SYM-AM-24-059

Excerpt from the Proceedings

of the

Twenty-First Annual Acquisition Research Symposium

Acquisition Research: Creating Synergy for Informed Change

May 8–9, 2024

Published: April 30, 2024

Prepared for the Naval Postgraduate School, Monterey, CA 93943.

Disclaimer: The views represented in this report are those of the author and do not reflect the official policy position of the Navy, the Department of Defense, or the federal government.

The research presented in this report was supported by the Acquisition Research Program at the Naval Postgraduate School.

To request defense acquisition research, to become a research sponsor, or to print additional copies of reports, please contact any of the staff listed on the Acquisition Research Program website (www.acquisitionresearch.net).

Acquisition Research Program
Department of Defense Management
Naval Postgraduate School

Acquiring Technology for Allies and Partners

Matthew Reed—is a researcher at the Institute for Defense Analyses (IDA). [mreed@ida.org]

Abu Naimzadeh—is a researcher at the Institute for Defense Analyses (IDA). [anaimzad@ida.org]

Jarrett Lane—is a researcher at the Institute for Defense Analyses (IDA). [jlane@ida.org]

EunRae Oh—is a researcher at the Institute for Defense Analyses (IDA). [eoh@ida.org]

Jennifer Taylor—is a research staff member at the Institute for Defense Analyses (IDA). [jtaylor@ida.org]

Abstract

The Institute for Defense Analyses (IDA) produced and submitted this paper for the Naval Postgraduate School's 21st Annual Acquisition Research Symposium, May 8–9, 2024, in Monterey, CA, as a discussion draft.

The Defense Security Cooperation Agency (DSCA) asked IDA to assist in developing new approaches to providing capabilities to partner nations—particularly commercially available capabilities 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. This paper offers a summary of research, findings, and potential recommendations for how the Department of Defense's (DoD's) security cooperation community, DSCA, and defense innovation organizations (DIOs) can develop new business strategies for incorporating commercially available capabilities into security assistance activities.

The project team's methodology included expert interviews and literature reviews. The project team conducted structured interviews with government, industry, and IDA experts on commercial technologies and their potential military applications, defense innovation initiatives, and security cooperation programs. The project team completed literature reviews to understand known and potential uses of commercial technologies by partners nation militaries. Finally, through a combined approach of expert interviews and literature reviews, the project team developed a heatmap designed to highlight which commercial technologies may yield the greatest impact on the ability of a partner nation's military to execute critical tasks. It is the IDA team's hope that this paper will elicit constructive feedback and insights that can further shape our research and recommendations to DSCA.

The 2022 U.S. National Defense Strategy (Austin, 2022) highlights the importance of leveraging commercial technologies and innovation to maintain U.S. warfighting advantages. Further, the use of commercial technologies in the Ukraine war demonstrates their utility and impact in modern conflict. While the DoD is increasingly investing in commercial technologies, there is no strategy for helping partner nations understand potential uses for commercial technologies; identify viable solutions in the commercial market; and acquire, integrate, and use commercial technologies in warfighting and task execution. DSCA's strategy and processes for enhancing partner nations' capabilities lean heavily on sales and transfers of hardware, platforms, and systems that were developed for the U.S. military and covered by current and past programs of record. These are often more expensive, harder to maintain, and more difficult to replace than commercially available capabilities.

Problem Statement

Commercial technologies can improve partner nations' capabilities across functional areas and tasks critical to self-defense and deterrence. However, the Defense Security Cooperation Agency's (DSCA's) current approach to enhancing partner nations' capabilities leans heavily on sales and transfers of traditional hardware, platforms, and systems—both 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. Further, many of these capabilities were developed in the context of U.S. military missions and the way in which the U.S. warfighter will act in conflict, which may be different from the approach of a partner military. Helping partner nations incorporate commercial technologies into their operations presents an opportunity to both improve their ability to counter Chinese and Russian aggression and improve the U.S.'s position as a partner of choice.

In an effort to displace the United States and establish itself as the partner of choice, the People's Republic of China (PRC) is capitalizing on shortcomings in the United States' current approach to security assistance (e.g., expensive items and long acquisition cycles) by incorporating cost-effective and agile commercial, dual-use technologies into its security assistance packages and foreign military sales. For example, Huawei sold cybersecurity capabilities to Indonesia's National Cyber and Crypto Agency—roughly equivalent to the U.S. National Security Agency (Syamsudin, 2023). The PRC can often provide its commercially available capabilities faster and cheaper than the United States, creating technological and economic dependencies that provide the PRC with global influence among U.S. partners (Nagar, 2022; Nouwens & Legarda, 2018; Russel & Berger, 2020).

