Delhi Policy Group

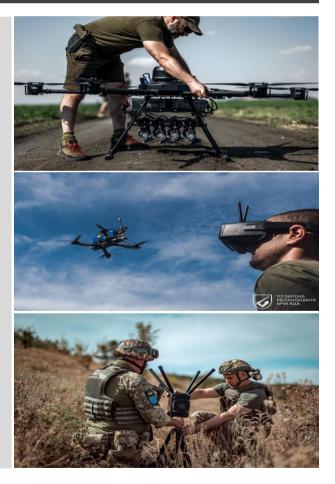Advancing India's Rise as a Leading Power

POLICY BRIEF

Harnessing Commercial Technology for Future Wars: The Lessons from Ukraine

Author

Deependra Singh Hooda

Volume IX, Issue 23

September 13, 2024

ABOUT US

Founded in 1994, the Delhi Policy Group (DPG) is among India's oldest think tanks with its primary focus on strategic and international issues of critical national interest. DPG is a non-partisan institution and is independently funded by a non-profit Trust. Over past decades, DPG has established itself in both domestic and international circles and is widely recognised today among the top security think tanks of India and of Asia's major powers.

Since 2016, in keeping with India's increasing global profile, DPG has expanded its focus areas to include India's regional and global role and its policies in the Indo-Pacific. In a realist environment, DPG remains mindful of the need to align India's ambitions with matching strategies and capabilities, from diplomatic initiatives to security policy and military modernisation.

At a time of disruptive change in the global order, DPG aims to deliver research based, relevant, reliable and realist policy perspectives to an actively engaged public, both at home and abroad. DPG is deeply committed to the growth of India's national power and purpose, the security and prosperity of the people of India and India's contributions to the global public good. We remain firmly anchored within these foundational principles which have defined DPG since its inception.

Author

Lt. Gen. Deependra Singh Hooda (Retd.), PVSM, UYSM, AVSM, VSM & Bar, Senior Fellow for Military Strategy, Delhi Policy Group

The views expressed in this publication are those of the author and should not be attributed to the Delhi Policy Group as an Institution.

Cover Photographs:

Ukrainian service man operating Vampire bomber drone on September 7, 2024.
(Source: Ministry of Defence of Ukraine/Official X Account)
Drone monitoring of the 117th Mechanized Brigade on August 28, 2024.
(Source: Ministry of Defence of Ukraine/Official X Account)
The electronic warfare company of the 110th Mechanized Brigade of Ukraine on August 31, 2024.
(Source: Ministry of Defence of Ukraine/Official X Account)

Harnessing Commercial Technology for Future Wars:
The Lessons from Ukraine
by
Deependra Singh Hooda

Contents

Harnessing Commercial Technology for Future Wars:
The Lessons from Ukraine
by
Deependra Singh Hooda

Introduction

Picture a battlefield where victory hinges not only on sheer numbers or firepower but on the ability to swiftly adapt, innovate, and outmanoeuvre the enemy through the use of cutting-edge technology. This is no longer a futuristic vision but a reality of modern warfare. Traditional military forces, once reliant on large, costly platforms, now face the urgent need to integrate agile, high-tech solutions into their operations, redefining what it takes to win in today's conflicts.

The ongoing war in Ukraine reveals that warfare hinges as much on commercial innovation as on conventional military might. Drones once intended for hobbyists now guide artillery with pinpoint accuracy; satellite internet systems initially designed for remote connectivity ensure uninterrupted communication on the front lines; cybersecurity tools from private firms fend off digital assaults. These examples from the Ukraine conflict are not just anomalies - they signal a shift in how wars are fought and won.

Over the past few decades, the locus of technological innovation has markedly shifted from the defence sector to private companies. Historically, defence-related research and development (R&D) were the primary drivers of technological advancements, with innovations like the internet and GPS originating from military projects. However, in recent years, private sector R&D has outpaced that of defence, both in terms of funding and the pace of innovation.

