Digi truce
SECURING DIGITAL GROWTH

MISSION स्वक्षम

Report: National Launch of Mission Swaksham 2026

powered by

MeitY
Government of India

DSCI
PROMOTING DATA PROTECTION

SIDM
SOCIETY OF INDIAN DEFENCE MANUFACTURERS

National Centre of Excellence
CYBERSECURITY TECHNOLOGY AND ENTREPRENEURSHIP

Research & Development Partner

IIM NAGPUR


MISSION स्वक्षम
From Self-Reliance to Capability
Strategic Manthan
FIRST RAISING DAY
आत्मनिर्भर
SWAVALAMBAN
OT SECURITY
SECURE AUTOMATION
SOVEREIGN AI

Executive Summary

This report presents the proceedings, deliberations, and strategic outcomes of the National Launch of Mission Swaksham held on 01 July 2026 at the Manekshaw Centre, Delhi Cantonment convened by Digitruce Private Limited as its inaugural Cyber Raising Day. Mission Swaksham is a whole-of-nation, multi-year initiative to secure the cyber and industrial sovereignty of Bharat through indigenous capability, structured collaboration, and coordinated action across the five national estates: Policy, Armed Forces, Industry, Academia & R&D, and Veterans. The report is submitted for the consideration of the Ministry of Electronics & Information Technology, the Ministry of Defence, and affiliated national institutions not as a record of dialogue, but as a charter for immediate institutional action in translating India's decade of self-reliance (Swavalamban) into demonstrated cyber-industrial capability (Saksham).

Key Findings

The deliberations across the five-estate panel converged on the following findings:

- The cyber threat curve is outpacing the indigenisation curve. While India's kinetic self-reliance reached historic highs of ₹1.78 lakh crore in indigenous defence production and ₹38,424 crore in exports, CERT-In recorded 29.44 lakh cyber incidents in 2025 and an attack rate of 702 attacks per minute, with seven APT groups active during Operation Sindoor and three persisting undetected for over thirty days.
- **India's core deficit is one of institutional trust, not technical capacity.** Ideas, funding instruments, and technical talent already exist across the ecosystem; what is missing is coordination, follow-through, and institutional willingness to place firm orders with certified indigenous developers.
- **Human capital is the binding constraint** across hardware, software, and AI layers of the cyber stack. Present certification models are attendance-based rather than outcome-driven, and AICTE-governed curricula lag at the pace of technological change.
- **Full-stack, "chip-to-code" indigenisation remains incomplete.** India's critical systems from airbases and refineries to defence production lines continue to run substantially on foreign hardware, firmware, software, and test tooling; hybrid and white-labelled solutions frequently qualify as "indigenous" on the strength of well-documented foreign test reports.
- **Structured civil-military integration is missing.** The disciplined, mid-career talent exiting the Armed Forces (25–40 age bracket) is captured through informal, serendipitous channels rather than formal mechanisms, denying industry and academia a proven strategic asset.

- **Deployable indigenous capability is demonstrable, not aspirational.** The launch of **DTroop** as India's first indigenous AI-powered Operational Technology Security Operations Centre which is developed and deployed within a single year of Digitruce's founding, proves that the cyber-sovereignty gap can be closed through disciplined execution rather than further deliberation.

The findings carry three strategic implications of national consequences. First, the character of national security has fundamentally shifted to hybrid warfare that has erased the distinction between military and civilian targets, and disruption of highways, power grids, or refineries now carries battlefield-equivalent consequences. Second, a nation that has invested ₹7.85 lakh crore in its defence budget cannot afford to defend the airframe in the sky while leaving the runway controls undefended in their basement; every kinetic platform in India's inventory now rests on a digital substrate that must be sovereign to be secure. Third, the strategic advantage in the coming decade will accrue to the nation that has built with its own hands and on its own soil — the cyber and industrial systems on which its strategic posture depends; and India, at the inflection point of a generational transition, is uniquely positioned to be that nation, provided institutional trust, procurement commitment, and coordinated execution now follow the technological momentum already established.

Introduction – Mission Swaksham

Mission Swaksham was conceived at the intersection of two defining curves in India's strategic trajectory — one of remarkable ascent, the other of accelerating threat. Between 2014 and 2026, India's defence ecosystem underwent a historic transformation: indigenous defence production reached a record ₹1.78 lakh crore in FY 2025–26, defence exports touched ₹38,424 crore across over eighty countries, and the defence R&D budget grew by 112 percent, with 25 percent opened to industry, startups, and academia. Operation Sindoor (May 2025) validated this decade of effort, with indigenous platforms performing under theatre-grade combat conditions.