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 development efforts and to advance dual-use technology projects (Cheng, 2023; China Power Team, 2018; DoD, 2023; Nouwens & Legarda, 2018). 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 (Nouwens & Legarda, 2018). Between 2022 and 2023, the U.S. Department of Commerce added more than 70 Chinese technology companies to the Entity List[1] 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 (Additions and Revisions to the Entity List and Conforming Removal from the Unverified List, 2022, p. 3; Additions of Entities to the Entity List and Removal of Entity from the Entity List, 2023). In fact, according to a 2022 RAND report, almost half of the PRC's manufacturing output is considered dual-use (Weinbaum et al., 2022, p. 4).

The PRC's civil-military fusion strategy also aligns with its Belt and Road Initiative—a strategy for growing the PRC's economic and political global influence (Syamsudin, 2023). 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 (Bouey et al., 2023; Montgomery & Sayers, 2023; Sahin, 2020). Since 2009, Chinese technology companies have sold cyber capabilities to Indonesia's National Cyber and Crypto Agency and signed contracts with more than 140 countries to install automated "safe city" surveillance equipment (including facial recognition technology) that allows governments to monitor cities and towns (Kynge et al., 2021).

[1] 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.

The PRC can also lean on ubiquitous availability of some Chinese-produced technologies—including commercial drones—to foster partnerships and become a source of low-cost, quickly acquirable capabilities. DJI, a Chinese commercial drone company, accounts for 70% of the global drone market (Anwar, 2023). In 2023, the Chinese government imposed new exports controls on commercial drones, ostensibly to curb militarized use of DJI and other Chinese-produced commercial drones (McDonald, 2023). However, DJI and other Chinese drones remain readily accessible and used for military purposes (Gosselin-Malo, 2023). Thus, helping partner nations acquire and use U.S. and/or allied-produced commercial technologies is important to ensuring the United States remains the partner of choice for national defense capability and capacity building.

Leveraging commercial technology is not only essential to defending American alliances and influence abroad, but is also key to helping U.S. partner nations deter and defend themselves against aggression in cost-effective and adaptable ways. The war in Ukraine highlights the potential impact of helping partners apply commercial technologies to bolstering deterrence and self-defense vis-à-vis larger aggressors. The first salvo in Russia's invasion was massive, widespread cyberattacks. In response, the Ukrainian government rapidly transitioned data and operations to commercial cloud environments which significantly improved the government's resilience against cyberattacks. Using edge computing devices, 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. At an industry event in November 2022, Ukraine's Vice Prime Minister and Minister of Digital Transformation, Mykhailo Federov, explained,

> We experience cyberattacks on a daily basis; this is a cyberwar. Under attack is our critical infrastructure. But we have been successful in protecting [it], and every week we are launching some new public resources. Digitalization is the best response to this challenge. (Konkel, 2022)

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. 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 (Borger, 2022). 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 (Jones et al., 2023).

Ukraine's use of commercial drones also serves as an example of the potential cost and speed advantages of commercial, dual-use technologies. Drones are enabling Ukrainian forces to efficiently and effectively deliver results that are traditionally achieved—at least in the context of U.S. doctrine—through artillery, missiles, and sophisticated platforms (e.g., aircraft). For example, Ukraine is using commercial drones to develop loitering munitions that target armor, weapons systems, entrenched combatants, and more. 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 cannot replace or eliminate the need for traditional materiel like artillery shells, but they may be useful in mitigating risks in supply shortages and augmenting partners' warfighting plans, and tactics. Ukraine's use of commercially available capabilities are not only cost-effective, they are 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 (Morris, 2023). 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 (Morris, 2023).

The *2022 National Defense Strategy* (*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 allies and partners as well (Austin, 2022, p. 19). The strategy states, "The [Department of Defense] will support the innovation ecosystem both at home and in expanded partnerships with our Allies and partners." The *NDS* also notes that the Department 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. (Austin, 2022, p. 8).

