



WHITE PAPER ON GUARDING THE FUTURE AI & CYBER SECURITY IN INDIA'S PRIVATE SECURITY REVOLUTION



AI & Cyber Security
Taskforce

GUARDING THE FUTURE: AI & CYBERSECURITY IN INDIA'S PRIVATE SECURITY REVOLUTION

CAPSI AI & CYBERSECURITY TASK FORCE Team &

SRINIVASMAHANKALI

Copyright © CAPSI All
Rights Reserved.

Contents

Foreword	5
Preface: Adjusting the Sails of the PSI Ship	6
Executive Summary	8
Vision for AI & Cybersecurity in the Indian Private Security Industry (PSI)	8
Chapter 1: Overview of Private Security Landscape & White paper Objectives	11
Chapter 2: Current State of Technology in Indian Private Security	16
Chapter 3: AI-Driven Challenges and Opportunities for PSI.....	20
Chapter 4: CAPSI's Strategic Pillars	22
Chapter 5: Emerging Technologies for Private Security Technology (PST) Adoption ...	26
Chapter 6: Creating Centers of Excellence (CoEs) in AI & Cybersecurity for PSI	30
Chapter 7: Case Studies, Initiatives, and Pilot Programs	33
Chapter 8: Strategic Recommendations to Enable the Ecosystem	36
Chapter 9: CAPSI's AI & Cybersecurity Task force driving Transformation	40
Chapter 10: Proposed Roadmap 2025–2027	43
Glossary of Tech Terms	47
Annexure 2: Stakeholders Consulted.....	48
Annexure 3: CAPSI Initiated Training Programs.....	48
CAPSI Governing Council & Advisors	50



Kunwar Vikram Singh
Chairman

Foreword

The Private Security Industry (PSI) in India has evolved into a cornerstone of the nation's safety and resilience framework. Once viewed merely as a supplementary force to government security apparatus, PSI today plays a pivotal role in guarding not just physical infrastructure but increasingly complex digital landscapes as well.

As of 2025, the Indian PSI has grown to an impressive market size of INR 1,00,000 crores, with over 48,000 licensed agencies under the PSARA Act, 2005.

This sector employs nearly 10 million people, making it one of India's largest employers, particularly for youth from rural and economically disadvantaged backgrounds. With minimum **wages as low as ₹15,500/month** for trained guards, the industry also provides a vital economic lifeline for millions.

Yet, the most dramatic shift confronting PSI today is not one of scale, but of nature. Traditional security paradigms are being rapidly disrupted by **AI-driven cyber threats**, such as ransomware, data breaches, deepfake attacks, and dark web activities. These threats do not just target corporations but entire digital ecosystems. As digital infrastructure underpins nearly all critical sectors—healthcare, finance, energy, defence—the **PSI must transform into a cyber-physical sentinel**.

To address this transformation, **CAPSI has established a dedicated AI & Cybersecurity Task Force** and is partnering with globally respected organizations such as **CyberPeace Foundation, IITM Pravartak**, and leading cybersecurity technology firms. Together, we are laying the groundwork for five national **Centers of Excellence (CoEs)** across India, designed to train PSI personnel, conduct domain-specific research, develop AI-aligned best practices, and foster collaboration between the private sector, academia, and policymakers.

The PSI is no longer just a service sector—it is becoming an integral part of national security architecture, industry 4.0 readiness, and digital sovereignty. This publication captures that ongoing transformation. It presents a strategic roadmap for industry stakeholders to adopt cutting-edge technologies, elevate workforce capabilities, and contribute meaningfully to India's security posture.

I congratulate all contributors and collaborators who have come together to shape this important work. It will serve not only as a knowledge compendium but also as a call to action for the PSI to boldly lead in the digital-first era.

Jai Hind !

Preface: Adjusting the Sails of the PSI Ship

A Call to Action for Private Security Industry Leaders

India's Private Security Industry (PSI), with an estimated market size of over ₹1,00,000 crores and a workforce of more than 10 million, stands at a critical juncture. Traditionally manpower-intensive and reactive in structure, the sector is now being reshaped by emerging technologies, evolving threat landscapes, and shifting client expectations. Senior PSI professionals must not only acknowledge this paradigm shift but also steer it through strategic foresight, structured transformation, and bold leadership.

As the PSI transits into a Digital-Physical ecosystem, industry leaders are now tasked with addressing both technological and human complexities—cybersecurity risks, AI-induced disruptions, integration of smart surveillance tools, and resistance to change within field operations. This is not merely a technical upgrade; it is a comprehensive reimagining of how security is conceptualized, delivered, and sustained.

1. Risk Management in a Digital-Physical PSI Ecosystem

To secure both physical and digital domains, PSI leaders must adopt a multi-layered risk management approach. The key risk vectors include:

- **Cybersecurity Threats:** Ransomware, phishing, insider threats, deepfakes, and AI-based manipulation of surveillance systems.
- **Technology Obsolescence:** Rapid evolution in AI and surveillance tools can quickly make current systems redundant.
- **Privacy & Compliance Risks:** Challenges in meeting data protection standards such as the DPDP Act and global equivalents.
- **Skill Gaps:** Limited availability of personnel trained in digital tools, cyber hygiene, and smart monitoring systems.

