DIU to determine the optimal business strategy and inform business process improvements.
DIU-Led Approach	Advocate for DIU to receive a mandate, headcount, resourcing, and support to build a team and portfolio focused on partner nations.
	Update policies to establish DIU's role akin to a MILDEP in the security cooperation apparatus.
	Incorporate DIU in the Security Cooperation Steering Group.
	Establish a framework and mechanisms for how partner nations and/or SCOs can reach directly to DIU for support.
	Leverage DIU's existing commercial solutions opening process to post problem statements on behalf of partner nations, receive proposals, vet potential solutions, and introduce partner nations to a selection of companies and capabilities.
Joint DSCA-DIU Approach	Develop a framework that leverages and aligns DSCA's and DIU's respective strengths and unique capabilities.
	Build a small footprint team (2-3 headcount) within DSCA responsible for cultivating and facilitating engagements between industry and partner nations focused on strategic or long-term commercial tech applications.
	Create a process through which DSCA determines if and when to request DIU's assistance when partner nations express interest in commercially-available capabilities.
	Leverage DIU's existing commercial solutions opening process to post problem statements on behalf of partner nations, receive proposals, and vet solutions.
	Detail DSCA employees and/or experienced SCOs to DIU. Detailees should serve as liaisons and assist DIU in developing new portfolios and processes.
	Coordinate with DIU to leverage the Intergovernmental Personnel Act (IPA) to embed security cooperation experts within DIU.
DSCA-Led Approach	Define DSCA's value proposition in enabling sales of commercially-available capabilities to partner nations.
	Validate advantages and willingness among supply-side and demand-side stakeholders for DSCA to facilitate procurements of commercially-available capabilities.
	Establish a dedicated team focused on cultivating and facilitating need-driven engagements between industry and partner nations.
	Enhance DSCA's market intelligence on capabilities and/or technologies of greatest potential impact.
	Conduct engagements with partner nations to elucidate how they may apply commercial technologies in new, novel ways.
	Proactively field assessment teams to apply the heatmap framework to specific partner nations and/or identify opportunities for commercially-available capabilities to improve partner nations' abilities to execute critical tasks.
	Collaborate with partner nations and industry to develop tailored strategies and roadmaps for effective commercial technology deployment, including building end-to-end solutions and transformative capabilities.

## References

---

- Addiscott, Richard, et al. "Top Trends in Cybersecurity 2023." Gartner, Inc., March 2023.
- Addiscott, Richard, et al. "Top Trends in Cybersecurity for 2024." Gartner, Inc., January 2024.
- Air Force Security Assistance & Cooperation Directorate. *Foreign Military Sales (FMS) Checklist for Developing Acquisition of Fighter Aircraft Letter of Request (LOR)*. <https://afsac.wpafb.af.mil/resources/lor/USAF-Fighter-Aircraft-Checklist.pdf>.
- Albon, Courtney. "Defense Innovation Unit's Tech-scaling Strategy Focuses on Partnerships." C4ISRNet, February 7, 2024. <https://www.c4isrnet.com/battlefield-tech/2024/02/07/defense-innovation-units-tech-scaling-strategy-focuses-on-partnerships/#:~:text=To%20help%20address%20these%20problems%2C%20DIU%20will%20lead,embedded%20support%20to%20combatant%20commands%20around%20the%20world>.
- Allen, Gregory C. "Across Drones, AI, and Space, Commercial Tech Is Flexing Military Muscle in Ukraine." CSIS, May 13, 2022. <https://www.csis.org/analysis/across-drones-ai-and-space-commercial-tech-flexing-military-muscle-ukraine>.
- Anwar, Nessa. "World's Largest Drone Maker Is Unfazed—Even if It's Blacklisted by the U.S." CNBC, February 7, 2023. <https://www.cnbc.com/2023/02/08/worlds-largest-drone-maker-dji-is-unfazed-by-challenges-like-us-blacklist.html>.
- Arms Export Control Act, Public Law 118-31, U.S. Statutes at Large (2023). <https://www.govinfo.gov/content/pkg/COMPS-1061/pdf/COMPS-1061.pdf>.
- Assessment, Monitoring, and Evaluation of Programs and Activities, U.S. Code 10, § 383.*
- Beck, Douglas A. "DIU 3.0: Scaling Defense Innovation for Strategic Impact." Center for a New American Security, February 7, 2024. <https://www.cnas.org/publications/reports/diu-3-0>.
- Berman, Noah, Lindsay Maizland, & Andrew Chatzky. "Is China's Huawei a Threat to U.S. National Security?" Council on Foreign Relations, February 8, 2023. <https://www.cfr.org/backgrounder/chinas-huawei-threat-us-national-security>.
- "Blue UAS for First Responders." U.S. Department of Homeland Security. <https://www.dhs.gov/science-and-technology/saver/blue-uas-first-responders>.
- Borger, Julian. "Our Weapons Are Computers": Ukrainian Coders Aim to Gain Battlefield Edge." The Guardian. December 18, 2022.