Yet in its immediate aftermath, sensors across India's critical infrastructure recorded 131 DDoS attacks every hour, and seven Advanced Persistent Threat groups were detected operating concurrently within Indian networks and many pre-positioned weeks in advance. In 2025 alone, CERT-In handled 29.44 lakh cyber incidents and tracked over 265 million malware detections, at an average rate of 702 attacks per minute, nearly sixty percent originating from the China–Pakistan axis. The aircraft is increasingly Indian; the radar is increasingly Indian but the code that protects the runway is, very often, not. In answer to this gap, Mission Swaksham was formally launched on 01 July 2026 at the Manekshaw Centre, Delhi Cantonment, coinciding with the First Raising Day of DigiTruce Private Limited, a K. S. Cheema Group enterprise founded by Armed Forces veterans that anchors the Mission's engineering and multi-year delivery.

Mission Swaksham is guided by five enduring convictions: sovereignty is built, not bought as imported capability carries embedded licences, kill-switches, and foreign approvals that erode true independence; the Nation itself is the architecture and no single estate can deliver sovereign capability alone; veterans are the indispensable bridge between strategy and execution, deployed for the ground truth they alone possess; the Mission values certified and operational solutions over academic publications or conferences, and is designed as a long-term initiative that will endure beyond its first phase and founders. Anchored in these principles, the Mission binds the five estates of the Nation — Policy, Armed Forces, Industry, Academia & R&D, and Veterans into a single, coordinated, multi-year working arrangement to deliver indigenous, deployable, and theatre-grade cyber and industrial sovereignty for India's critical infrastructure and defence-industrial base.

Mission Swaksham is architected as the cyber and industrial sovereignty layer of the larger national vision. It extends Atmanirbhar Bharat from platforms into the cyber and industrial-control systems that underpin them; strengthens the security foundations of Digital India; aligns with Make in India by targeting export-ready capabilities by 2030; and forms the cyber-industrial substrate of Viksit Bharat 2047, measured by a single test whether the digital foundation of India's defence, economy, and democracy is one that India itself has built. The Mission is aligned with the IndiaAI Mission and the National RDI Scheme on sovereign AI, data, and post-quantum readiness, and operates in structural coherence with DAP 2020, DPM 2025, the Positive Indigenisation Lists, iDEX, ADITI, TDF, NCIIPC frameworks, CERT-In advisories, the draft CEA Cyber Security Regulations, NCRF 2024, IEC 62443, and the emerging DPDP Rules reinforcing the national policy architecture.

1. Inaugural Proceedings

The proceedings opened with the traditional lamp-lighting ceremony, performed jointly by the assembled dignitaries and guests of honour - Air Chief Marshal R.K.S. Bhadauria, Lt. Gen. Dushyant Singh, Prof. Bhimrai Meitri (IIM Nagpur), Air Vice Marshal (Dr.) Devesh Vatsa, VSM, Mr. Sandeep Saini, Prof. Somnath Mitra, Mr. Garry Singh, Group Captain Rajeev Chandel, and Digitruce Co-Founder & Managing Director Mr. K.S. Cheema. The lamp lighting was followed by a Ganesh Vandana, invoking blessings for an auspicious start to the inaugural Cyber Raising Day.

2.Welcome Address by Wing Commander Sonika Tanwar (Retd.), CEO & Founder, Digitruce

The proceedings opened with the traditional lamp-lighting ceremony, performed jointly by the assembled dignitaries and guests of honour - Air Chief Marshal R.K.S. Bhadauria, Lt. Gen. Dushyant Singh, Prof. Bhimrai Meitri (IIM Nagpur), Air Vice Marshal (Dr.) Devesh Vatsa, VSM, Mr. Sandeep Saini, Prof. Somnath Mitra, Mr. Garry Singh, Group Captain Rajeev Chandel, and Digitruce Co-Founder & Managing Director Mr. K.S. Cheema. The lamp lighting was followed by a Ganesh Vandana, invoking blessings for an auspicious start to the inaugural Cyber Raising Day.

Wing Commander Sonika Tanwar (Retd.) delivered the welcome address and defined Mission Swaksham as a movement from self-reliance to capability, encapsulated in her formulation "Swavlamban se Swaksham." She stated that this is not a slogan but a doctrine that everyone presents in the room already lives. Marking the occasion as the first edition of Mission Swaksham, she asserted a founding premise: no outside actor secures a nation, a nation secures itself. She reaffirmed that India has spent the past decade living the principle of Swavlamban, and declared that the nation now acts on that principle directly in silicon and in code.

She welcomed each distinguished guest to the stage with a short introduction, naming Air Chief Marshal R.K.S. Bhadauria, Lt. Gen. Dushyant Singh, Prof. Bhimrai Meitri (IIM Nagpur), Air Vice Marshal (Dr.) Devesh Vatsa, Mr. Sandeep Saini, Prof. Somnath Mitra, Mr. Garry Singh, and Group Captain Rajeev Chandel, and called it a proud honour for Cheema Enterprises' Digitruce to host them.