Notwithstanding recognition of commercial technologies' potential impact on partner nations' warfighting capabilities, there is currently no established lead, strategy, or initiative to help partner nations understand potential uses for commercial technologies; identify viable solutions in the commercial market; and acquire, integrate, and use commercial technologies in warfighting and task execution. To help address this gap, the DSCA aims to develop new approaches for providing innovative commercial capabilities to partners.

Defense Innovation Organizations: Insights and Lessons Learned

As a first step to help DSCA identify commercially available capabilities, the Institute for Defense Analyses (IDA) team researched whether defense innovation organizations (DIOs) are incorporating partner nations into their activities, as well as how DSCA could collaborate with DIOs to help partner nations procure and integrate commercially available capabilities. IDA engaged with 17 DIOs and interagency organizations to determine if DSCA can access their data and insights into commercially available capabilities. IDA also captured lessons learned about how the organizations interact with industry and explored opportunities and challenges to leveraging the organizations' expertise and resources to support moderately capable partner nations.[2]

Through this research, IDA found that the DIOs generally 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 Department of Defense. In cases where 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. There are periodic engagements with moderately capable partners, though typically in response to an active conflict or acute problem (e.g., the war in Ukraine).[3] However, the DIOs do not have focused lines of effort or goals associated with helping partner nations leverage commercially available capabilities.

IDA found that individuals throughout DIOs recognize the importance of supporting partner nations and expressed willingness to help DSCA on a case-by-case basis. Working with willing leaders and individuals within DIOs may allow DSCA to tap the DIOs' networks,

[2] Loosely defined, "moderately capable partner nations" are partners with limited resources that have the potential to fight alongside or in lieu of U.S. forces. These partners are DSCA's priority focus for developing new approaches to delivering commercially available capabilities.

[3] See, for example, the Defense Innovation Unit'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 (Beck, 2024).

expertise, and capabilities for identifying, vetting, and sourcing commercially available capabilities. Connecting DIOs' knowledge of commercial capabilities with the expertise of DSCA and Security Cooperation Organizations (SCOs) has the potential to deliver value to partner nations. But, until DIOs are appropriately resourced and directed to support partner nations, scaling collaboration between DSCA and DIOs will be difficult and engagements will be reliant on the goodwill and bandwidth of DIO team members.

Innovation Organizations: Data Sources

The Undersecretary for Research and Engineering identified 271 DoD organizations as "innovation organizations."[4] One of these organizations, the Defense Innovation Unit (DIU), reported in FY 2022 that they received over 1,600 pitches from industry. That same year, the DIU delivered 82 prototypes and transitioned 17 capabilities (DIU, 2023). 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. The DIU and other DIOs curate their 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.

DIOs and interagency organizations often work closely with trade associations. Working with trade associations (e.g., the Association for Uncrewed Vehicle Systems International) could help DSCA scale outreach and engagement with industry, as well as access datasets maintained by the associations on members and their respective products (AUVSI, n.d.). For example, the Association of Drone Manufacturers maintains a dataset that is accessible for a fee and updated daily with technical specifications and contact information for specific drones (AUVSI, 2022).

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).[5] Although not all of these technologies are going to be U.S.- or ally-provided, DSCA can use open-source reporting and researcher datasets to find examples of technologies and products used by military and security forces globally. Additionally, 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) will give DSCA insights into key trends and potential solutions for partner nations.

Innovation Organizations: Opportunities for Collaboration

IDA met with innovation organizations that 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." 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.

[4] Not all of these organizations conduct substantial commercial outreach for mature technologies; others engage in deeper, longer-term technology development, technology assessments, or some other role in the tech development process (DoD Innovation Pathways, n.d.).

[5] See, for example, a publicly accessible spreadsheet covering drone incidents in Ukraine accessible on Google (*Ukraine Drone War Incidents 2024*). This database was highlighted by *Foreign Policy* in a February 2023 article, "The Drone War in Ukraine is Deadly, Cheap, and Made in China" (Greenwood, 2023).

Collaborating with innovation organizations can also help DSCA identify vetted, proven capabilities critical to ensuring partner nations acquire effective solutions and mitigating risks of deploying untrustworthy or unproven technologies. For example, the 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 U.S. allies (e.g., unmanned aerial systems [UAS] for first responders, counter-UAS, counter-improvised explosive device, and protection against lasers; U.S. Department of Homeland Security, n.d.-a, n.d.-b; National Urban Security Technology Laboratory, 2022) DHS indicates that they are willing to provide access to non-public documents for other federal agencies (U.S. Department of Homeland Security, n.d.-c).