<https://www.theguardian.com/world/2022/dec/18/our-weapons-are-computers-ukrainian-coders-aim-to-gain-battlefield-edge>.

Bouey, Jennifer, Lynn Hu, Keller Scholl, William Marcellino, Rafiq Dossani, Ammar Malik, Kyra Solomon, Sheng Zhang, and Andy Shufer. “China’s AI Exports: Technology Distribution and Data Safety.” RAND, December 11, 2023. [https://www.rand.org/pubs/research\\_reports/RRA2696-2.html](https://www.rand.org/pubs/research_reports/RRA2696-2.html).

Cheng, Evelyn, “China to Increase Defense Spending by 7.2%.” CNBC, March 4, 2023. <https://www.cnbc.com/2023/03/05/china-defense-budget-two-sessions.html>.

China Power Team, “How Dominant Is China in the Global Arms Trade?” CSIS, April 26, 2018. <https://chinapower.csis.org/china-global-arms-trade/>.

Christou, Chris, & Michael Lundberg. “Automating Cybersecurity Using Software-Defined Networking.” *United States Cybersecurity Magazine*, 2016. <https://www.uscybersecurity.net/csmag/automating-cybersecurity-using-software-defined-networking/>.

DeBeasi, Paul. “Top Trends in Data and Analytics, 2021.” Gartner, Inc., July 2021.

Defense Acquisition University. “International Acquisition—Direct Commercial Sales (DCS).” <https://www.dau.edu/acquippedia-article/international-acquisition-direct-commercial-sales-dcs>.

Defense Innovation Unit. “Careers.” Accessed August 13, 2024. <https://www.diu.mil/careers>.

Defense Innovation Unit. “DIU Hosts Ukraine and the Future of Unmanned Aerial Systems Forum in Warsaw.” Accessed August 13, 2024. <https://www.diu.mil/latest/diu-hosts-ukraine-and-the-future-of-unmanned-aerial-systems-forum-in-warsaw>.

Defense Security Cooperation Agency. *Guidelines for Foreign Military Financing of Direct Commercial Contracts*. 2017. [https://www.dscsa.mil/sites/default/files/dsca\\_guidelines\\_for\\_foreign\\_military\\_financing\\_of\\_direct\\_commercial\\_contracts\\_updatedfinal.pdf](https://www.dscsa.mil/sites/default/files/dsca_guidelines_for_foreign_military_financing_of_direct_commercial_contracts_updatedfinal.pdf)

Defense Security Cooperation University. The Greenbook, chap. 5, <https://www.dscu.edu/sites/default/files/2024-08/05-chapter.pdf>.

D’Hoinne, Jeremy, et al. “Predicts 2024: AI & Cybersecurity—Turning Disruption into an Opportunity.” Gartner, Inc., December 2023. “DIU’s FY22 Year-in-Review.” Defense Innovation Unit, 2023, <https://www.diu.mil/fy22-year-in-review>.

Easley, Mikayla. “Pentagon Creating New Role to Break Down ‘Language Barrier’ between Non-traditional Vendors, DoD.” Defense Scoop, December 8, 2023. <https://defensescoop.com/2023/12/08/transition-concierge-pentagon/>.

“Figure C5.F14. Standard Letter of Request Advisory. Defense Security Cooperation Agency. Accessed August 13, 2024, <https://samm.dscsa.mil/figure/figure-c5f14>.