She traced the period between 2014 and 2026 as a transformational, historic phase for India's defence ecosystem, and cited Operation Sindoor as proof of homegrown capability and the strategic dividend of a decade of indigenous effort. She drew a sharp line, however, between the kinetic and cyber dimensions of this progress: the kinetic dimension has delivered visible results, but the cyber dimension remains an uncomfortable truth, with the threat curve rising faster than the nation's response. She committed the first edition of Mission Swaksham to close that gap.

She explained that military veterans founded Digitruce, people who understand the exchange of one uniform for another, and who recognise that the frontline has simply moved into control rooms, protection grids, and critical information infrastructure within the cyber domain. As the day's marquee announcement, she revealed that Digitruce would earmark India's first indigenous Operational Technology Security Operations Centre, named "Dtroop," and called it the highlight of the session.

She stressed that nothing that would follow was a proposal for tomorrow it is, in her words, a system that works and stands deployed today. She closed by reframing the mission's purpose: this is not a call for any single estate to defend the nation from outside its ranks, but a call for every estate policy, forces, academia, industry, and veterans to jointly lift Bharat's cyber industry into the future. She then formally sought the permission of Air Chief Marshal R.K.S. Bhadauria, as Chief Guest, to commence the session with the panel discussion on Strategic Manthan.

3. Session Overview: Moderator's Opening Remarks

Air Vice Marshal (Dr.) Devesh Vatsa, VSM — Moderator

AVM Vatsa opened the session by placing India's cyber threat environment in stark statistical relief. He cited 131 distributed denial-of-service (DDoS) attacks recorded during the Operation Sindoor observation window, alongside the concurrent presence of seven Advanced Persistent Threat (APT) groups inside Indian networks. He noted that many of these actors had prepositioned themselves weeks before the first kinetic strike, underscoring the premeditated and state-linked nature of the campaign.

He further cited 29.44 lakh cyber incidents recorded nationally in the same year, and an attack rate against Indian organisations of approximately 72% which is well above the global average. Framing this as a present reality rather than a future contingency, he observed that India's critical systems run substantially on foreign-built hardware, software, and ICT equipment.

Contrasting this with the defence sector's indigenous progress of ₹1.78 lakh crore in indigenous production, ₹38,424 crore in exports, and a 112% increase in R&D spend, as stated by the Raksha Mantri on 7 June 2026, he posed the session's organising question: Can the nation defend what it builds without extending the same indigenous resolve to the cyber domain?

He introduced the guiding principle of the dialogue: “Dependability is a vulnerability.” He closed his opening remarks by directing the panel toward the detection-to-response gap illustrated by the three APT groups that persisted inside Indian networks for over thirty days, asking what single policy decision remains untaken to close it.

4. Panel Deliberations — The Five National Estates

4.1 Voice of Policy — Lt Col Amrinder Singh, NITI Aayog

Lt Col Singh opened by contextualising the threat data positively: while numerous cyber and DDoS attacks occurred during the observation period, most failed to penetrate critical infrastructure, and four of the seven observed APT groups were detected and neutralised in time. He argued that this demonstrates that frameworks, technology, and guidelines already exist. However, the operative question is why the remaining three groups persisted for over thirty days.

His central diagnosis was that human capital, not technology, is the binding constraint across every layer of the cyber stack — hardware, software, and AI alike. He cautioned that there is no certainty that additional dormant APTs are not already resident in Indian networks today.

He argued that a single, one-size-fits-all training method cannot build overall cyber resilience, as different areas of cybersecurity require different ways of thinking.

On one hand, there is a compliance-focused mindset suited to following rules and policies. Whereas, on the opposite exists a mindset required for reverse engineering and threat hunting, which requires questioning and probing rules rather than following them. Explaining how APT groups operate, he noted that once attackers gain entry into a network, they immediately create multiple backup access points. They eventually settle in the parts of the network that were not properly mapped or monitored for compliance.

On training reform, he criticised certification models based simply on hours of attendance. Instead, he called for outcome-based training, where success is measured by real tasks completed similar to live red-team exercises. He also proposed identifying and nurturing specialised cyber talent from a young age, using a model like the Services Selection Board (SSB). He noted that India already has adequate innovation missions and startup-support schemes in place; the real challenge is aligning these existing resources. He also critiqued AICTE-governed engineering curricula for lacking updated cybersecurity content, arguing that syllabi in this domain cannot remain static given the pace of technological change.

On inter-agency coordination, Lt Col Singh proposed a joint cyber group positioned at the National Security Council Secretariat (NSCS)/National Cyber Security Coordinator (NCSC) level, drawing operational representatives from CERT-In, NCIIPC, RAW, IB, DoT, and other mandated bodies, with a mandate for daily intelligence and best-practice sharing. Drawing on the analogy of counter-terrorism operations, where threat actors leave “breadcrumbs” across agency boundaries that only interoperable intelligence-sharing can assemble into an actionable picture.