In addition, some technology accelerators partner with DoD research organizations to technically vet members of their defense portfolios (Director of Private Sector Technology Accelerator, personal communication [phone interview], November 16, 2024). 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 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 in response to a clear demand from partner nations. 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,[6] but Commerce does not collect data on U.S. corporate participation, nor does Commerce conduct technical vetting.

Innovation Organizations: Barriers and Challenges to Collaboration

Though DIOs indicated openness to partnering with DSCA, there are legal and policy roadblocks to data sharing. For example, contractual and policy restrictions designed to safeguard proprietary and competitive industry data inhibits the transfer of technical data to other DoD organizations, creating a hesitance or inability for DIOs to provide unlimited data access to DSCA. 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 and scale of requests. This can be mitigated by creating more targeted, specific requests to individual program managers for data already organized. However, 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 that DIU could provide a pathway for streamlining data requests as DIU takes on responsibility for coordinating activities across DIOs. DIU Director Doug Beck recently 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

[6] See, for example, a March 2024 webinar organized by the U.S. Department of Commerce regarding defense export opportunities in the Philippines (U.S. Department of Commerce Industry & Analysis-Aerospace Office and U.S. Commercial Service, 2024).

> 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. (Beck, 2024)

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.

Heatmap: Prioritizing Technologies and Capabilities

Following its findings that DIOs are willing to assist DSCA but lack the mission and capacity to scale activities supporting partner nations, the IDA team recalibrated its efforts to helping DSCA determine ways it could lead, scale, and sustain efforts to help partner nations harness commercially available 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 moderately capable partners. However, commercially available capabilities will not be appropriate for all missions and tasks, and some capabilities may not be relevant to moderately capable partners. Nor is it 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, etc.; see Appendix A). 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 (Wilkinson & Friendly, 2009). 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.

Heatmap Methodology

To build the heatmap, the project 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 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 typical moderately capable partners:

1. **Applicability.** Technologies must be relevant to measurably improving and/or enabling a partner nations' defense and deterrence of larger aggressors.
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) seven or higher.[7] This indicates the technologies are no longer experimental and have been successfully prototyped, at a minimum, 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 DoD to partner nations (e.g., via international military education and training [IMET]).[8]

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). UJTLs that may be applicable to moderately capable partners were included, whereas highly advanced or U.S.-only tasks were excluded. Examples of excluded functional areas and tasks are those pertaining to nuclear capabilities and top secret–level communications networks.

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

[7] Note that TRLs are not typically 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 (Office of the Under Secretary of Defense for Research and Engineering, 2023).

[8] IMET is a program that provides U.S. government funds for international military personnel to attend educational programs and training at U.S. military facilities.

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. The IDA team collaborated with subject matter experts (e.g., technical experts, functional experts and leaders, 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.

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 five 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. **Multi-modal AI.** Multi-modal 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 intelligence, surveillance, and reconnaissance (ISR).
5. **Generative AI.** Generative AI has the potential to deliver impact across the vast majority of functional areas and tasks. Generative AI is a fast-developing technology and may have a larger impact on numerous tasks in the near future.

Beyond the top-five technologies, software-defined networking may also have a greater 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 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.

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.

After ISR, the following tasks rate highest in terms of their potential to benefit from commercial technologies.

- Measurement and signals intelligence (MASINT)
- Maritime warning (i.e., maritime domain awareness)
- Joint command and control
- IT infrastructure
- Special operations[9]

The heatmap also illustrates that though some technologies have the potential to deliver higher impacts, realizing their transformational potential within a functional area or task often requires integrating multiple technologies and designing end-to-end solutions. For example, though 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.

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.

Next Steps and Recommendations

The following recommendations are organized across three phases DSCA can follow to best develop and execute new business strategies for delivering commercially available capabilities to moderately capable partners.

Phase 0: Pilot

As an initial phase (or in parallel with the other phases we outline in this section), DSCA should scope a pilot in partnership with a DIO, such as the DIU. A pilot will allow DSCA to test how engagement and procurement models typically employed by DIOs could be used to address partner nation needs. Scoping the pilot to a proactive use case rather than a response to acute needs in conflict will enable DSCA to pressure-test commercially available capabilities and learn how to best incorporate them into security assistance packages and long-term security cooperation strategies.