Finance Research Team. “CFOs Must Change to Unlock the Future of Autonomous Finance.” Gartner, Inc., August 2022.

Firstbrook, Peter, et al. "Top Trends in Cybersecurity 2022." Gartner, Inc., February 2022.

Gandhi, Animesh. "Market Guide for Revenue Management in Pharmaceuticals and Biotechnology." Gartner, Inc., April 2020.

Gartner, Inc. "2023 Technology Adoption Roadmap for Data and Analytics Functions in Large Enterprises." Gartner Inc., March 2023.

Gartner, Inc. "2023 Technology Adoption Roadmap for Security and Risk Management." Gartner, Inc., February 2023.

Gartner, Inc. "2023 Technology Adoption Roadmap for Software Engineering." Gartner, Inc., February 2023.

Gilman, Derek, Robert Nichols, Jade C. Totman, and Christine Minarich. "Foreign Military Sales & Direct Commercial Sales." September 30, 2014. [https://www.dscamilitary.com/sites/default/files/final-fms-dcs\\_30\\_sep.pdf](https://www.dscamilitary.com/sites/default/files/final-fms-dcs_30_sep.pdf).

Gosselin-Malo, Elisabeth. "Ukraine Continues to Snap up Chinese DJI Drones for Its Defense." C4ISRNet, October 23, 2023. <https://www.c4isrnet.com/global/europe/2023/10/23/ukraine-continues-to-snap-up-chinese-dji-drones-for-its-defense/>.

Greenwood, Faine. "The Drone War in Ukraine Is Cheap, Deadly, and Made in China." Foreign Policy, February 16, 2023. <https://foreignpolicy.com/2023/02/16/ukraine-russia-war-drone-warfare-china/>.

Herschel, Gareth, et al. "Top Trends in Data and Analytics, 2023." Gartner, Inc., March 2023.

Jaffri, Afraz. "Hype Cycle for Artificial Intelligence." Gartner, Inc., July 2023.

Jones, Grace, Janet Egan, and Eric Rosenbach. "Advancing in Adversity: Ukraine's Battlefield Technologies and Lessons for the U.S." Harvard University Belfer Center, July 31, 2023. <https://www.belfercenter.org/publication/advancing-adversity-ukraines-battlefield-technologies-and-lessons-us>.

Jones, Mike, et al. "Predicts 2020: Healthcare Providers Must Strike a Balance for Digital Business Success." Gartner, Inc., December 2019.

Kina, Chris, et al. "Predicts 2024: Logistics." Gartner, Inc., December 2023.

Klappich, Dwight. "Hype Cycle for Mobile Robots and Drones." Gartner, Inc., July 2023.

Klappich, Dwight. "Hype Cycle for Supply Chain Execution Technologies, 2023," Gartner, Inc., July 2023.

Klappich, Dwight, et al. "Predicts 2023: Supply Chain Technology." Gartner, Inc., November 2022.

Konkel, Frank. "Ukraine Tech Chief: Cloud Migration 'Saved Ukrainian Government and Economy.'" Nextgov, December 1, 2022. <https://www.nextgov.com/digital-government/2022/12/ukraine-tech-chief-cloud-migration-saved-ukrainian-government-and-economy/380328/>