He concluded that India currently lacks a true apex cybersecurity body, the National Cyber Security Coordinator role carries limited institutional weight. He recommended the constitution of a full-fledged National Cyber Security Commission, on the model of the Election Commission or the University Grants Commission, to provide the whole-of-government authority currently missing in the cyber domain.

4.2 Voice of Forces — Group Captain Rajeev Chandel

Gp Capt Chandel observed that while indigenous kinetic platforms have proven themselves in actual combat conditions, the cyber and operational-technology (OT) substrates beneath those very platforms remain, in significant measure, non-indigenous, a vulnerability spanning airbases, refineries, defence production lines, and critical infrastructure installations.

Identifying the single most concerning capability shortfall for the next conflict, he declined to isolate one technology or sector,

arguing that hybrid warfare has removed the distinction between military and civilian targets:

disruption of highways, railways, or power systems now carries consequences comparable to a battlefield casualty. His prescription was full lifecycle, “chip-to-code” indigenisation across every technology layer of hardware, firmware, software, and test tooling rather than a narrow, sector-specific fix.

He substantiated the threat with concrete incidents: an attack on Tata's electronics operations (which handled sensitive Tesla and Apple-linked work), assessed as a deliberate signal that India cannot be trusted with critical IP,

with reports of roughly 22 design files compromised; and a 2025 ransomware attack on the Indian company JLR in the UK, alongside the Marks & Spencer breach in the same geography, which he read as evidence of a geopolitically patterned targeting campaign.

His closing intervention was a direct challenge to industry and institutional leadership: Indian startups can produce credible solutions but are frequently denied real opportunity because large institutions and established players do not trust homegrown technology. He framed this explicitly as a trust deficit rather than a capability deficit, and without domestic market access and scale, indigenous ventures cannot generate the revenue needed to sustain R&D and achieve global competitiveness.

4.3 Voice of Industry — Mr. Sandeep Saini

Mr. Saini acknowledged a structural limitation in the IT sector's historical growth model. He observed that four decades of sector growth were built primarily on service-delivery relationships with global clients, which generated scale and employment but did not result in Indian ownership of the underlying technology stack

He structured industry's commitment around four layers. First, silicon: while leading-edge nodes (2nm–4nm) remain, a distant prospect given ASML's monopoly on advanced fabrication equipment,

his organisation is investing to become one of India's largest silicon producers, progressing from 12nm toward 6nm, to reduce decades-long dependency on imported equipment. He was candid that full sovereignty remains elusive end-to-end, since data will continue to transit foreign infrastructure (citing Ericsson base stations and Cisco backbone equipment) even where it terminates in a sovereign model describing the present state as “hybrid sovereignty.”

He proposed the development of a "forward/field-deployed engineer" cadre. This cadre would consist of technically proficient, domain-aware professionals capable of rapidly building AI-enabled solutions. He specified industry to sourcing this cadre from personnel exiting the defence forces, citing the discipline and quality of training associated with short-service commission officers.

He identified the startup ecosystem's core weakness as "isolated point-solutioning" building narrow, single-purpose tools that don't connect to the broader data ecosystem. He illustrated this with an example from the Ministry of Rural Development: an AI tool used to verify construction progress under a housing scheme analysed photographs of houses but failed to flag an unrelated welfare concern a malnourished child visible in the same photograph. This gap occurred because the tool's underlying model was built to work in isolation, without access to or connection with other public datasets that could have flagged the additional need. Thus, he proposed a "connected services framework" that would sit above India's Digital Public Infrastructure (DPI) layer, enabling different AI tools and datasets to share information with one another. He drew an explicit parallel to UPI's success as a unifying, interoperable platform for payments, and emphasied the ecosystem to build an equivalent unifying platform for AI and defence-technology innovation.

4.4 Voice of Academia — Prof. Somnath Mitra

Prof. Mitra identified capital structuring and not talent or ideas as the binding constraint. He noted that despite a 112% increase in defence R&D expenditure and the formal opening of a share of R&D funding (cited at roughly ₹29,000 crore) to industry, startups, and academia, the journey from laboratory to operational platform remains slower than in comparable domains.

His central proposal was a dedicated, theme-based Alternative Investment Fund (AIF) for cybersecurity startups, modelled on the SEBI-regulated AIF structures already operating within legacy IIT ecosystems.

He distinguished this explicitly from the government's broader National Research Foundation (NRF), arguing that a general-purpose fund dilutes focus and outcomes across too many themes. Whereas a themed fund would deliver a concentrated, undiluted outcome. He cited UAE and OECD precedents for theme-based, sector-specific risk-capital vehicles built on precisely this philosophy.