The pilot could be structured into two parts: the first being a solicitation (e.g., needs discovery and requirements generation, problem statement development, solicitation release) in

[9] Much like the technologies included in the taxonomy, some functional areas and tasks may overlap or be subsets of another. For example, MASINT can be considered a subset or specific type of ISR. IDA is continuing to refine the structure of the functional areas and tasks included in the heatmap to account for this.

partnership with one or more DIOs and the Department of Commerce, and the second (pending successful outcomes from the first) being identification of viable solutions for a partner nation.[10]

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. Of the low-risk task areas for which commercially available capabilities may be most impactful, distribution and logistics and health services may be the best candidates. DSCA might also focus attention on an underdeveloped, but important, capability area that is expected to be a future priority for moderately capable partners.

Phase 1: Market Validation and Market 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.

Recommendation 1.1. Define DSCA's value proposition in enabling sales of commercially available capabilities to partner nations.

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 foreign military financing (FMF) could be used to facilitate direct commercial contracts (DCCs) of in-scope technologies. FMF may be useful for developing proofs of concept and pilots or for acquiring items for which there is little to no sustainment cost. DSCA could also explore other authorities that could be used to acquire commercial technologies.

Recommendation 1.2. 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. DSCA should also leverage in-house market analysis and lessons from ongoing engagements and work with moderately capable partners to validate their interest and ability to procure, use, and sustain commercially available technologies.

[10] 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 and its relevance to the partner 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.

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.

Recommendation 2.1. 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.

Recommendation 2.2. Develop training materials, resources, and guidance for SCOs.

SCOs are not trained today on commercially available capabilities, nor does guidance exist for how to identify if and when a commercially available capability may be a viable solution—viability not being determined only by functionality, but also factors such as cost, complexity, and sustainability—for an identified partner nation requirement. The Defense Security Cooperation University should consider ways to prepare security cooperation officers to address commercially available capabilities when engaging with partners.

Recommendation 2.3. 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:

Recommendation 2.3.1. Coordinate an industry outreach 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. The technologies priorities should be refined through information gathered during Phase 0 (pilot) and Phase 1.

Recommendation 2.3.2. Establish a consortium of industry partners who can advise and assist in the 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.

Recommendation 2.3.3. Subscribe to publicly available market intelligence platforms databases.

Acquiring access to commercial market intelligence platforms and databases can accelerate DSCA's visibility into technologies, companies, and industry trends.

Recommendation 2.3.4. Partner with DIOs and interagency offices with 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.

Phase 3: Execute and Scale

Recommendation 3.1. Conduct engagements with partner nations that can elucidate how they may apply commercial technologies in new, novel 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 engage with partner nations on ways that commercially available technologies can meet their requirements and priorities.

Recommendation 3.2. 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.

Recommendation 3.3. Collaborate with partner nations and industry to develop tailored strategies and roadmaps for effective 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 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 above, some partners may need assistance in recognizing the opportunities through commercially available military capabilities and the demands of absorbing, applying, and sustaining procured solutions.

Additional Considerations

Other factors 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:

- **Export controls.** Some technologies in the heatmap, including those that could significantly improve partner nations' capabilities, are subject to export controls.[11] 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

[11] See information on restrictions posted by the Bureau of Industry and Security (U.S. Department of Commerce, n.d.).

technologies that fall under export control restrictions. Interagency coordination and collaboration will likely be a core component of overcoming export-related blockers (and more).

- **Partner nations' culture of innovation and technical capacity.** There may be limitations to the lessons that can be drawn from Ukraine, particularly regarding the feasibility of helping other partner nations leverage commercially available capabilities for self-defense and deterrence. Ukraine's ability to innovate with commercial technologies may be due, in large part, to country's robust IT industry and sizeable technical workforce.[12] Further research should explore the importance of a culture of innovation for effective use of commercially available capabilities and ways to improve or encourage innovation within partner nations.
- **DSCA and SCO 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.
- **Procurement methods**. As noted above, FMF may present an option for facilitating procurements, but its utility is limited. Procurement methods must be timely as commercial technology evolves rapidly. Further research should include a careful examination of existing authorities, consideration of potential needs for new authorities, and engagement with both partner nations and industry to understand their procurement-related needs.

Conclusion

Commercially available technologies present significant opportunities for helping partner nations improve capabilities and also significant challenges. The IDA team continues to research this topic, and we appreciate the opportunity to present our findings to date at the 21st Annual Acquisition Research Symposium. We look forward to your feedback and engagement.