Mitigation Strategies:

- Conduct regular **Digital Threat Audits** and **Vulnerability Assessments**.
 - Deploy **Virtual CISO (vCISO)** tools and establish **Security Operations Centers (SOCs)** for real-time threat detection.
 - Partner with **Centers of Excellence (CoEs)** for ongoing threat intelligence and research.
 - Implement **AI-based Risk Scoring** to prioritize response efforts.
-

2. Change Management Imperatives for Senior PSI Professionals

Embracing digital transformation demands cultural agility and operational overhaul. Senior professionals must become enablers of this shift, addressing:

- **Mindset Shifts:** Inspiring mid-level supervisors and ground staff to trust and adopt digital tools.
 - **Workforce Reskilling:** Empowering guards and managers with training in digital literacy, AI-assisted surveillance, analytics, and escalation protocols.
 - **Leadership Alignment:** Ensuring strategic vision is shared across CXOs, ops heads, and field officers.
 - **Process Redesign:** Moving from paper-based SOPs to cloud-based, AI-augmented workflows.
- Change Management Actions:**
- Establish a **Change Champions Network** within PSI organizations to pilot and scale tech initiatives.
 - Launch **Blended Learning Programs** through CAPSI and CyberPeace Foundation for continuous upskilling.
 - Monitor progress through **Digital Adoption KPIs** and **Behavioral Change Metrics**.
 - Celebrate key transformation milestones to build morale and reinforce commitment.
-

Conclusion

Senior PSI professionals are no longer just operational managers—they are the stewards of a future-ready, AI-enabled security architecture. Their ability to manage risk, lead change, and foster a digitally capable workforce will determine whether India's PSI sails smoothly into the next decade or is left adrift in a sea of disruption.

This white paper calls for coordinated action from CAPSI, regulatory bodies, private sector leaders, and international partners to support this transition. It is time to adjust the sails—not wait for the wind to change.

Author:

*Editorial Board, CAPSI Future PSI Taskforce
In collaboration with Industry Thought Leaders*

Executive Summary

Vision for AI & Cybersecurity in the Indian Private Security Industry (PSI)

The Indian Private Security Industry (PSI), comprising over 10 million personnel and contributing significantly to national safety and employment, stands at the cusp of a transformative evolution. As India accelerates its digital journey with smart cities, Industry 4.0, 5G rollouts, and connected infrastructure, the need for technologically empowered security services has become imperative. In this context, the integration of Artificial Intelligence (AI) and Cybersecurity into the fabric of private security operations is no longer optional but a national necessity.

The vision for AI and cybersecurity in the Indian PSI is to build a future-ready, intelligent, and secure private security ecosystem that complements national security objectives, supports smart infrastructure, and provides resilient protection against physical and digital threats. This vision includes upgrading the PSI from a largely manpower-intensive sector to a tech-enabled, data-driven, and digitally coordinated force capable of addressing 21st-century security challenges.

AI technologies such as facial recognition, behavioural analytics, anomaly detection, predictive surveillance, and autonomous patrolling systems can amplify the capabilities of traditional guards. Simultaneously, cybersecurity ensures that the data and digital tools used in these operations are safeguarded from breaches, tampering, and cyberattacks.

India's PSI must evolve from static vigilance to dynamic intelligence-led security management, using AI to anticipate, detect, and prevent incidents rather than merely respond to them. This transformation will enable PSI personnel—from frontline guards to senior officers—to move up the value chain as digitally enabled security professionals.

The CAPSI AI Task Force, in collaboration with strategic partners such as CyberPeace Foundation, IIT Madras Pravartak, and various government and industry stakeholders, envisions a structured, inclusive, and fast-tracked adoption framework to transform the PSI with a national strategy for AI and cybersecurity training, standardization, innovation, and deployment.

Strategic Objectives and Key Recommendations

To achieve this vision, the whitepaper proposes the following strategic objectives and key recommendations that address policy, infrastructure, skill development, industry collaboration, and regulatory frameworks:

Strategic Objective 1: Modernize the PSI through AI and Emerging Technologies

Key Recommendations:

Technology Integration Mandate: Encourage adoption of AI-powered surveillance systems, drones, smart CCTVs, biometrics, and real-time data dashboards for incident management.

Pilot Tech Projects: Launch pilot programs across key industry verticals (e.g., airports, metro, logistics hubs) showcasing use of AI in physical security.

Digital Twin and Predictive Analysis: Enable digital simulation of high-security areas for predictive threat modelling using AI/ML.

Smart Uniforms & IoT Devices: Equip guards with wearables that track location, vitals, alertness, and provide live updates to control rooms. Establish a 'Centre of Excellence (CoE)' for AI in Security under CAPSI, with partner institutions to incubate and evaluate AI solutions for PSI.

Strategic Objective 2: Build a Skilled AI & Cybersecurity-Ready Workforce

Key Recommendations:

National Curriculum for AI & Cybersecurity in Security Services: In partnership with CyberPeace Foundation and IIT Madras Pravartak, design a multi-tiered skilling framework from basic to advanced levels.

CAPSI Learning Platform & Community App: Launch CAPSI's digital platform offering AI, cybersecurity, drone, and analytics training programs for all cadres of security professionals.

Career Mobility through Certification: Develop certification programs endorsed by government and industry for AI & cyber-trained guards to grow into control room operators, analysts, and cyber sentinels.

Train-the-Trainer Programs: Certify master trainers who can then cascade AI and cybersecurity training to field staff across India.

Strategic Objective 3: Promote National Security through Public-Private Collaboration

Key Recommendations:

MOU with Government Agencies: Sign strategic MOUs with Ministry of Home Affairs, Ministry of Electronics & IT, Rashtriya Raksha University (RRU), and others to align PSI tech adoption with national security priorities.

Cybersecurity Integration with National Grids: Integrate PSI cybersecurity capabilities with smart city grids, local police networks, and private command centers.