He closed by noting strong grassroots demand: cybersecurity student clubs are active across IIT campuses (citing engagement of 400-plus in his own National Centre of Excellence), with interest extending well beyond computer-science students into non-technical streams, inspiring the commitment to a talent pipeline championing within his own institutional ecosystem.

4.5 Voice of Veterans — Lt. Gen Dushyant Singh

Lt. Gen Dushyant Singh challenged the prevailing perception that veterans have little further to contribute post-service, noting that a significant number continue to self-fund incubation centres and think tanks, citing his own early contribution toward establishing a think tank in Lucknow that has since gained institutional credibility.

His central recommendation was structured civil-military fusion: since many veterans are already employed within defence industries, they should be actively co-opted into day-to-day problem-definition rather than consulted only at the top of the process.

He further argued that veterans' operational familiarity with legacy systems is an underused asset in an era of rapid technological change, citing veteran involvement in upgrading the Zorawar tank as an example.

In extended remarks later in the session, he situated Operation Sindoor as a live demonstration of the depth of automation and networked capability already achieved by the forces, while cautioning that greater capability correlates with greater exposure. He observed that even sophisticated, well-resourced organisations (citing the JLR ransomware incident despite the availability of India's own software expertise) can be breached arguing that complexity, not culpability, explaining such failures. He credited the forces' relative success against cyber intrusion to network isolation, minimal external openings, and rigorously enforced process discipline for border indigenous capability development.

His most pointed institutional recommendation was on trust and procurement: he argued that indigenous technology will only mature into a viable industry once the state across every department, service, and public institution commits to placing firm orders with certified indigenous developers. Thus, ceasing the authorize “mixed” or white-labelled solutions dressed as indigenous products, which currently pass certification more easily on the strength of well-documented foreign test reports. He further urged the establishment of formal, structured engagement mechanisms as opposed to reliance on informal recruitment channels to capture the talent of officers' exiting service. He noted that this cohort, particularly those in the 25–40 age bracket, brings a disproportionately high level of discipline and training, and should be actively engaged both as engineers and as startup founders.

He closed by flagging the absence of adversarial (“black strategy”) thinking in Indian educational institutions, arguing that an excessive institutional focus on procedural correctness and ethics leaves India unprepared for adversaries who operate by no such constraint.

Moderator’s Closing Remarks

Air Vice Marshal (Dr.) Devesh Vatsa, VSM — Moderator

In his closing remarks, AVM Vatsa noted that defence personnel today serve with distinction across leading global aerospace and defence organisations, underscoring that officers cannot be narrowly understood as "security personnel.” Their training extends far beyond that description, as reflected in the Air Force and Navy's growing preference for engineering talent. He endorsed the industry's earlier submission that embedding defence personnel into projects from inception would yield superior, field-ready products. He cited the United States as a model where structured military-to-civilian transition programmes ensure veterans are actively sought after for their strategic and operational knowledge. He illustrated this with Airtel's early operations in India (circa 1998–2000), when the company inducted former signal officers into technical and advisory roles, one of whom continues to serve on its advisory board today.

He concluded that India consists of the talent required to replicate this model and that the country's veterans possess it in abundance. However, a formal, structured mechanism is missing to deploy that talent systematically, rather than through informal or ad hoc channels. He closed by observing that India's shortfall in this respect lies not in a lack of awareness, but in a persistent tendency to articulate the need for such integration without following through on institutional execution.

The esteemed panel was felicitated by Shri Amanjeet Bakshi, Chairman, Steel Consumer Forum, in recognition of their valuable contributions to the discourse on Strategic Manthan.

5. Official Unveiling of the White paper: Mission Swaksham

Mission Swaksham was formally unveiled by the esteemed panel members, together with distinguished guests Air Chief Marshal R.K.S. Bhadauria, Mr. K.S. Cheema, Shri Amanjeet Bakshi, and Wing Commander Sonika Tanwar (Retd.).

6. Formal Address by Air Chief Marshal R.K.S. Bhadauria (Retd.)

In his remarks, Air Chief Marshal Bhadauria cited Operation Sindoor as a demonstrated window into the depth of automation and networked capability already achieved by the armed forces, noting the rapidity with which coordinated operations were executed over a three-and-a-half-day window despite significant constraints. He cautioned, however, that as defence capability advances year-on-year,

the corresponding exposure to vulnerability rises in equal measure, a paradox that renders the scale of the cyber challenge difficult to overstate.

He illustrated this complexity by referencing the ransomware attack on JLR in the United Kingdom, noting that the attack succeeded despite the availability of India's own software expertise to the group involved. He attributed this not to any specific failure but to the inherent complexity of large, vertically siloed organisations, where one business vertical may operate entirely disconnected from the team responsible for cybersecurity. He drew the broader lesson that any industry, institution, or capability that is network-dependent and reliant on communication infrastructure remains inherently exposed to similar risk.