References

Additions of Entities to the Entity List and Removal of Entity from the Entity List, 15 C.F.R. § 744 (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

Additions and Revisions to the Entity List and Conforming Removal from the Unverified List, 88 Fed. Reg. 38739 (December 19, 2022). https://public-inspection.federalregister.gov/2022-27151.pdf

Anwar, N. (2023, February 7). *World's largest drone maker is unfazed—even if it's blacklisted by the U.S.* CNBC. https://www.cnbc.com/2023/02/08/worlds-largest-drone-maker-dji-is-unfazed-by-challenges-like-us-blacklist.html

Austin, L. (2022, October 27). *2022 national defense strategy*. U.S. Department of Defense. https://media.defense.gov/2022/Oct/27/2003103845/-1/-1/1/2022-NATIONAL-DEFENSE-STRATEGY-NPR-MDR.PDF

AUVSI. (2022). *Pricing—Uncrewed systems and robotics database.* https://roboticsdatabase.auvsi.org/pricing

[12] By some estimates, Ukraine's IT workforce totals 285,000 specialists who generate 4% of the national GDP (~$6.8 billion). Of that population, many are in the armed forces or work in national cyber defense (Kontsevoi, 2022; Tan, 2022).

AUVSI. (n.d.). *Uncrewed systems & robotics database*. https://www.auvsi.org/usrd

Beck, D. A. (2024). *“DIU 3.0” Scaling Defense Innovation for Strategic Impact*. Center for a New American Security. https://www.cnas.org/publications/reports/diu-3-0

Borger, J. (2022, December 18) “Our weapons are computers”: Ukrainian coders aim to gain battlefield edge. *Guardian.* https://www.theguardian.com/world/2022/dec/18/our-weapons-are-computers-ukrainian-coders-aim-to-gain-battlefield-edge

Bouey, J., Hu, L., Scholl, K., Marcellino, W., Dossani, R., Malik, A., Solomon, K., Zhang, S., & Shufer, A. (2023). *China’s AI exports: Technology distribution and data safety*. RAND. https://www.rand.org/pubs/research_reports/RRA2696-2.html

Cheng, E. (2023, March 5). *China to increase defense spending by 7.2%.* CNBC. https://www.cnbc.com/2023/03/05/china-defense-budget-two-sessions.html

China Power Team. (2018). *How dominant is China in the global arms trade?* CSIS. https://chinapower.csis.org/china-global-arms-trade/

Defense Innovation Unit. (2023). *DIU’s FY22 year-in-review*. https://www.diu.mil/fy22-year-in-review

DoD Innovation Pathways. (n.d.). *Innovation organizations*. https://www.ctoinnovation.mil/innovation-organizations/

Google. (n.d.). *Ukraine war drone incidents 2024*. Google Sheets. https://docs.google.com/spreadsheets/d/1oItrQ7RceC8w1eR2ttpoqSz3zHhW1-tZkrU7yfZTqAU/edit#gid=0

Gosselin-Malo, E. (2023). *Ukraine continues to snap up Chinese DJI drones for its defense*. C4ISRNet. https://www.c4isrnet.com/global/europe/2023/10/23/ukraine-continues-to-snap-up-chinese-dji-drones-for-its-defense/

Greenwood, F. (2023). The drone war in Ukraine is cheap, deadly, and made in China. *Foreign Policy*. https://foreignpolicy.com/2023/02/16/ukraine-russia-war-drone-warfare-china/

Jones, G., Egan, J., & Rosenbach, E. (2023). *Advancing in adversity: Ukraine’s battlefield technologies and lessons for the U.S.* Harvard Belfer Center. https://www.belfercenter.org/publication/advancing-adversity-ukraines-battlefield-technologies-and-lessons-us

Konkel, F. (2022). *Ukraine tech chief: Cloud migration “saved Ukraine government and economy.”* Nextgov. https://www.c4isrnet.com/global/europe/2023/10/23/ukraine-continues-to-snap-up-chinese-dji-drones-for-its-defense/

Kontsevoi, B. (2022, October 12). *The Ukrainian IT industry is alive and healthy*. Forbes. https://www.forbes.com/sites/forbestechcouncil/2022/10/12/the-ukrainian-it-industry-is-alive-and-healthy/?sh=5dd8f2d67f2c