Emergency Response Network: Establish AI-enabled response systems in gated societies, industries, and campuses that instantly connect with authorities during incidents.

Inclusion in Government Tenders: Amend government tendering norms to give preference to tech-enabled private security agencies and AI-certified personnel.

Strategic Objective 4: Establish Regulatory Frameworks and Standards

Key Recommendations:

AI in PSI Guidelines: Create a policy framework for the ethical and secure use of AI in private security, addressing data privacy, surveillance limits, and human rights concerns.

Cybersecurity Protocols for PSI: Mandate cybersecurity SOPs for agencies handling critical infrastructure and sensitive data.

Standardization of Technology Procurement: Define protocols for the procurement, deployment, and audit of AI and cybersecurity solutions used by private security agencies.

Strategic Objective 5: Enable Data-Driven Insights for Better Decision Making

Key Recommendations:

CAPSI Security Data Intelligence Platform: Launch a centralized dashboard aggregating anonymized data from AI-powered surveillance devices across PSI agencies.

Incident Heatmaps and Predictive Crime Mapping: Use AI analytics to provide real-time incident alerts and future risk mapping to both private and public stakeholders.

Annual Security Intelligence Reports: Publish a data-driven report on PSI trends, vulnerabilities, and AI-based risk mitigation outcomes to inform policy and strategy.

Strategic Objective 6: Foster Innovation and Indian Start-Up Ecosystem

Key Recommendations:

AI for PSI Grand Challenges: Host annual hackathons and innovation challenges with support from MeitY, DST, and Startup India to develop Indian AI-based security solutions.

Startup Sandbox in Collaboration with IITs and Incubators: Provide regulatory and real-world testing access to Indian startups working in AI for surveillance, access control, and emergency response.

CAPSI Tech Partners Program: Create a formal platform for vetted tech vendors and solution providers to collaborate with PSI stakeholders under CAPSI.

Strategic Objective 7: Strengthen CAPSI as the National Digital Security Integrator

Key Recommendations:

CAPSI National Platform & App Ecosystem: Launch a unified national portal and app that integrates training, job matching, certification, grievance redressal, and technology updates.

Digital Badge Program: Issue digital ID cards with verified credentials and training badges for all CAPSI-registered guards and officers.

Cybersecurity Incident Reporting Tool: Enable PSI agencies to report cyber incidents and suspicious activities via the CAPSI platform to a national threat intelligence hub.

Strategic Objective 8: Influence Policy, Awareness and Global Alliances

Key Recommendations:

National Whitepaper and Policy Submission: Submit the CAPSI AI & Cybersecurity whitepaper to relevant ministries and parliamentary committees for inclusion in national digital security frameworks.

Awareness Programs and Public Engagement: Conduct nationwide campaigns on the role of AI-trained guards and cyber vigilance in schools, offices, and communities.

Global Alliances and Best Practice Exchange: Build collaborations with AI-driven PSI models in Singapore, the US, Israel, and UAE to adapt successful technologies and training approaches.

Final Note:

The successful implementation of these strategic objectives will position India as a global leader in intelligent private security, with PSI professionals not only providing physical protection but also becoming the first line of defense in cyber-physical ecosystems. The CAPSI AI Task Force, with its esteemed partners, shall lead this mission as a bridge between traditional security expertise and next-gen technological empowerment.

This whitepaper serves as both a blueprint for the future of Indian security services and a call to action for government, industry, academia, and civil society to collaborate in this national endeavour. As AI and cybersecurity become foundational to safety and sovereignty, India's PSI must evolve from being a follower to a global trendsetter in security innovation.

Chapter 1: Overview of Private Security Landscape & White paper Objectives

Introduction:

Based on the industry insights, here are the key opportunities and imperatives for India's Private Security Industry (PSI) concerning electronic surveillance, employment, and training:

1. Electronic Surveillance: A Strategic Growth Driver

- **Shift Towards Technology:** The PSI is transitioning from traditional manned guarding to integrated security solutions, including electronic surveillance, access control, and biometric systems.
- **Integration with National Initiatives:** Programs like 'Smart Cities' and 'Make in India' are catalyzing the adoption of advanced surveillance technologies, creating new avenues for PSI companies to offer tech-enabled services.

2. Employment Opportunities: Expanding Workforce Needs

- **Significant Employment Generator:** The PSI employs over 10 million individuals & supports their families, with projections indicating the potential to add significant numbers every year. This positions the industry as a major employment provider, especially for rural youth.
- **Diversification of Roles:** The evolution towards technology-driven services necessitates new roles such as electronic surveillance operators and cyber risk analysts, expanding career paths within the industry.

3. Training and Skill Upgradation: Imperative for Industry Advancement

- **Need for Structured Training:** With the increasing complexity of security challenges, there is a pressing need for structured training programs focusing on technology integration, soft skills, and compliance.
- **Recognition of Prior Learning (RPL):** Implementing RPL initiatives can help in upskilling existing personnel, ensuring they meet the evolving demands of the industry.
- **Standardization and Certification:** Establishing standardized certification processes will enhance the credibility and professionalism of security personnel, aligning with global best practices.

The Indian Private Security Industry stands at a pivotal juncture, with significant opportunities arising from technological advancements and increasing security demands. To capitalize on these, the industry must focus on integrating electronic surveillance solutions, expanding employment opportunities, and investing in comprehensive training and skill development programs.

About CAPSI

The Central Association of Private Security Industry (CAPSI) is India's premier organization representing the interests of the private security sector. Formed in 2005, CAPSI functions as a unifying body and a voice for over 40,000 private security agencies employing nearly 10 million guards, making it the largest security workforce in the world. The organization plays a critical role in supporting the Indian government, law enforcement, corporate entities, and citizens by ensuring that private security services maintain the highest standards of integrity, discipline, and professionalism.