- Kontsevoi, Boris. "The Ukrainian IT Industry Is Alive and Healthy." *Forbes*, October 12, 2022. <https://www.forbes.com/sites/forbestechcouncil/2022/10/12/the-ukrainian-it-industry-is-alive-and-healthy/?sh=5dd8f2d67f2c>.
- Kullab, Samya. "How Ukraine Soldiers Use Inexpensive Commercial Drones on the Battlefield." *PBS News*, September 26, 2023. <https://www.pbs.org/newshour/world/how-ukraine-soldiers-use-inexpensive-commercial-drones-on-the-battlefield>.
- Kynge, James, Valerie Hopkins, Helen Warrell, and Kathrin Hille. "Exporting Chinese Surveillance: The Security Risks of 'Smart Cities'." *Financial Times*, June 9, 2021. <https://www.ft.com/content/76fdac7c-7076-47a4-bcb0-7e75af0aadab>.
- Lacheca, Dean. "National and Federal Governments' 2024 CIO Agenda: Insights and Data." *Gartner, Inc.*, January 2024.
- Lacheca, Dean. "State and Local Governments' 2024 CIO Agenda Insights and Data." *Gartner, Inc.*, January 2024.
- Ling, Justin. "To Beat Russia, Ukraine Needs a Major Tech Breakthrough." *WIRED*, January 4, 2024. <https://www.wired.com/story/ukraine-russia-future-war-tech/>.
- McDonald, Joe. "China Restricts Civilian Drone Exports, Citing Ukraine and Concern About Military Use." *AP News*, July 31, 2023. <https://apnews.com/article/china-ukraine-russia-drone-export-dji-e6694b3209b4d8a93fd76cf29bd8a056#:~:text=BEIJING%20%28AP%29%20%E2%80%94%20China%20imposed%20restrictions%20Monday%20on,says%20it%20is%20neutral%20in%20the%2017-month-old%20war>.
- Mickoleit, Arthur, et al. "Top Technology Trends in Government for 2023." *Gartner, Inc.*, May 2023.
- Mishra, DD, et al. "Market Guide for Enterprise IT Sustainability Services." *Gartner, Inc.*, August 2022.
- Mitchell, Russ. "How Amazon Put Ukraine's 'Government in a Box'—and Saved Its Economy from Russia." *Los Angeles Times*, December 15, 2022. <https://www.latimes.com/business/story/2022-12-15/amazon-ukraine-war-cloud-data>.
- Montgomery, Mark, & Eric Sayers, "Don't Let China Take Over the Cloud—US National Security Depends on It." *The Hill*, November 13, 2023. <https://thehill.com/opinion/national-security/4307002-dont-let-china-take-over-the-cloud-us-national-security-depends-on-it/>.
- Morris, Frank. "Slow Manufacturing and Price Gouging Threaten the New U.S. Military Arms Race." *NPR*, April 14, 2023. <https://www.npr.org/2023/04/07/1168725028/manufacturing-price-gauging-new-u-s-military-arms>.
- Nagar, Sarosh. "ZTE's Revenge: Russia's Technological Power Vacuum in the Wake of the Ukraine War." *Harvard International Review*, August 24, 2022.

<https://hir.harvard.edu/ztes-revenge-russias-technological-power-vacuum-in-the-wake-of-the-ukraine-war/>.

- Nouwens, Meia, & Helena Legarda. “China’s Pursuit of Advanced Dual-use Technologies.” International Institute for Strategic Studies, December 18, 2018. <https://www.iiss.org/research-paper/2018/12/emerging-technology-dominance>.
- Office of the Undersecretary of Defense for Research and Engineering. “Innovation Organizations.” Department of Defense. <https://www.ctoinnovation.mil/innovation-organizations/>.
- Orup Lund, Pia, et al. “Magic Quadrant for Supply Chain Planning Solutions.” Gartner, Inc., May 2023.
- Outpacing China: Expediting Innovation to the Warfighter, Before the United States House of Representatives Armed Services Committee, 118<sup>th</sup> Cong.* (2024) (statement of Douglas A. Beck, Director of Defense Innovation Unit).
- Pearson, James, & Christopher Bing. “The Cyber War Between Ukraine and Russia: An Overview.” Reuters, May 10, 2022. <https://www.reuters.com/world/europe/factbox-the-cyber-war-between-ukraine-russia-2022-05-10/>.
- “Pricing—Uncrewed Systems and Robotics Database.” AUVSI, 2022. <https://roboticsdatabase.auvsi.org/pricing>.
- Resnick, Marty, et al. <https://spectrum.ieee.org/drone-warfare-ukraine> “Predicts 2024: Prepare Today for the Impact of Future Forces.” Gartner, Inc., December 2023.
- Ross, Philip E. “Budget Drones in Ukraine Are Redefining Warfare: Small, Low-cost Tech Enables New Military Tactics.” IEEE Spectrum, May 17, 2023.
- Russel, Daniel R., & Berger, Blake H. “Weaponizing the Belt and Road Initiative.” Asia Society Policy Institute. September 2020. [https://asiasociety.org/sites/default/files/2020-09/Weaponizing%20the%20Belt%20and%20Road%20Initiative\\_0.pdf](https://asiasociety.org/sites/default/files/2020-09/Weaponizing%20the%20Belt%20and%20Road%20Initiative_0.pdf).
- Sahin, Kaan. “The West, China, and AI Surveillance.” Atlantic Council, December 18, 2020. <https://www.atlanticcouncil.org/blogs/geotech-cues/the-west-china-and-ai-surveillance/>.
- Sanchez Duran, Oscar, et al. “Market Guide for Last-Mile Delivery Technology Solutions.” Gartner, Inc. December 2022.
- Sallam, Rita, et al. “Top Trends in Data and Analytics, 2022.” Gartner, Inc., March 2022.
- Scharre, Paul. “Interview on February 2, 2024.” Interview by Jarrett Lane, February 2, 2024.
- Shanahan, Jack, Lieutenant General (ret.), “Interview on January 22, 2024.” Interview by Jarrett Lane, January 22, 2024.
- Shanler, Michael, et al. “Hype Cycle for Life Science Manufacturing, Quality and Supply Chain.” Gartner, Inc., July 2023.
- Shanler, Michael, and Rohan Sinha. “Market Guide for Laboratory Informatics.” Gartner, Inc., August 2021.