Kynge, J., Hopkins, V., Warrell, H., & Hille., K. (2021). Exporting Chinese surveillance: The security risks of “smart cities.” *Financial Times.* https://www.ft.com/content/76fdac7c-7076-47a4-bcb0-7e75af0aadab

McDonald, J. (2023). *China restricts civilian drone exports, citing Ukraine and concern about military use.* AP News. 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

Montgomery, M., & Sayers, E. (2023). Don’t let China take over the Cloud—US national security depends on it. *The Hill.* https://thehill.com/opinion/national-security/4307002-dont-let-china-take-over-the-cloud-us-national-security-depends-on-it/

Morris, F. (2023, April 14). *Slow manufacturing and price gouging threaten the new U.S. military arms race*. NPR. https://www.npr.org/2023/04/07/1168725028/manufacturing-price-gauging-new-u-s-military-arms

Nagar, S. (2022). ZTE's revenge: Russia's technological power vacuum in the wake of the Ukraine war. *Harvard International Review.* https://hir.harvard.edu/ztes-revenge-russias-technological-power-vacuum-in-the-wake-of-the-ukraine-war/

National Urban Security Technology Laboratory. (2022, January). *Saver technote: Laser protective eyewear*. U.S. Department of Homeland Security. https://www.dhs.gov/sites/default/files/2022-01/SAVER_Laser%20Protective%20Eyewear_TechNote_508%20final_18Jan2022.pdf

Nouwens, M., & Legarda, H. (2018). *China's pursuit of advanced dual-use technologies.* International Institute for Strategic Studies. https://www.iiss.org/research-paper/2018/12/emerging-technology-dominance

Office of the Under Secretary of Defense for Research and Engineering. (2023). *Technology readiness assessment guidebook*. https://www.cto.mil/wp-content/uploads/2023/07/TRA-Guide-Jun2023.pdf

Russel, D., & Berger, B. (2020). *Weaponizing the belt and road initiative.* Asia Society Policy Institute. https://asiasociety.org/sites/default/files/2020-09/Weaponizing%20the%20Belt%20and%20Road%20Initiative_0.pdf

Sahin, K. (2020). *The West, China, and AI surveillance.* Atlantic Council. https://www.atlanticcouncil.org/blogs/geotech-cues/the-west-china-and-ai-surveillance/

Syamsudin, A. (2023). *Huawei's role in Indonesia raises digital colonization concerns.* Radio Free Asia. https://www.rfa.org/english/news/china/china-bri-indonesia-09272023104442.html

Tan, H. (2022, April 8). *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. https://www.businessinsider.com/ukraine-it-specialists-still-working-through-war-2022-4

U.S. Department of Commerce. (n.d.). *Export administration regulations*. Bureau of Industry and Security. https://www.bis.doc.gov/index.php/regulations/export-administration-regulations-ear

U.S. Department of Commerce Industry & Analysis-Aerospace Office and U.S. Commercial Service. (2024, February 26). *Aerospace and defense exporter alert, February 2024*. International Trade Administration. https://content.govdelivery.com/accounts/USITATRADE/bulletins/38a8c39

U.S. Department of Defense. (2023). *Military and security developments involving the People's Republic of China*. 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 Homeland Security. (n.d.-a). *Blue UAS for first responders*. https://www.dhs.gov/science-and-technology/saver/blue-uas-first-responders

U.S. Department of Homeland Security. (n.d.-b). *National urban security technology laboratory*. https://www.dhs.gov/science-and-technology/national-urban-security-technology-laboratory

U.S. Department of Homeland Security. (n.d.-c). *System assessment and validation for emergency responders (SAVER) program*. https://www.dhs.gov/science-and-technology/saver

Weinbaum, C., O'Connell, C., Popper, S., Bond, S., Byrne, H., Curriden, C., Weider Fauerbach, G., Lilly, S., Mondschein, J., & Schmid, J. (2022). *China's defense industrial base.* RAND. https://www.rand.org/pubs/research_briefs/RBA930-1.html

Wilkinson, L., & Friendly, M. (2009). The history of the cluster heat map. *The American Statistician*, *63*(2), 179–184. https://doi.org/10.1198/tas.2009.0033

Acquisition Research Program
Department of Defense Management
Naval Postgraduate School
555 Dyer Road, Ingersoll Hall
Monterey, CA 93943

www.acquisitionresearch.net