Under the leadership of its founding members—many of whom are distinguished senior officers from the Indian Police Services, Armed Forces, and Intelligence Bureau—CAPSI has transformed the fragmented PSI into a more cohesive, policy-influencing, and skill-building ecosystem. The organization actively collaborates with ministries

such as the Ministry of Home Affairs, Ministry of Labour and Employment, and Skill Development and Entrepreneurship, and works closely with regulatory bodies, training councils, and international partners. With the formation of focused task forces—such as the AI & Cybersecurity Task Force, Drone Security Task Force, and Women Security Empowerment Task Force—CAPSI is expanding the scope of PSI from traditional guarding services to become a strategic component of India’s hybrid security and surveillance architecture. CAPSI’s aim is not only to enhance internal security preparedness but also to transform PSI into a global leader by leveraging digital transformation, technological convergence, and skilled manpower.

Purpose and Audience of the Whitepaper

This whitepaper, titled "Adoption of Artificial Intelligence & Cybersecurity Frameworks in India’s Private Security Industry", has been conceptualized as a strategic and action-oriented document to guide policymakers, private security entrepreneurs, technology providers, and academic institutions on how to integrate AI, cybersecurity, and advanced technologies into the operational and regulatory fabric of PSI.

Purpose:

- **Policy Influence:** Present a compelling case to the Government of India to support the modernization of PSI through policy interventions, funding, incentives, and public-private collaboration.
- **Roadmap for Modernization:** Define a future-ready roadmap for digital transformation, covering AI integration, drone operations, cybersecurity, and workforce upskilling.
- **Awareness and Advocacy:** Raise awareness about the urgent need to protect India’s digital-physical assets through the deployment of tech-enabled security personnel and systems.
- **Standardization and Training:** Recommend national-level training, certification, and audit mechanisms for ensuring secure, ethical, and efficient use of AI and autonomous systems in PSI.
- **Industry Collaboration:** Encourage Indian startups, global innovators, and research institutions to co-develop customized security technology solutions tailored for India’s unique socio-economic environment.

Audience:

- **Government Ministries:** Home Affairs, Electronics & IT, Skill Development, Defence, Urban Development, Civil Aviation.
- **Lawmakers and Policy Think Tanks:** NITI Aayog, Bureau of Police Research & Development, Parliament Standing Committees.
- **Private Security Agencies and Facility Managers**
- **Technology Providers and System Integrators**
- **Academic and Research Institutions**
- **Media and Public Interest Groups**
- **International Security and AI Forums**

This whitepaper also seeks to mobilize national attention on the urgency of empowering PSI to defend India not just from physical threats, but from a rising spectrum of cyber-physical risks posed by hostile state and non-state actors, digital disruption, and global uncertainties.

Summary of Key Developments in PSI Globally and in India

The PSI landscape is undergoing a tectonic shift, influenced by geopolitical tensions, technological breakthroughs, and the redefinition of "security" itself in the age of smart cities and hybrid warfare. Below is a summary of these transformations:

A. Global Trends in Private Security Industry

- **Technology-First Security Models**

Global PSI players are deploying AI-powered surveillance, facial recognition, predictive policing tools, smart uniforms, real-time dashboards, and autonomous drones. Countries like the USA, UK, UAE, and Israel have integrated technology into every layer of private security—from gatekeeping to event security to maritime surveillance.

- **Rise of Autonomous Systems**

Robotic sentries, automated access control systems, and autonomous surveillance drones are reducing dependence on human guards while increasing operational reach. These systems, however, pose cybersecurity vulnerabilities if not properly secured.

- **Cyber-Physical Convergence**

The definition of “security” has expanded. Protection of critical infrastructure now includes both physical access and cybersecurity of embedded IoT systems. Security personnel are being trained in digital forensics, cyber hygiene, and incident response.

- **Increased Use of Drones and Aerial Surveillance**

Drones have become essential for monitoring large perimeters, crowd control, border security, and emergency response. However, drone hijacking, GPS spoofing, and cross-border surveillance threats by rogue actors have raised cybersecurity red flags.

- **Insider and Non-State Threats**

Cyber mercenaries, freelance hackers, and ideologically motivated actors have emerged as major risks. The ability of non-state actors to target critical infrastructure using cheap, scalable technology is creating new security challenges.

- **Skill Shortage and Role Redefinition**

Traditional security guards are being replaced or re-deployed as AI systems take over repetitive tasks. This demands a rapid re-skilling and upskilling agenda, globally led by hybrid training institutions.

- **Regulatory and Ethical Frameworks**

Nations are creating regulatory guardrails for ethical AI use, surveillance rights, and cyber accountability in private security services. Standardization bodies are forming new ISO/IEC codes for AI-based private security.

B. Key Developments in India’s PSI

Expansion of Guarding Services to Tech-Enabled Operations

Major Indian players like SIS, G4S, and Peregrine are incorporating surveillance tech, command centers, access control software, and even cyber incident handling as part of their portfolio.

- **Introduction of Drone Surveillance**

Drones are being used for securing industrial corridors, VIP events, oil pipelines, and border states. CAPSI's drone task force is laying down SOPs and training protocols for safe deployment.

- **Smart City Integration**

PSI agencies are working with municipal bodies and private developers in smart cities to run integrated control rooms, AI camera grids, and real-time threat detection systems.