In 2023, R&D spending by the top 2,500 corporate companies reached an estimated $1.4 trillion, with tech giants like Meta, Alphabet, and Microsoft, each investing over $34 billion annually in R&D.[1] Private companies are now at the forefront of technological development, driving innovations in areas such as artificial intelligence (AI), cybersecurity, autonomous systems, quantum

---

[1] "R&D Spending by the Top 2,500 R&D Spenders Crossed the €1.3 Trillion Mark in 2022." Accessed August 12, 2024. https://www.wipo.int/global_innovation_index/en/gii-insights-blog/2024/r-and-d-spenders.html.

computing, and virtual reality - technologies that are increasingly critical to modern warfare.

This brief explores the critical need for defence planners and military forces to forge strong partnerships with commercial entities, particularly non-traditional military suppliers and startups, to adopt and integrate cutting-edge technologies. The Ukraine war serves as a compelling case study, illustrating that the future of warfare will be shaped not only by state-of-the-art military platforms, but also by the innovative solutions born from commercial collaboration.

The Ukraine War: A Case Study

The Ukraine war offers a powerful and contemporary example of how commercial technologies have become crucial in a modern conflict. The supply of weapon systems like HIMARS, Bradley Fighting Vehicles, air defence and anti-tank systems, have been of tremendous help to Ukraine in beating back the initial Russian offensive. However, the role played by private companies has enabled Ukraine to continue resisting a conventionally superior force in a war that has now lasted two and a half years. This section delves into specific instances where commercial innovation played a pivotal role in shaping the dynamics of the war.

(i) Drone Wars

Drones have dominated the skies over Ukraine. The initial stages of the war saw the use of military-specific Turkish TB2 Bayraktar and the US Switchblade drone. However, as the war progressed, the focus shifted to smaller commercial drones like the Chinese DJI Mavic, costing $2000, and now to First Person View (FPV) drones costing as little as $500. These drones are employed for gathering information, coordinating artillery fires, and carrying out direct strikes on military targets.

Reports suggest that Ukraine is losing around 10,000 drones each month,[2] highlighting just how extensively they are being used in the conflict. The domestic production of drones has rapidly expanded, with around 200 companies producing drones in Ukraine, compared to just seven at the start of the war.[3]

---

[2] "Meatgrinder: Russian Tactics in the Second Year of Its Invasion of Ukraine," August 14, 2024. https://rusi.orghttps://rusi.org.

[3] Kitsoft. "Cabinet of Ministers of Ukraine - Prime Minister: Our Key Task Is to Intensify Production of Drones, Ammunition and Other Modern Weapons." Accessed August 14,

As manufacturing expands, Ukraine has set a target of more than one million domestically produced drones in 2024 – around double the number of artillery shells supplied by the European Union over the past year.[4] A coalition of around ten countries has promised to deliver one million more drones to Ukraine by February 2025.[5]

Early in the war, the Russians relied on the Iranian Shahed kamikaze drones, which are now being domestically produced. However, the vulnerability of this relatively large UAV led them to switch to smaller Orion, Eleron-3, Orlan-10, and Lancet drones.[6] The Russian military was slow to adopt commercial drones, but that appears to be changing. Military quadcopter production has gone from nothing to 100,000 a month.[7]

Despite the increase in production, Russia has not been as effective as Ukraine in utilising its commercial sector in the drone war. Some reasons for this are Russia's centralised procurement process, a preference for military-grade equipment, and a lack of support for startups.[8] There are lessons in this for militaries which wish to take advantage of commercial technologies.

(ii) AI on the Battlefield

The war in Ukraine has become a giant lab for AI to be tested on the battlefield, and private companies are taking the lead. These companies have provided advanced AI and data analytics tools that have enhanced Ukraine's military intelligence and operational capabilities.

In June 2022, US-based company Palantir offered its services to the Kyiv government. Palantir's AI software integrates data from multiple sources such as satellite imagery, open-source data, drone footage, and reports from the ground to present commanders with military options. Today, Palantir is

---

2024. https://www.kmu.gov.ua/en/news/premier-ministr-nashe-kliuchove-zavdannia-aktyvizuvaty-vyrobnytstvo-bezpilotnykiv-boieprypasiv-inshoi-suchasnoi-zbroi.