Stakeholder at a Geographic Combatant Command. “Interview on August 28, 2024.” In-person interview by Jarrett Lane. August 28, 2024.

Stakeholder at Air Force CyberWorx. “Interview on November 17, 2023.” Interview by EunRae Oh and Matthew Reed. November 17, 2023.

Stakeholder at Air Force Life Cycle Management Center. “Interview on August 15, 2023.” Interview by Abdullah Naimzadeh, EunRae Oh, and Matthew Reed. August 15, 2023.

Stakeholder at Big Safari. “Interview on August 8, 2023.” Interview by Abdullah Naimzadeh, EunRae Oh, and Matthew Reed. August 11, 2023.

Stakeholder at Department of Commerce. “Interview on September 13, 2023.” Interview by Abdullah Naimzadeh, EunRae Oh, and Matthew Reed. September 13, 2023.

Stakeholder at DSCA IOPS/WPNS. “Interview on August 15, 2023.” Interview by Abdullah Naimzadeh, EunRae Oh, and Matthew Reed. August 15, 2023.

Stakeholder at Institute for Defense Analyses. “Interview on July 28, 2023.” Interview by Abdullah Naimzadeh, EunRae Oh, and Matthew Reed, with email follow-up. July 28, 2023.

Stakeholder at Institute for Defense Analyses. “Interview on July 31, 2023.” In-person interview by Abdullah Naimzadeh and Matthew Reed. July 31, 2023.

Stakeholder at National Security Innovation Network, “Interview on August 7, 2023,” Interview by Abdullah Naimzadeh, EunRae Oh, and Matthew Reed, with email follow-up. August 7, 2023.

Stakeholder at National Security Innovation Network. “Interview on August 11, 2023.” interview by Abdullah Naimzadeh, EunRae Oh, and Matthew Reed, August 11, 2023.

Stakeholder at Office of the Undersecretary of Defense for Research & Engineering. “Interview on August 10, 2023.” Interview by Abdullah Naimzadeh, EunRae Oh, and Matthew Reed. August 10, 2023.

Stakeholder at SOF Vulcan, “Interview on September 29, 2023,” interview by Abdullah Naimzadeh, EunRae, and Matthew Reed.

Stakeholder at TechStars Space. “Interview on October 16, 2023.” Interview by Matthew Reed. October 16, 2023.

Stakeholder at TechStars. “Interview on November 8, 2023.” In-person interview by Abdullah Naimzadeh with email follow-up. November 8, 2023.

Stakeholder at the Catalyst Accelerator. “Interview on November 3, 2023” Interview by Abdullah Naimzadeh, EunRae Oh, and Matthew Reed. November 3, 2023.

Stakeholder at the Defense Security Cooperation Agency. “Interview on October 18, 2023.” Interview by EunRae Oh and Matthew Reed. October 18, 2023.