- **Rise of Cybercrime & Need for Secure Autonomous Systems**

Increased digitization has made PSI agencies vulnerable to data leaks, ransomware, and system hijacking. Agencies deploying autonomous systems without hardened cybersecurity frameworks are increasingly under threat.

- **Training Gaps and Skill Deficits**

Over 80% of PSI workforce remains under-skilled in AI, cybersecurity, or tech usage. Rashtriya Raksha University (RRU), in collaboration with CAPSI, is working to bridge this gap.

- **Inadequate Policy and Incentives**

While India has made strides with the Drone Rules, 2021, and Digital India, private security remains outside the ambit of most national innovation and digital empowerment missions. The absence of clear guidelines on AI use in private security hinders innovation.

- **Global Collaboration Opportunities**

With India becoming a key global partner in digital diplomacy and cybersecurity, PSI can leverage international collaborations with nations like UAE, Australia, and Israel to adopt world-class practices.

The Urgency for Transformation

The world is transitioning into the Age of Agentic AI Systems—where software agents act independently, make decisions, and carry out tasks in physical or digital environments. This change is already replacing human roles across transport, logistics, security, and monitoring. India cannot afford for its PSI to lag behind. Without a strong policy push, a structured modernization strategy, and reskilling pathways, millions of Indian guards risk being left behind.

Moreover, the proliferation of dual-use drones, autonomous patrol bots, AI-based facial recognition, and surveillance systems being weaponized by adversarial non-state actors, requires India to prepare its PSI to counter such threats both physically and digitally.

Call to Action

This whitepaper is a wake-up call for all stakeholders to act collectively—modernize, secure, and empower the PSI of India. By integrating AI, drones, and cybersecurity frameworks into security operations, and by ensuring continuous training and reskilling, India can:

- Secure its critical infrastructure,
- Defend against digital intrusions,
- Improve security efficiency and accuracy, and
- Generate high-value employment in tech-enabled roles.

The CAPSI AI & Cybersecurity Task Force is committed to catalyzing this shift by providing leadership, policy advocacy, and actionable blueprints for nationwide adoption. This whitepaper serves as a foundational document in that mission.

Chapter 2: Current State of Technology in Indian Private Security

2.1 Tech Readiness of Indian Agencies

The Indian Private Security Industry (PSI), comprising over 48,000 agencies and employing nearly 10 million people, is vast but unevenly digitized. While the top 5–10% of large, organized players have started integrating technology into their service delivery models, the majority of small and medium enterprises (SMEs) in the sector continue to operate with outdated manual processes, low-tech surveillance setups, and negligible cybersecurity measures.

A. Digitization Maturity

- Top-tier PSI agencies have adopted basic digitization measures such as biometric attendance, GPS- based guard tracking, digital shift scheduling, and mobile app-based field reporting.
- Mid-tier firms often still use Excel sheets, manual registers, and landline-based control rooms.
- Bottom-tier and rural-focused agencies are entirely offline, with no digital records, workforce analytics, or operational dashboards.

B. Surveillance Technology Usage

Some leading agencies use CCTV with cloud access, motion sensors, RFID systems, and metal detectors. However, the integration of AI-powered video analytics, facial recognition, or anomaly detection remains minimal.

Drones for surveillance, though promising, are only being piloted by a handful of agencies due to cost, regulatory ambiguity, and lack of skilled drone operators.

C. Automation and Robotics

Robotic sentry and patrol bots are emerging globally, but Indian adoption is negligible.

There are isolated cases of firms experimenting with autonomous security drones and smart patrolling bots in gated communities or industrial zones.

Most PSI companies lack the technical or financial capacity to explore such innovations independently.

D. Command-and-Control Integration

Few firms operate centralized command centers for real-time coordination across locations.

Use of incident reporting apps, panic buttons, or alert escalation systems is rare and unstandardized. Integration with city-wide smart surveillance infrastructure (as seen in Smart Cities projects) remains aspirational.

E. Cybersecurity Consciousness

Most PSI firms still view cybersecurity as an IT function, not a core security offering.

Very few agencies offer cyber protection services for client premises, such as endpoint monitoring, network security, or digital threat alerts.

Summary of Tech Readiness

Category	High (Top 10%)	Medium (30-40%)	Low (50-60%)
Digitized Guard Management	✓	Partial	X
AI-based Surveillance	Partial	X	X
Drone Surveillance	Pilot stage	X	X
Cybersecurity Capabilities	Emerging	X	X
Training on Tech Tools	Limited	X	X
Client Awareness of Tech Needs	Medium	Low	Very Low

Summary of Technology Readiness in PSI- India

2.2 Training, Infrastructure, and Policy Gaps

A. Training and Skill Development Deficit

The biggest gap in technology adoption is human capacity. Most guards come from underprivileged backgrounds, with limited formal education or digital exposure.

- Digital Literacy: Over 70% of the guard workforce lacks basic smartphone or computer literacy.
- AI/Cyber Training: Negligible access to structured training on AI tools, data protection, surveillance ethics, or cyber incident response.
- Drone Operation Certification: Few training centers in India provide DGCA-compliant drone pilot training focused on security use-cases.
- Skilling Institutions: Current skilling under traini and Sector Skill Councils (SSC) focuses on physical guarding; integration of AI, drone, and cyber modules is urgently needed.

B. Infrastructure Constraints

Lack of Funding: Small firms do not have the capital to invest in modern tech infrastructure, data centers, or AI tools.

Connectivity: Rural and semi-urban PSI operations often suffer from poor internet connectivity, making real-time surveillance or cloud-based operations difficult.

Hardware Limitations: Many firms use outdated cameras, analogue radios, and unencrypted communication systems.