[4] Zafra, Mariano, Max Hunder, Anurag Rao, and Sudev Kiyada. "How Drone Combat in Ukraine Is Changing Warfare." Reuters, March 26, 2024. https://www.reuters.com/graphics/UKRAINE-CRISIS/DRONES/dwpkeyjwkpm/.

[5] "Ukraine Is Losing the Drone War," May 27, 2024. https://www.intellinews.com/long-read-ukraine-is-losing-the-drone-war-323020/.

[6] Ibid

[7] Hambling, David. "Is Russian Drone Production Overtaking Ukraine?" Forbes. Accessed August 14, 2024. https://www.forbes.com/sites/davidhambling/2024/07/01/is-russia-overtaking-ukraine-in-drone-production/.

[8] Hambling, David. "Russian Drones Could Win This War, If Entrenched Bureaucracy Lets Them." Forbes. Accessed August 14, 2024. https://www.forbes.com/sites/davidhambling/2024/08/13/russian-drones-could-win-this-war-if-entrenched-bureaucracy-lets-them/.

responsible for most of the targeting by Ukrainian forces. The company's data analytics is also being used for projects like collecting evidence of war crimes, clearing land mines, resettling displaced refugees, and rooting out corruption.[9]

Clearview AI, an American facial-recognition company, has assisted the Ukrainian government in identifying over 230,000 Russian soldiers and officials involved in the military invasion. The company boasts the world's largest database of human faces, comprising 40 billion images scraped from the Internet. To counter Russian propaganda that denies their troops are suffering heavy casualties, Ukraine's Ministry of Internal Affairs launched a website called Poter.net, named after the Russian term for "No Losses." The site features a searchable database of dead Russian soldiers, identified with the help of Clearview's technology.[10]

Primer has contributed by providing AI-driven natural language processing (NLP) tools that help rapidly analyse and translate large volumes of Russian communications and highlight critical statements relevant to the battlefield situation. This capability has been crucial in identifying threats, understanding enemy tactics, and disseminating information quickly across military units.

Additionally, many smaller companies are working to incorporate AI in drones. Russia's electronic warfare has been increasingly effective against Ukraine drones, and the target strike rate of FPV drones has dropped to 30-50%. It is predicted that AI-operated FPV drones could post hit rates of around 80%.[11]

The use of AI for real-time intelligence analysis, pattern recognition, and predictive analytics has given Ukrainian forces a significant edge. These tools have improved targeting accuracy, reduced response times, and enhanced the overall efficiency of military operations.

(iii) Cybersecurity

The Ukraine war has been as much a cyber conflict as a physical one. At the start of the war, Russia knocked out Viasat satellite networks, cutting off internet access to thousands of Ukraine citizens. In the first half of 2022, 1,350 cyberattacks were registered, and 22% of Ukraine's fibre network was damaged

---

[9] Kyiv, Vera Bergengruen /. "How Tech Giants Turned Ukraine Into an AI War Lab." TIME, February 8, 2024. https://time.com/6691662/ai-ukraine-war-palantir/.

[10] Bergengruen/Kyiv, By Vera. "Ukraine's 'Secret Weapon' Is a Controversial Tech Company." TIME, November 14, 2023. https://time.com/6334176/ukraine-clearview-ai-russia/.

[11] Hunder, Max. "Ukraine Rushes to Create AI-Enabled War Drones." Reuters, July 18, 2024, sec. Artificial Intelligence. https://www.reuters.com/technology/artificial-intelligence/ukraine-rushes-create-ai-enabled-war-drones-2024-07-18/.

or destroyed.[12] However, Russia's cyber operations had only a limited impact, mainly due to support provided by private companies.