He attributed the armed forces' resilience against cyber intrusion to deliberate network isolation going well beyond simple air-gapping and reinforced by minimal external access, continuous monitoring shaped by past lessons, and strict discipline in procedures. He proposed this isolation-and-discipline model as the standard to be replicated across every technological and capability-development effort, including in fibre and AI domains. He also welcomed the emergence of over 400 supporting startups in this space as a positive indicator.

He identified the principal gap in India's indigenisation effort not as a shortfall in technology development, but as an institutional reluctance to trust indigenous solutions and commit firm orders to indigenous developers, whether startups or established industry. He argued that once an indigenous alternative is developed, corresponding imports must cease and noted the irony that foreign products often receive faster certification clearance owing to well-documented test reports, while indigenous alternatives are held to a higher threshold of scrutiny. He defined genuine indigenisation as complete, full-stack development, and called on every government department, armed force, and institution requiring cyber protection to commit to procuring indigenous solutions as soon as they become available. He further cautioned against the practice of marketing partially indigenous, white-labelled, or open-source-based solutions as fully "Made in India," and called for mutual confidence-building between industry and end-users particularly in defence, where network failure during live operations could immobilise an entire force with minimal warning.

He noted that quantum technology and General AI as critical areas requiring urgent industry and institutional preparedness. In particular, the need to build readiness for adopting General AI in defence systems while guarding against AI-enabled attack capabilities.

On the subject of veterans, he urged veterans to look beyond conventional employment and actively pursue entrepreneurial roles as founders or core members of startup and MSME technical teams. Also, noting that senior, experienced veterans continue to hold significant value as advisors and sources of strategic direction for industry.

He concluded by thanking the organisers and commending the panel for a substantive discussion, affirming that the nation is broadly on the right track. He closed with a direct call to action: India must move beyond deliberation, place genuine trust in its own people and industry, and commit **to procuring indigenous solutions in the national interest.**

7. Digitruce Journey – From Founding to DTroop

The genesis of Digitruce lies in a conviction carried over from uniformed service: that the systems entrusted with a nation's protection must never depend on external permission to function. It was this principle and the gap it exposed that gave birth to the organisation in July 2025, building upon research that had already been underway for three years prior.

Digitruce was established without a client base or revenue stream, founded on the conviction that the nation would require this capability. The founding team deliberately pursued the more demanding course of developing a sovereign engine from first principles, rather than licensing foreign technology and supplementing it with Indian labour. This choice remains the organisation's founding ethos.

By September 2025, Digitruce secured its first enterprise engagement with one of the world's most demanding engineering majors, establishing early proof that an indigenously built system could hold its own on the global stage. In October 2025,

the team took the more difficult route of writing its own code rather than importing foreign components, reinforcing its commitment to complete indigenous ownership of the technology stack. November 2025 saw the organisation re-engage with its founding institutional roots in the Air Force, secure new projects, and successfully deliver proof-of-concept demonstrations. December 2025 brought formal industry recognition and incubation under the Data Security Council of India (DSCI), providing critical mentoring and ecosystem support.

In January 2026, Digitruce opened its first office and marked its presence on the national stage on Republic Day, an occasion the organisation treated as a responsibility. February 2026 saw the team resolve a technical challenge that had remained unsolved for seven years, doing so within sixty days through sustained and focused effort. In March 2026, with the organisation only nine months old, Digitruce demonstrated its capability before an independent technical audit, proving its solution on merit rather than through presentation alone. April 2026 marked the formal closure Mission KAPA, a seven-year-old challenge, an outcome the team attributed not to exceptional cleverness but to a precise and disciplined understanding of the problem itself.

By May 2026, Digitruce had moved beyond problem-solving into knowledge creation, entering research and development partnership with IIT Gandhinagar, including the Indian Institute of Science (IISc), and undertaking joint work on an aircraft structural integrity platform with a leading defence research establishment. In June 2026, the organisation secured formal empanelment as a development partner with Defence Research and Development Organisation (DRDO) following an extended audit process, coinciding with its first anniversary a milestone reached on the strength of continuous, disciplined engineering effort behind the scenes.

8. National Launch of Dtroop

Marking the culmination of this first year, Digitruce announced the launch of Dtroop, its flagship product and a complete sovereign solution for securing critical information infrastructure, a capability already proven and deployed with two corporate clients. In presenting this milestone, the organisation reaffirmed its founding intent: to build people, products, and self-reliance not as a slogan, but as a settled and demonstrated fact for a sovereign nation.

9.Address by Dr. Bhimaraya Metri, Director of IIM Nagpur

Dr. Bhimaraya Metri extended his congratulations to the founders Wing Commander Sonika Tanwar (Retd.) and Mr. K.S. Cheema with the entire Digitruce team on this milestone event, describing it as a significant initiative in India's technology landscape.