Stakeholder at the Department of the Air Force Artificial Intelligence Accelerator. “Interview on October 31, 2023.” Interview by Abdullah Naimzadeh, EunRae Oh, and Matthew Reed. October 31, 2023.



- Stakeholder at the Office of the Assistant Secretary of Defense for Industrial Base Policy. “Interview on November 14, 2023.” Interview by Abdullah Naimzadeh, EunRae Oh, and Matthew Reed. November 14, 2023.
- Stakeholder at the Office of the Deputy Assistant Secretary of the Army for Defense Exports and Cooperation. “Interview on September 29, 2023.” Interview by Matthew Reed. September 29, 2023.
- Stakeholder at the Office of the Undersecretary of Defense for Acquisition and Sustainment. “Interview on November 6, 2023.” Interview by Abdullah Naimzadeh, EunRae Oh, and Matthew Reed. November 6, 2023.
- Standards of Ethical Conduct for Employees of the Executive Branch, Code of Federal Regulations 5*, (1992), Part 2635.
- Stegman, Eric, et al. "IT Key Metrics Data 2020: Industry Measures—Executive Summary." Gartner, Inc., December 2019.
- Stegman, Eric, et al. "IT Key Metrics Data 2020: Industry Measures—Framework Definitions." Gartner, Inc., December 2019.
- Stegman, Eric, et al. "IT Key Metrics Data 2021: Industry Measures—Executive Summary." Gartner, Inc., December 2020.
- Stegman, Eric, et al. "IT Key Metrics Data 2022: Industry Measures—Executive Summary." Gartner, Inc., December 2021.
- Stegman, Eric, et al. "IT Key Metrics Data 2023: Industry Measures—Executive Summary." Gartner, Inc., December 2022.
- Stegman, Eric, et al. "IT Key Metrics Data 2024: Industry Measures—Executive Summary." Gartner, Inc., December 2023.
- Syamsudin, Ahmad, & Chen Mei Hua. “Huawei’s Role in Indonesia Raises Digital Colonization Concerns.” Radio Free Asia, September 27, 2023. <https://www.rfa.org/english/news/china/china-bri-indonesia-09272023104442.html>.
- Tan, Huileng. “Ukraine’s 285,000 IT Specialists Power Apps and Software around the Globe, and Many of Them Are Still Working from Ukraine as the War Rages around Them.” Business Insider, April 8, 2022. <https://www.businessinsider.com/ukraine-it-specialists-still-working-through-war-2022-4>.
- Titze, Christian, et al. “Cool Vendors in Cross-Functional Supply Chain Management Technology.” Gartner, Inc. August 2023.
- “Uncrewed Systems & Robotics Database” AUVSI. <https://www.auvsi.org/usrd>.
- “Ukraine War Drone Incidents 2024,” Google Sheets, <https://docs.google.com/spreadsheets/d/1oItrQ7RceC8w1eR2tppoqSz3zHhW1-tZkrU7yfZTqAU/edit#gid=0>.
- U. S. Department of Commerce, Industry and Security Bureau, “Additions of Entities to the Entity List and Removal of Entity from the Entity List.” Federal Register, June 14, 2023. <https://www.federalregister.gov/documents/2023/06/14/2023->

12726/additions-of-entities-to-the-entity-list-and-removal-of-entity-from-the-entity-list.