As terrestrial communication infrastructure was compromised or destroyed, American company SpaceX delivered over 30,000 Starlink terminals to Ukraine in the first 15 months of the war. These became the backbone of the communication infrastructure, providing secure communications to the military, the government, and the public.[13]

Companies like Cloudflare and CrowdStrike provide a full suite of cyber protection. Google expanded access to its free Project Shield software so that Ukrainian government websites could stay online. Mandiant, a part of Google Cloud, provides direct assistance to Ukrainian government entities under the Cyber Defense Assistance Collaborative.[14]

Since the beginning of the war, Microsoft has provided $540 million in aid to state bodies, state-owned companies, and businesses. Some of this help is provided in the form of products and services, such as cloud storage and cyber security products.[15]

In order to protect Ukraine's critical data, it was moved into the cloud and stored outside the country. Amazon supplied Ukraine with Snowball Edge units – suitcase-sized solid-state hard drives – to help store and transfer data. More than 10 million gigabytes of Ukrainian government and economic data was thus saved.[16]

(iv) Information Warfare

The war has seen a sharp battle of narratives, with Russia and Ukraine both trying to shape public perceptions in their favour. Social media has played a vital role in this contest, with commercial companies taking clear sides.

---

[12] admin, Techinformed. "One Year on: 10 Technologies Used in the War in Ukraine." TechInformed, February 24, 2023. https://techinformed.com/one-year-on-10-technologies-used-in-the-war-in-ukraine/.

[13] Söderström, Ulrike Franke, Jenny. "Star Tech Enterprise: Emerging Technologies in Russia's War on Ukraine." ECFR, September 5, 2023. https://ecfr.eu/publication/star-tech-enterprise-emerging-technologies-in-russias-war-on-ukraine/.

[14] Google. "New Ways We're Supporting Ukraine," December 1, 2022. https://blog.google/outreach-initiatives/public-policy/new-ways-were-supporting-ukraine/.

[15] Center, CEE Multi-Country News. "The Focus Has Shifted to Cyber Security." CEE Multi-Country News Center, April 29, 2024. https://news.microsoft.com/en-cee/2024/04/29/the-focus-has-shifted-to-cyber-security/.

[16] Tangalakis-Lippert, Katherine. "Amazon Helped Rescue the Ukrainian Government and Economy Using Suitcase-Sized Hard Drives Brought in over the Polish Border: 'You Can't Take out the Cloud with a Cruise Missile.'" Business Insider. Accessed August 16, 2024. https://www.businessinsider.com/amazon-saved-the-ukrainian-government-with-suitcase-sized-hard-drives-2022-12.

Facebook has routinely taken down fake accounts linked to Russian disinformation campaigns. In March 2022, Meta Platforms temporarily relaxed its hate policy to allow Facebook and Instagram users in some countries to call for violence against Russians and Russian soldiers in the context of the Ukraine invasion.[17]

After Russia began to block access to major social media platforms like Twitter and Facebook to control the narrative around the Ukraine war, Twitter introduced a special version of its platform, which was accessible via the Tor network. The Tor service was designed to help users in Russia with restricted internet access to use Twitter securely.[18]

In March 2022, YouTube banned all Russian state-funded media from its platform globally, citing a policy barring content that "denies, minimizes or trivializes well-documented violent events."[19] Google removed Russian state-funded publishers such as RT from its news-related features, including the Google News search tool.[20]

It could be an oversimplification to state that Ukraine is winning the information war. Still, the role of private technology companies has certainly helped it in pushing its narrative and propaganda, while restricting Russia's.

(v) Growth of Defence Startups

Since the war began, the Ukrainian defence startup sector has witnessed significant growth and transformation. There are more than 300 defence startups, most of which were founded in 2022-23.[21] The Ukrainian deputy minister of digital transformation on IT industry development, Oleksandr Bornyakov, has stated, "As an outcome of this war, we could build up to 100

---

[17] Vengattil, Munsif, Elizabeth Culliford, Munsif Vengattil, and Elizabeth Culliford. "Facebook Allows War Posts Urging Violence against Russian Invaders." Reuters, March 11, 2022, sec. Europe. https://www.reuters.com/world/europe/exclusive-facebook-instagram-temporarily-allow-calls-violence-against-russians-2022-03-10/.