He observed that the world has transitioned from the industrial era into the intelligence era, within which cybersecurity has emerged as a subject of critical importance.

He cited estimates placing the global cybercrime economy in the range of four to five trillion dollars, underscoring the scale and severity of the challenge. He noted that as businesses increasingly migrate to digital and machine-based platforms, cybersecurity has correspondingly become a board-level priority, with Chief Information Security Officers (CISOs) now assuming a role of comparable institutional importance to that of statutory bodies such as audit and finance committees within corporate governance structures.

He argued that this moment represents a particular opportunity for India, given its scale of population and the resulting volume of data generated, factors that position the country favourably for research and development, not only in cybersecurity but across technology domains more broadly. He noted that India, long recognised as the world's largest consumer of technology, now stands at a juncture where it must also become one of the world's foremost producers of technology. He referenced ongoing government initiatives, including the Anusandhan National Research Foundation (ANRF) and the Department of Science and Technology, as institutional mechanisms already in place to support this transition.

He was emphatic that India's technology and research efforts must no longer be oriented primarily toward serving Western markets but directed first at building indigenous capability for India and only then extending outward to the world. He framed this shift as essential not only to India's own technological leadership, but to its ability to contribute meaningfully to the global technology ecosystem.

He closed by once again thanking the organisers for the invitation, noting that in the year since Digitruce's founding in July 2025, the team has accomplished substantial work under the founder/CEO Wing Commander Sonika Tanwar's (Retd.) leadership. He expressed confidence that Digitruce is positioned to become a leading company both globally and within the defence sector, extending his best wishes for the organisation's continued success.

10. Address by Mr. K.S. Cheema, Co-Founder & Managing Director, Digitruce

In his address, Mr. Cheema reflected on the moment the founding team took what he described as a leap of faith, noting that from that point onward, there was no looking back. He observed that people took note of the conviction with which the organisation was started, the trust placed between its founding members, and the intensity with which the team worked driven not by immediate returns, but by a shared sense of purpose.

He was emphatic that Digitruce was never conceived as merely another startup, but as a team building toward a world-class Indian technology company capable of standing at par with the best in the world. One that would demonstrate India as a creator of technology and not merely a consumer. He framed this as a deliberate contribution to the vision of Atmanirbhar Bharat, and, most importantly, as a commitment to building genuinely indigenous cybersecurity capability from the ground up.

He stated that Digitruce was never merely a business venture for the founding team, but a mission rooted in the conviction that India's critical industries must not be left dependent on foreign technology for their defence.

He defined true self-reliance as the ability of a nation to design, develop, and continuously improve the technologies critical to its own ecosystems and argued foreign dependency in cybersecurity, as an unaffordable vulnerability. It was for this reason, he said, that the organisation chose the tougher path of indigenous innovation, a technology built in India, by Indians, for India, and ultimately for the world.

He attributed this achievement to every member of Digitruce who chose to believe in the vision before it became reality, and specifically credited the leadership of the organisation's CEO, Wing Commander Sonika Tanwar (Retd.), for transforming that belief into execution — leading from the front, remaining composed, relentless and committed. He was careful to note, however, that no organisation is built by any one individual; every milestone achieved in the first year reflects the combined effort of the entire team, and that collective spirit now forms the foundation on which Digitruce stands.

He closed with a reflective analogy, likening the process of building a startup as a venture that one nurtures, safeguards, and remains vigilant over, before ultimately presenting it to the world.

11. Recommendations

Institutional & Governance Reform

1. Constituting a National Cyber Security Commission with a whole-of-government authority.
2. Establishing a **standing joint cyber intelligence group** at the National Security Council Secretariat (NSCS) level, drawing operational representatives from CERT-In, NCIIPC, RAW, IB, and DoT, with a mandated daily intelligence and best-practice sharing protocol to close APT dwell-time gaps.

Indigenisation Standards & Procurement Policy

1. Define and enforce a formal “full-stack indigenous” certification standard covering hardware, firmware, and software to prevent white-labelled/hybrid solutions from qualifying as indigenous.
2. Mandate procurement preference for certified full-stack indigenous cyber and OT products across all government departments, defence services, and public-sector undertakings, after complete POC procedures with a defined timeline.

Human Capital & Education

1. Reform cyber-training certification toward outcome-based, task-driven models (live red-team style assessment) in place of attendance-based certification.
2. Pilot early talent identification and specialised-track nurturing for cyber sub-domains (Black strategist, threat hunting, reverse engineering, compliance/audit), modelled on the SSB approach.