- U.S. Department of Commerce, Bureau of Industry and Security. *Advisory Opinion Regarding Cloud Computing Service Providers*, by C. Randall Pratt, 2011, <https://www.bis.doc.gov/index.php/documents/advisory-opinions/533-cloud-computing-and-deemed-exports/file>.
- U.S. Department of Commerce, Bureau of Industry and Security. (n.d.). Export Administration Regulations. <https://www.bis.gov/ear>.
- U.S. Department of Commerce, Bureau of Industry and Security. “Additions and Revisions to the Entity List and Conforming Removal from the Unverified List,” December 19, 2022. <https://public-inspection.federalregister.gov/2022-27151.pdf>. <https://www.bis.doc.gov/index.php/regulations/export-administration-regulations-ear>.
- U.S. Department of Commerce, International Trade Administration. “Aerospace and Defense Exporter Alert, February 2024.” February 26, 2024. <https://content.govdelivery.com/accounts/USITATRADE/bulletins/38a8c39>.
- U.S. Department of Defense. “Department of Defense Enhances Technology Transitions Through New Advisory Group.” April 10, 2024, accessed August 13, 2014. <https://www.defense.gov/News/Releases/Release/Article/3736929/department-of-defense-enhances-technology-transitions-through-new-advisory-group/>.
- U. S. Department of Defense. “Military and Security Developments Involving the People’s Republic of China.” U.S. Department of Defense, 2023. <https://media.defense.gov/2023/Oct/19/2003323409/-1/-1/1/2023-MILITARY-AND-SECURITY-DEVELOPMENTS-INVOLVING-THE-PEOPLES-REPUBLIC-OF-CHINA.PDF>.
- U.S. Department of Defense. “Transition Tracking Action Group (TTAG) Charter,” March 13, 2024, accessed September 3, 2024. <https://media.defense.gov/2024/Apr/10/2003435539/-1/-1/0/ESTABLISHMENT-OF-THE-TRANSITION-TRACKING-ACTION-GROUP-TTAG-CHARTER.PDF>.
- U.S. Department of Defense, Joint Chiefs of Staff. *Universal Joint Task List*. 2024. [https://www.jcs.mil/Portals/36/Documents/Doctrine/training/ujtl\\_tasks.pdf?ver=C-PWxKHQGWo00CB3IQBhTg%3d%3d](https://www.jcs.mil/Portals/36/Documents/Doctrine/training/ujtl_tasks.pdf?ver=C-PWxKHQGWo00CB3IQBhTg%3d%3d)
- U. S. Department of Defense, Office of the Executive Director for Systems Engineering and Architecture, Office of the Under Secretary of Defense for Research and Engineering. *Technology Readiness Assessment Guidebook*. U.S. Department of Defense, June 2023. <https://www.cto.mil/wp-content/uploads/2023/07/TRA-Guide-Jun2023.pdf>.
- U.S. Department of Defense, Office of the Secretary of Defense. *DoD Directive 5105.65: Defense Security Cooperation Agency (DSCA)*. Arlington, Virginia, 2012. <https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/510565p.pdf>.
- U.S. Department of Defense, Office of the Secretary of Defense. *DoD Directive 5132.03: DoD Policy and Responsibilities Relating to Security Cooperation*. Arlington,

- Virginia, 2016.  
[https://open.defense.gov/portals/23/Documents/foreignasst/DoDD\\_513203\\_on\\_Security\\_Cooperation.pdf](https://open.defense.gov/portals/23/Documents/foreignasst/DoDD_513203_on_Security_Cooperation.pdf).
- U.S. Department of Defense. *2022 National Defense Strategy of the United States of America*. October 27, 2022. <https://media.defense.gov/2022/Oct/27/2003103845/-1/-1/1/2022-NATIONAL-DEFENSE-STRATEGY-NPR-MDR.PDF>.
- U.S. Department of Homeland Security, Science and Technology. “National Urban Security Technology Laboratory.” <https://www.dhs.gov/science-and-technology/national-urban-security-technology-laboratory>.
- U.S. Department of Homeland Security, National Urban Security Technology Laboratory. “Saver Technote: Laser Protective Eyewear.” January 2022. [https://www.dhs.gov/sites/default/files/2022-01/SAVER\\_Laser%20Protective%20Eyewear\\_TechNote\\_508%20final\\_18Jan2022.pdf](https://www.dhs.gov/sites/default/files/2022-01/SAVER_Laser%20Protective%20Eyewear_TechNote_508%20final_18Jan2022.pdf).
- U.S. Department of Homeland Security. “System Assessment and Validation for Emergency Responders (SAVER) Program.” <https://www.dhs.gov/science-and-technology/saver>.
- U.S. Library of Congress, Congressional Research Service. *Department of Defense Contractors and Efforts to Mitigate Foreign Influence*, by Alexandra G. Neenan, R48110 (2024), 1.
- Weinbaum, Cortney, Caolionn O’Connell, Steven W. Popper, M. Scott Bond, Hannah Jane Byrne, Christian Curriden, Gregory Weider Fauerbach, Sale Lilly, Jared Mondschein, and Jon Schmid. “China’s Defense Industrial Base.” RAND. February 11, 2022. [https://www.rand.org/pubs/research\\_briefs/RBA930-1.html](https://www.rand.org/pubs/research_briefs/RBA930-1.html).
- West, Carly, and Oscar Sanchez Duran. “Market Guide for Transportation Mobility.” Gartner, Inc., August 2022.
- West, Carly, and Oscar Sanchez Duran. “Use-Case Prism: Artificial Intelligence for Transportation.” Gartner, Inc., January 2023.
- “What Is Software-defined Networking (SDN)?.” IBM, accessed August 13, 2024. <https://www.ibm.com/topics/sdn>
- Wilkinson, Leland, and Michael Friendly. “The History of the Cluster Heat Map.” *The American Statistician* 63 no. 2, 179–84. <https://doi.org/10.1198/tas.2009.0033>