[18] News, V. O. A. "Twitter Offers Darkweb Site to Restore Access for Russian Users." Voice of America, March 10, 2022. https://www.voanews.com/a/twitter-offers-darkweb-site-to-restore-access-for-russian-users-/6479360.html.

[19] Paul, Kari. "RT Videos Spreading Ukraine Disinformation on YouTube despite Ban – Report." The Guardian, February 23, 2023, sec. Media. https://www.theguardian.com/media/2023/feb/22/rt-ban-youtube-videos-google-disinformation.

[20] "Google Drops RT, Other Russian State Media from Its News Features | Reuters." Accessed August 16, 2024. https://www.reuters.com/technology/exclusive-google-drops-rt-other-russian-state-media-its-news-features-2022-03-01/.

[21] Genome, Startup. "Startup Genome." Startup Genome. Accessed August 18, 2024. https://startupgenome.com/article/adaptation-and-resilience-first-hand-insights-into-the-ukrainian-startup-ecosystem.

Ukrainian companies valued at $100 million and maybe 10 or 20 companies could become unicorns in defence tech."[22]

In April 2023, the Ukrainian government launched the BRAVE1 defence tech cluster to provide startups with resources, networking opportunities, and access to both military and commercial markets. For 2024, the BRAVE1 has been allotted a budget of $39 million.[23] Ukrainian D3 Venture Capital fund, which finances startups, has attracted foreign investors, including former Google CEO Eric Schmidt. The fund plans to grow to $30 million in 2024.[24]

With Ukraine becoming a testing ground for new military technologies, foreign investment is flowing in. German company Quantum-Systems has opened a new drone factory in Ukraine and established a dedicated R&D centre.[25] Turkish defence company Baykar is building a factory near Kyiv where it will manufacture either its TB2 or TB3 drone models.[26]

The rapid growth and innovation within Ukraine's defence startup sector have positioned the country as a potential leader in the global defence market. As these startups continue to grow and innovate, Ukraine is increasingly seen as a hub for cutting-edge defence technologies.

The experiences in Ukraine suggest that future conflicts will increasingly rely on integrating commercial technologies into military operations. As military forces worldwide observe the developments in Ukraine, the strategic importance of military-commercial partnerships must become a focus of defence planning. This case study illustrates that in modern warfare, technological superiority may be as much about leveraging commercial innovation as it is about traditional military strength.

---

[22] Hartmann, Théophane. "Ukrainian Deputy Minister Lays out Vision for Defence Tech." www.euractiv.com, May 27, 2024. https://www.euractiv.com/section/europe-s-east/news/ukrainian-deputy-minister-lays-out-vision-for-defence-tech/.

[23] "Ukraine's Defense Tech Cluster BRAVE1 to Invest $39M in Startups in 2024. How Is It Working - AIN." Accessed August 18, 2024. https://en.ain.ua/2023/11/28/brave1-to-invest-39m-in-startups-in-2024.

[24] "The D3 Investment Fund to Scale to More than $10M and Has Already Invested in Seven Military-Tech Startups from Ukraine InVenture." Accessed August 18, 2024. https://inventure.com.ua/en/news/ukraine/the-d3-investment-fund-to-scale-to-more-than-dollar10m-and-has-already-invested-in-seven-military-tech-startups-from-ukraine.

[25] Zoria, Yuri. "German Quantum-Systems Opens Its Drone Factory in Ukraine." Euromaidan Press, April 19, 2024. https://euromaidanpress.com/2024/04/20/german-quantum-systems-opens-its-drone-factory-in-ukraine/.

[26] Magid, Pesha. "Turkey's Drone Maker Baykar Begins to Build Plant in Ukraine." Reuters, February 7, 2024, sec. Aerospace & Defense. https://www.reuters.com/business/aerospace-defense/turkeys-drone-maker-baykar-begins-build-plant-ukraine-2024-02-06/.