Lack of Common Platforms: There is no standardized national platform for PSI firms to access tools like guard scheduling, training simulators, or cyber alert systems.

C. Policy and Regulatory Ambiguity

No National AI Policy for PSI: While NITI Aayog has promoted AI in health and education, there is no equivalent roadmap for PSI modernization.

Drone Policy Gaps: The Drone Rules, 2021, are progressive but lack alignment with private security applications (e.g., use for crowd surveillance or perimeter security).

Cybersecurity Policy Disconnect: PSI agencies are not directly addressed in India's Cybersecurity Policy drafts, despite being critical to protecting physical entry points of digital infrastructure.

Licensing and Compliance: PSARA (Private Security Agencies Regulation Act) does not mandate tech use or cybersecurity protocols, making enforcement of digital standards impossible.

D. Awareness Among Clients and Policymakers

Clients (residential societies, small businesses) often demand the lowest-cost guard services, ignoring tech integration.

Government security tenders rarely prioritize or reward use of AI, surveillance analytics, or autonomous systems.

There is limited engagement between policymakers and PSI stakeholders on modernization goals.

2.3 Cybersecurity Maturity in PSI Companies

The cybersecurity posture of most PSI companies is weak or non-existent. Despite being responsible for safeguarding high-value clients—banks, airports, logistics hubs, corporate parks—PSI firms themselves are ill-prepared to deal with modern cyber threats.

A. Internal Cyber Hygiene

Password sharing, lack of multi-factor authentication, unsecured devices, and unencrypted communications are common.

Many PSI firms store client data in Excel sheets or unsecured local servers, exposing them to breaches. Very few companies have CISO-level leadership or cybersecurity audits.

B. Incident Preparedness

No formal Incident Response Plans (IRP) exist in most companies.

There is low awareness about ransomware, phishing attacks, deepfakes, or social engineering threats.

Firms that rely on CCTV networks often fail to secure IoT endpoints, making them susceptible to botnet infections or remote hijacking.

C. Third-Party Exposure

PSI companies access client buildings, digital systems, and sometimes personal data—making them potential entry points for cyberattacks on clients.

However, most clients do not mandate cybersecurity audits of their security vendors.

PSI companies often subcontract services to even smaller vendors without cyber vetting, increasing the attack surface.

D. Opportunity: Cybersecurity-as-a-Service

With growing awareness, PSI firms could expand into cybersecurity service offerings—such as SOC-lite (Security Operation Center for SMEs), endpoint protection, or digital surveillance.

However, this requires investment, training, and regulatory support.

Summary: Cybersecurity Maturity

Category	Status
Data Security Practices	Weak
Incident Response Plan	Rare
IoT & Surveillance Security	Neglected
Cyber Awareness & Training	Very Low
Cyber Services to Clients	Emerging Potential
Regulatory Oversight	Absent

Summary of Cybersecurity Readiness of PSI-India

Conclusion

The Indian Private Security Industry is at a strategic inflection point. While the physical size and employment power of the industry are formidable, its technological maturity, cybersecurity posture, and training infrastructure are grossly inadequate in the face of emerging threats.

To realize the vision of a digitally empowered PSI capable of defending India's critical infrastructure, urgent efforts are needed to:

- Build digital literacy and cyber awareness across all ranks.
- Encourage investment in surveillance AI, drones, and automation.
- Integrate PSI into national cybersecurity and AI strategies.
- Create strong public-private partnerships and innovation ecosystems.

The following chapters will provide strategic objectives, key recommendations, and actionable roadmaps to accelerate this transformation.

Chapter 3: AI-Driven Challenges and Opportunities for PSI

Introduction

Artificial Intelligence (AI) has emerged as both a transformative force and a complex threat vector in the evolving landscape of security. As AI technologies become more pervasive—powering everything from surveillance cameras to automated threat detection systems—they are simultaneously being exploited by malicious actors to carry out sophisticated cyber and physical attacks. For the Private Security Industry (PSI), this duality presents a critical inflection point. Embracing AI is no longer optional; it is essential to remain relevant, effective, and future-ready.

AI-Driven Challenges: A New Cyber-Physical Threat Frontier

1. Autonomous Threats and Deepfake Exploits

AI is enabling the creation of hyper-realistic deepfakes and synthetic media that can deceive even the most seasoned professionals. In PSI, this means threats like:

- Fake video footage used to manipulate evidence from surveillance systems.
- Voice cloning to bypass voice-based authentication systems.
- Impersonation of VIP clients or security personnel to gain unauthorized access.

Example: In 2023, a major European bank lost \$35 million after deepfake audio impersonated a company executive in a fraudulent transfer.

2. AI-Enhanced Cyberattacks

Attackers are leveraging AI to automate the scanning of vulnerabilities, craft highly personalized phishing campaigns, and even launch self-adapting malware. These tactics target the digital infrastructure of PSI providers and clients alike.

Example: AI-powered ransomware variants have been observed analyzing file structures and user behaviour before encrypting, making recovery more complex.

3. Smart Surveillance Misuse

Advanced surveillance systems using AI for facial recognition and behaviour analytics can be vulnerable to algorithmic bias, spoofing, or misuse by rogue insiders, creating significant legal and ethical implications.

AI-Driven Opportunities: Redefining PSI's Role

1. Predictive Threat Intelligence & Smart Policing

AI models can analyze massive datasets from CCTV footage, access control logs, social media, and public databases to identify abnormal patterns and predict threats before they occur.

- Predictive patrols in gated communities.
- Real-time alerts for unattended objects or crowd surges at high-security events.