## Abbreviations

---

AI	artificial intelligence
AUKUS	Australia, United Kingdom, United States
AUVSI	Association for Uncrewed Vehicle Systems
C2	command and control
C4S	command, control, communications, and computer systems
CBRN	chemical, biological, radiological, and nuclear
CSO	commercial solution offering
COTS	commercial-off-the-shelf
DCC	direct commercial contract
DCS	direct commercial sales
DICE	Defense Innovation Community of Entities
DIO	Defense Innovation Organizations
DIU	Defense Innovation Unit
DoD	Department of Defense
DoDD	Department of Defense Directive
DSCA	Defense Security Cooperation Agency
DCSU	Defense Security Cooperation University
ERGT	Expeditionary Requirements Generation Team
FMF	Foreign Military Financing
FMS	Foreign Military Sales
FOCI	Foreign Ownership, Control, or Influence
GCC	Geographic Combatant Command
IDA	Institute for Defense Analyses
IED	improvised explosive device
ISR	intelligence, surveillance, and reconnaissance
IT	information technology
LOR	Letter of Request
MASINT	measurement and signals intelligence
MILDEP	military department
NATO	North Atlantic Treaty Organization
NDS	National Defense Strategy
OUSD A&S	Office of the Undersecretary of Defense for Acquisition and Sustainment
PRC	People's Republic of China
RFP	request for proposal
SCO	Security Cooperation Organization
SOF	Special Operations Forces
TRL	technology readiness level
TTAG	Transition Tracking Action Group

UAS	unmanned aerial system
UJTL	Universal Joint Task List
USD R&E	Under Secretary of Defense for Research and Engineering
VEO	violent extremist organization

**REPORT DOCUMENTATION PAGE**

*Form Approved  
OMB No. 0704-0188*

The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

**PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.**

<b>1. REPORT DATE</b> ( <i>DD-MM-YYYY</i> )	<b>2. REPORT TYPE</b>	<b>3. DATES COVERED</b> ( <i>From - To</i> )
---	-----------------------	--

<b>4. TITLE AND SUBTITLE</b>	<b>5a. CONTRACT NUMBER</b>
	<b>5b. GRANT NUMBER</b>
	<b>5c. PROGRAM ELEMENT NUMBER</b>

<b>6. AUTHOR(S)</b>	<b>5d. PROJECT NUMBER</b>
	<b>5e. TASK NUMBER</b>
	<b>5f. WORK UNIT NUMBER</b>

<b>7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)</b>	<b>8. PERFORMING ORGANIZATION REPORT NUMBER</b>
---	---

<b>9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)</b>	<b>10. SPONSOR/MONITOR'S ACRONYM(S)</b>
	<b>11. SPONSOR/MONITOR'S REPORT NUMBER(S)</b>

**12. DISTRIBUTION/AVAILABILITY STATEMENT**

**13. SUPPLEMENTARY NOTES**

**14. ABSTRACT**

**15. SUBJECT TERMS**

<b>16. SECURITY CLASSIFICATION OF:</b>			<b>17. LIMITATION OF ABSTRACT</b>	<b>18. NUMBER OF PAGES</b>	<b>19a. NAME OF RESPONSIBLE PERSON</b>
a. REPORT	b. ABSTRACT	c. THIS PAGE			<b>19b. TELEPHONE NUMBER</b> ( <i>Include area code</i> )