Leveraging Commercial Technologies in India

(i) Current Initiatives and Challenges

In recent years, the Indian government has firmly pushed for greater indigenisation under the policy of AtmaNirbhar Bharat (Self-Reliant India). In the 2024 defence budget, 75% of the capital acquisition budget has been earmarked for procurement from local companies.[27]

Private companies are increasingly taking an interest in the defence sector, and several big players like Tata, Larsen & Tubro, Mahindra & Mahindra, and Bharat Forge are already in the market. These companies will be important in building an indigenous defence industry in India. However, this brief focuses on the smaller, non-traditional, suppliers and startups.

Encouraging smaller suppliers in the defence industry offers significant advantages by injecting innovation, agility, and cost-effectiveness into the sector. Startups can innovate and deploy cutting-edge technologies like AI, cybersecurity tools, and drones far more rapidly than larger contractors, often operating with lower costs and offering fresh, disruptive perspectives. Startups also excel at developing dual-use technologies, allowing faster integration and scalability.

In the Ukraine war, tech giants like Meta, Microsoft, and Google came out in support of Ukraine as they had to align with the US stance and policies. Until India can create something close to these tech giants' capacities, the startup ecosystem's innovation ability must be exploited to develop tools for cyber defence, AI, and information warfare.

Several initiatives have been taken to provide incentives for innovation and indigenous development. Scheme for iDEX-Innovations for Defence Excellence was launched in May 2021 by the Defence Innovation Organization under the aegis of the Department of Defence Production. iDEX provides grants of up to Rs 1.50 Cr (up to Rs 10 Cr in the case of iDEX Prime) to startups and MSMEs to fund projects in defence technology.[28] Rs 518 crore ($61.7 million) were allotted in the current fiscal year for iDEX. In March 2024, the Acing Development of Innovative Technologies with the iDEX (ADITI) scheme

---

[27] The Economic Times. "India Sets Annual Defence Production Target of Rs 3 Lakh Cr and Defence Exports Worth Rs 50,000 Cr by 2028-29." February 25, 2024. https://economictimes.indiatimes.com/news/defence/three-services-used-to-work-in-silos-earlier-now-they-have-better-coordination-to-jointly-confront-challenges-rajnath-singh/articleshow/107971490.cms?from=mdr.

[28] myScheme - One-stop search and discovery platform of the Government schemes. "Innovations for Defence Excellence." Accessed August 22, 2024. https://myscheme.gov.in.

was launched. Under the scheme, startups can receive a grant-in-aid of up to Rs 25 crore for their research, development, and innovation endeavours in defence technology.[29]

The Defence Research and Development Organisation (DRDO) has initiated several partnership programs with startups and MSMEs under its Technology Development Fund (TDF). The scheme provides a funding of up to Rs 10 Crores.[30] The three service headquarters, too, have funds allotted for engaging with startups and MSMEs for advanced technology products.

There have been some successes, but much more needs to be done. In the six years since its raising, the iDEX scheme has led to the procurement of 35 items worth Rs 2,000 crore ($240 million). In February 2024, the Chief of Army Staff announced that under the iDEX route, 55 Indian Army projects, worth Rs 400 crore ($48 million), were being pursued.[31] Considering the size of the Indian defence budget, these are modest amounts.

There have often been observations that the financial incentive being provided to startups needs to be increased, particularly for hardware prototype development.[32] Additional funding would help, but in order to provide real impetus to exploiting technology from the commercial sector, we will have to relook the complete ecosystem linked to procurements. The military's procurement process is bureaucratic, rigid, and slow. This is true for most militaries, but in India's case, this problem seems particularly acute, as is evident from the long time taken to develop and deploy new platforms.

A bureaucratic procurement process that lacks flexibility prevents the establishment of partnerships with small companies and non-traditional suppliers. The military, therefore, falls back on the government-owned Public Sector Undertakings (PSUs), for which procurement practices are more relaxed. The PSUs account for almost 80% of defence production in India. This share

[29] "DefConnect 2024: Raksha Mantri Launches ADITI Scheme to Promote Innovations in Critical & Strategic Defence Technologies." Accessed September 7, 2024. https://pib.gov.in/pib.gov.in/Pressreleaseshare.aspx?PRID=2011171.