Financing Instruments

1. Launch a dedicated, theme-based Cybersecurity Alternative Investment Fund, distinct from the broader National Research Foundation, modelled on existing SEBI-regulated AIF structures within the IIT ecosystem.
2. Mandate periodic, dynamic revision of AICTE-governed engineering curricula to reflect current cybersecurity and OT-security practice.

Veteran & Industry Integration

1. Establish a formal Veteran Integration Framework requiring defence-linked industries to embed veteran personnel in integration in day-to-day ground level roles.
2. Support industry-led **"forward/field-deployed engineer"** cadres sourced from exiting defence personnel, and formal channels (beyond informal or serendipitous recruitment) to capture mid-career (25–40 age) talent exiting service.

Ecosystem Architecture

1. Develop a connected-services framework abstracting India's Digital Public Infrastructure (DPI) layer to prevent isolated, non-interoperable point solutions among cybersecurity and AI startups.

Way Forward

The inaugural Cyber Raising Day and the national launch of Mission Swaksham have established both a diagnosis and a demonstrated capability. The five national estates — Policy, Forces, Industry, Academia, and Veterans arrived at a shared conclusion: India's cyber and operational-technology vulnerability is not a deficit of ideas, funding instruments, or technical capacity, but a deficit of institutional trust, coordination, and follow-through. The launch of Dtroop, India's first indigenous OT Security Operations Centre, developed and deployed within a single year of Digitruce's founding, stands as evidence that this gap can be closed through sustained, disciplined execution rather than further deliberation.

The way forward, therefore, rests on translating the day's commitments into time-bound institutional action across five fronts:

First, on governance, the constitution of a National Cyber Security Commission and a standing joint cyber intelligence group at the NSCS level should be taken up as an immediate legislative and administrative priority, closing the coordination gap that currently allows Advanced Persistent Threats to persist undetected for extended periods.

Second, on indigenisation policy, MeitY and the Ministry of Defence should jointly formalise a full-stack indigenous certification standard, and correspondingly commit government departments, defence services,

and public-sector undertakings to procurement preference for certified indigenous cyber and OT solutions, with a defined and published timeline for phasing out functionally equivalent imports.

Third, on human capital, pilot programmes for outcome-based cyber certification and early specialised-talent identification, together with dynamic revision of AICTE curricula, should be initiated within the current academic cycle to begin closing the talent pipeline gap identified across every estate.

Fourth, on financing, the proposed theme-based Cybersecurity Alternative Investment Fund should be taken forward in consultation with SEBI and the existing IIT AIF ecosystem, providing indigenous cybersecurity startups the patient, undiluted capital that general-purpose research funding does not offer.

Fifth, on institutional integration, the recommended Veteran Integration Framework and forward-deployed engineer cadres should be piloted with willing industry partners, formalising a channel for ex-service talent that has, until now, relied on informal and serendipitous recruitment.

This report accordingly recommends that MeitY, the Ministry of Defence, and affiliated national think tanks treat the recommendations set out in Section 11 not as a discussion agenda for future dialogue, but as a charter for immediate institutional action, with Mission Swaksham's subsequent editions serving as a periodic forum to review progress against each of these five fronts.

Team Profile

Veteran-led. Mission-focused. Innovation-driven. DigiTruce is an Indian startup with deep specialization in OT/ICS security, Aerospace software development, and critical infrastructure protection. Our leadership includes defense and national cyber policy veterans with decades of experience.

KS CHEEMA
Co-Founder & Chairman

MD & Chairman KS Cheema Group

AVM (Dr) D VATSA (Retd.)
Strategic Advisor

+37Yrs | IIT Mumbai | EX-IAF | DSCI | NASSCOM | National Security Leader | Policy Maker

WG CDR SONIKA (Retd.)
Founder & CEO

+17Yrs | EX-IAF | Ex-Amazon | Operational Technology Security

GP CAPT NAVNEET DUTTA (Retd.)
CTO

+28YRS | AI & Automation & Aviation

WG CDR (Dr) AK AGRAWAL (Retd.)
CISO

+29Yrs | CISSP | CEH | PHD (Cyber Security)

DR. R. SUNDER, PhD
(Aeroengineering)

+40Yrs | Aeronautical Structural Integrity & Fatigue Testing

PROF. PRAVEEN KUMAR, PhD
(Materials Science)

+20Yrs | Structural Integrity (Engineering Materials)

PROF. VIKRAM JAYARAM, PhD
(Materials Science)
IISC Banglore

+35Yrs | Fracture Mechanics | Defence, Areospace & Energy Sector

SHANTAN SAWA
Business Development Head

+8 yrs | Ex-ZS Tech Strategy Consulting

SQN LDR ISHA GUPTA (Retd.)
HEAD - Procurement & Training

15+ Yrs | Ex- IAF, Ex- UBS , Cybersecurity talent hunt & Training

Contact Us:

Email: digitruce@digitruce.com

Phone: 9910179231