Example: AI tools deployed at public infrastructure sites have helped reduce unauthorized access by 40% through anomaly detection and early alerts.

2. Advanced SOCs and SIEM Systems

AI-enabled Security Operations Centers (SOCs) and Security Information and Event Management (SIEM) systems can:

- Filter and prioritize thousands of daily alerts.
- Correlate events from multiple sources.
- Automatically respond to known threat signatures.

These systems reduce response time from hours to minutes and enhance accuracy in threat triage.

3. Enhanced Electronic Surveillance

Integration of AI into electronic surveillance:

- Smart cameras detect intrusion or aggression without human monitoring.
- License plate recognition systems track vehicles in real time.
- AI drones assist in perimeter surveillance for industrial and remote sites.

4. Upskilling the PSI Workforce

AI opens new employment paths within PSI—cybersecurity analysts, drone operators, surveillance auditors, SOC analysts. It empowers PSI firms to:

- Upskill existing guards in tech surveillance operations.
- Create tiered job roles based on AI-system interaction.

Imperatives for PSI: Navigating the AI Era

1. Invest in Training and Simulation

Every PSI organization must incorporate AI and cybersecurity in its training curricula. Simulation-based training on cyber threats, facial recognition accuracy, and emergency response are essential.\

2. Collaborate with Tech Companies

Collaborations with AI companies and tech partners (e.g., Microsoft, IBM, Palo Alto Networks) can ensure access to cutting-edge tools and best practices.

3. Establish Centers of Excellence (CoEs)

Set up CoEs in partnership with CAPSI, CyberPeace, and global vendors to:

- Train PSI personnel in emerging technologies.
- Serve as hubs for research, testing, and deployment of AI-integrated solutions.
- Conduct cybersecurity drills and live threat simulations.

4. Adopt Regulatory and Ethical AI Standards

Work with government bodies to shape AI regulations that protect privacy and civil liberties while allowing innovation.

Conclusion

The convergence of AI and security is reshaping the mission and scope of the Private Security Industry. While AI brings unprecedented efficiency and capability, it also introduces a new era of complex, fast-moving threats. The PSI must respond with agility, investing in people, partnerships, and platforms to not only counteract risks but to lead the transformation of security services in the digital age. India has the unique opportunity to become a global leader in AI-integrated private security by embracing innovation with responsibility and speed.

Chapter 4: CAPSI's Strategic Pillars

Skilling, Policy Advocacy, Tech Adoption, PPP Models

India's Private Security Industry (PSI) stands at a critical juncture where traditional guarding services must evolve into technology-enabled, intelligence-backed, and digitally resilient operations. As the leading national body representing over 10 million security professionals, the Central Association of Private Security Industry (CAPSI) has laid down a robust foundation to navigate this transformation.

This chapter elaborates on CAPSI's four strategic pillars that will shape the future of PSI in India:

- Skilling and Reskilling for the Future
- Policy Advocacy and Regulatory Reform
- Technology Adoption and Innovation Enablement
- Public-Private Partnership (PPP) Models for National Security

4.1 Chairman, Kunwar Vikram Singh's Message

"India's private security sector is no longer just a uniformed force; it is an extension of our national security ecosystem. As threats evolve—from cyberattacks to drone incursions, from data theft to autonomous systems misuse—so too must the industry evolve. CAPSI is committed to building a new generation of skilled, ethical, and tech-savvy professionals who can safeguard both physical and digital assets. We are advocating at the highest levels for reform in regulation, investment in digital skilling, and integration of the PSI into national security strategy through collaborative Public-Private Partnerships. This whitepaper is our call to action for all stakeholders to unite in building a secure India for the 21st century."

— Kunwar Vikram Singh, Chairman, CAPSI

4.2 Pillar 1: Skilling and Reskilling for the Future

The Imperative

With nearly 50% of guarding functions expected to be automated by 2030, CAPSI recognizes the urgent need to reskill India's vast PSI workforce. Automation, AI surveillance, drone patrolling, and cyber protocols are reshaping job roles. The future of private security lies not only in muscle and vigilance but in data fluency, technical competence, and ethical cyber practices.

Key Initiatives

- National Occupational Standards (NOS) Revamp: CAPSI, in partnership with RRU is redesigning occupational standards to include:
 - Drone surveillance
 - AI-integrated patrolling
 - Cyber hygiene and digital incident reporting
- AI & Cybersecurity Training Curriculum: CAPSI's training blueprint now includes:
 - Introduction to autonomous security systems
 - Cybersecurity awareness and incident reporting
 - Protocols for data protection and privacy
- Train-the-Trainer Model: Over 500 master trainers will be certified to deliver tech-enabled skilling across CAPSI-affiliated training centers.
- Recognition of Prior Learning (RPL): Incorporating upskilling pathways for currently employed guards to stay relevant in the age of automation.

Strategic Outcome

Positioning private security personnel as multi-skilled security professionals who can safeguard physical spaces, digital assets, and client trust in one integrated role.

4.3 Pillar 2: Policy Advocacy and Regulatory Reform

The Challenge

Current laws governing PSI—most notably the Private Security Agencies Regulation Act (PSARA), 2005—do not address digital surveillance, cyber risks, or the integration of autonomous technologies. There is no mention of AI, drones, or cybersecurity protocols.