[30] "About Us | Defence Research and Development Organisation - DRDO, Ministry of Defence, Government of India." Accessed August 22, 2024. https://www.drdo.gov.in/drdo/headquarter-directorates/about-us/directorate-technology-development-fund-dtdf.

[31] Singh, Dalip. "Army Pursuing ₹400 Crore Worth 55 Projects through iDEX Route: General Pande." BusinessLine, February 26, 2024. https://www.thehindubusinessline.com/news/national/army-pursuing-400-crore-worth-55-projects-through-iDEX-route-general-pande/article67888429.ece.

[32] "India's Path to Defence Self-Reliance: Challenges and Progress in the iDEX Initiative | Manohar Parrikar Institute for Defence Studies and Analyses." Accessed September 7, 2024. https://www.idsa.in/issuebrief/Indias-Path-to-Defence-Self-Reliance-SNAhmed-190724#footnote35_4okr08g.

has remained unchanged in the last eight years, despite incentives to the private industry.[33]

The iDEX programme is funded and managed by a 'Defence Innovation Organization', which has been formed as a 'not for profit' company. The founder members of iDEX are two Defence PSUs - HAL & BEL. There are some concerns that the presence of HAL and BEL at iDEX could be viewed as a conflict of interest when they are competing with private companies for the same product. At the same time, BEL and HAL are India's equivalents of large US companies. There are many areas where small and medium companies cannot venture because of the sheer size and resources required. It is, therefore, important for both public and private entities to co-exist, by putting in place a competitive system that prevents monopolies, and ensures that big companies don't shut smaller players out.

The slow pace of acquisition is not in line with the accelerating rate of technology change. For capital procurements, the time taken from Acceptance of Necessity (AoN), Request for Information (RFI), Request for Proposal (RFP), trials, commercial negotiations, formal order and delivery of the first system, is often anywhere between 3-8 years. The same system is then supplied over another 3-5 years.

Apart from the fact that the identified technology may have become obsolescent by the time it is inducted, these timelines present challenges for startups who may not have the resources to wait for years to get approval. While much of funding is allotted in the early stages of development, the extended period of procurement, and the lack of certainty in securing the contract, results in some of the technology languishing in the "valley of death" - that is, the technology has been demonstrated but does not find its way to timely adoption by the military.[34]

(ii) Accelerating Innovation

Currently, there are multiple agencies and programs working with the industry for technology adoption in the military. Apart from iDEX and DTF, each service has the equivalent of a design bureau to meet their individual requirements. The field commanders of the three services have also been granted funds for

---

[33] "Dashboard For Defence Minister." Accessed September 4, 2024. https://ddpdashboard.gov.in/DefenceProduction/Defence_Production.

[34] "What Does Valley of Death Refer to? | Secureframe | Secureframe." Accessed September 11, 2024. https://secureframe.com/glossary/valley-of-death.

R&D and special financial powers for the procurement of operationally urgent requirements.

All these agencies serve a useful purpose, but it would help if there were greater coordination and information sharing between their work to avoid duplication in effort. In the absence of a centralised coordinator, interagency task forces could be set up to synchronise efforts on cross-cutting technologies. A combined website of all the different programmes like iDEX, TDF, and service-specific proposals could be created to enable all agencies to view what the others are pursuing. Such a website would also be immensely useful for companies to gain an understanding of the military's requirements in a comprehensive manner.

There is a need to further strengthen the iDEX organisational structure by bringing in full-time serving military personnel, technology experts, and commercial executives. The involvement of HAL and BEL should be gradually moderated due to issues, as highlighted earlier, of a possible conflict of interest.

The iDEX should become the nodal agency for engaging with non-traditional defence companies and focus on dual-use technologies that are commercially available. The US has the world's most advanced defence industrial base, the best military R&D agency in DARPA, and innovation cells at the service level. However, it still felt the need in 2015 to create the Defense Innovation Unit (DIU) to accelerate the adoption of leading commercial technology throughout the military.[35]

The iDEX regularly comes out with Defence India Startup Challenges to support startups and MSMEs in developing prototypes and solutions in the area of defence and security. It must also become more proactive in scouting for commercial technology which has potential military applications. Many startups thrive on a risk-taking model, and the iDEX must mirror this practice to some extent to tap into greater innovation.

The Ministry of Defence would have to relook at its procurement process for the adoption of technologies like AI, cyber, software, information technology, etc., that are rapidly and constantly changing. A model like the US 'Other Transaction Authority' (OTA) could be adopted. OTAs are legally binding agreements utilising statutory authorities that permit federal agencies to enter into transactions other than procurement contracts, grants, or cooperative

---

[35] "About DIU." Accessed September 9, 2024. https://www.diu.mil/about.

agreements. As such, they are not subject to the federal laws and regulations governing procurement contracts.[36]

The successful application of OTA provides for the quick development and acquisition of solutions for force readiness, i.e., R&D, prototype development, and transition through initial production. As an example, the OTA was used for the development of the Mine-Resistant Ambush Protected (MRAP) vehicle to reduce IED casualties to US troops in Iraq and Afghanistan. The development and fielding of the MRAP - from R&D into production - only took 90 days, versus the typical 18-24 months through the traditional procurement route.[37]

The Indian government must set up a defence-oriented venture capital fund. This fund would have to be run by professional managers and not bureaucrats. While the Ministry of Defence provides the money and retains oversight, the fund must retain a high level of autonomy in decision-making to ensure its agility. The CIA-funded In-Q-Tel, which has been extremely successful in supporting critical technologies for the US intelligence community, is a model that could be studied in this regard.[38]

Creating a collaborative ecosystem that encourages open communication and cooperation between the military and the commercial sector is also vital. Regular forums, workshops, and conferences should be organised to facilitate dialogue between military leaders and tech startups. We must build a partnership that conveys a shared vision and equal investment from both sides.

Within the military, there is often a concern about sharing sensitive information. Instead of this becoming a hurdle, it would be better to lay down clear protocols on robust data security that must be complied with. There must also be clear IP-sharing agreements that outline ownership rights, usage rights, and revenue-sharing arrangements for technologies developed through joint projects. These agreements should balance the interests of both the military and commercial companies.

Conclusion

The nature of modern warfare has evolved to place commercial innovation as an essential element of military capability. The war in Ukraine has provided a

---

[36] "Other Transaction Authority."
https://acquisitioninnovation.darpa.mil/docs/Articles/Contract%20Management%20Dobria nsky%20OTA.pdf
[37] Ibid
[38] "IQT." Accessed September 9, 2024. https://www.iqt.org/.

clear example of how commercial technologies, from drones to AI and cybersecurity, have played a pivotal role in shaping battlefield outcomes. This shift is not an anomaly, but a signal of the future direction of military planning.

What Ukraine has shown is that an agile, private sector-led system outperforms a state-led system in the induction and utilisation of innovative ideas and processes. India's system is predominantly state-led and will be handicapped, just as the Russian system is, when it comes up against a private sector-led system.

To remain competitive, the Indian military must strengthen programmes like iDEX and enhance coordination among different agencies. Streamlining procurement practices could bring agility and significantly reduce timelines for adopting emerging technologies. Establishing a defence-focused venture capital fund and creating a collaborative ecosystem with open communication between the military and commercial tech sectors will further enhance innovation.

These steps will enable the Indian military to tap more effectively into the rapid advancements being made in AI, cybersecurity, drones, information warfare, and other critical areas, ensuring it maintains a technological edge in the ever-evolving landscape of modern warfare.

***

DPG

Delhi Policy Group
Core 5A, 1st Floor,
India Habitat Centre, Lodhi Road
New Delhi - 110003
India

www.delhipolicygroup.org