CAPSI's Advocacy Priorities

- Amending PSARA to include Technology Mandates: Proposals include:
- Mandatory tech audits for large agencies
- Incentivizing adoption of surveillance AI and drone systems
- Inclusion in National Cybersecurity Frameworks:

CAPSI has petitioned for PSI to be recognized under India's upcoming cybersecurity policy as a frontline security provider

Policy on Autonomous Systems Security: Advocating for formal guidelines on the ethical use and protection of AI agents, drones, and robotic systems in civilian spaces

Insurance and Compliance Advocacy:

Working with IRDAI to create specialized cyber-risk coverage for PSI vendors

Strategic Outcome

Ensuring that India's regulatory ecosystem evolves in tandem with emerging threats, positioning PSI as an accountable and digitally enabled force.

4.4 Pillar 3: Technology Adoption and Innovation Enablement

The Challenge

Most PSI agencies, particularly SMEs, are unable to invest in modern technology due to cost, lack of training, and regulatory uncertainty. The industry is missing out on AI-powered surveillance, drone capabilities, and incident management platforms.

CAPSI-Led Solutions (In the Pipeline)

- AI & Drone Task Force: A dedicated working group exploring use-cases, guidelines, and pilot projects involving:
- Autonomous drone patrols for perimeter surveillance
- AI facial recognition integrated with guard check-in systems
- Technology Vendor Marketplace:
- A curated B2B platform to connect PSI agencies with verified tech providers for CCTV, analytics, AI dashboards, and cybersecurity solutions

Innovation Incubation Program:

Collaborating with IITs, NITs, and private accelerators to co-develop PSI-specific tech tools and platforms

Digital Guard Passport:

A blockchain-based certification repository to track skills, training, assignments, and incident performance for guards, ensuring transparency and accountability

Strategic Outcome

Bridging the digital divide across PSI through structured, cost-effective tech adoption pathways.

4.5 Pillar 4: Public-Private Partnership (PPP) Models for National Security**The Opportunity**

Private Security now guards everything from banks and tech parks to transport terminals and data centers—many of which are designated Critical Information Infrastructure (CII). However, there is no formal PPP model that integrates private security into India’s national or state-level security planning.

CAPSI’s PPP Engagement Blueprint

- **State-Level Security Councils:**
CAPSI is working with state governments to form Private Security Councils that advise on citywide security, digital surveillance, and risk preparedness
- **Smart City Partnerships:**
Enabling PSI participation in integrated command centers through CAPSI’s standard training and technology protocols
- **Cyber Threat Coordination Cells:**
CAPSI is proposing regional coordination units where PSI firms can report, alert, and escalate digital threats observed in the field
- **Disaster & Crisis Response Integration:**
CAPSI-trained PSI personnel can be deputed during natural disasters, cyber sabotage incidents, or public health crises

Strategic Outcome

Creating formal bridges between private security and national/state governance, especially for urban security, cyber vigilance, and disaster readiness.

4.6 CAPSI’s Current Programs (MoUs, Task Forces, Training)**A. Training Programs**

CAPSI and its affiliate Training partners runs over 70 training institutions across India.

Ongoing programs include:

- Cyber Awareness & Risk Detection
- Drone Surveillance Techniques
- Workplace Conflict Resolution
- Digital Patrolling Systems

B. Strategic MoUs

RRU: Joint development of new skill qualifications for Tech-Enabled Security

AICTE/UGC: University-certified skilling for youth entering the PSI domain

DRDO Collaborations: Exploring autonomous patrolling systems and AI-vision capabilities for high-security Zones

C. Task Forces

- AI & Drone Task Force: Developing framework for drone deployment in PSI
- Cybersecurity & Data Protection Group: Creating SOPs for PSI companies handling sensitive digital assets
- Women in Security Task Force: Promoting diversity and gender-inclusive roles in modern private security roles

Conclusion

CAPSI's four strategic pillars are not just aspirational frameworks—they are concrete pathways to enable India's Private Security Industry to transition into a 21st-century force multiplier for national resilience. Through skilling, tech enablement, regulatory influence, and public-private collaboration, CAPSI is shaping the future of a secure, modern, and digitally integrated India.

Chapter 5: Emerging Technologies for Private Security Technology (PST) Adoption

India's Private Security Industry (PSI) is undergoing a paradigm shift, moving from conventional guarding services to intelligent, data-driven, and technology-augmented operations. The rise of Industry 4.0, national digital infrastructure, and smart city projects is generating a complex security landscape, where emerging technologies play a vital role in enhancing situational awareness, risk prevention, response time, and operational efficiency. This chapter explores the key emerging technologies that are expected to redefine Private Security Technology (PST) adoption in India:

5.1 Artificial Intelligence (AI) & Machine Learning (ML)

Why AI/ML for PSI?

AI and ML technologies have the power to process vast amounts of surveillance data, detect patterns, and predict threats with greater speed and accuracy than human operators. For private security, this translates to:

- Real-time threat detection and analysis
- Predictive risk analytics
- Automated patrol planning and resource deployment

Use Cases in PSI

- Facial recognition systems for identity verification at entry points
- Anomaly detection in access control logs and surveillance footage
- AI-powered workforce management tools for guard shift optimization and performance monitoring
- Sentiment analysis of crowds in public areas for early detection of civil unrest or aggression

Indian Adoption Examples

- AI-enabled command centers in smart cities
- Private security contracts in industrial zones integrating AI video analytics
- Early adoption by metro rail systems and airports for predictive surveillance

5.2 Computer Vision, Robotics & Automation

Computer Vision

Computer vision leverages AI to "see" and analyze video content in real-time. It's the backbone of modern surveillance, enabling:

- Automatic number plate recognition (ANPR)
- Intrusion detection with behavior analytics
- Perimeter breach alerts in low-light or no-light environments
- Mask/no-mask, helmet/no-helmet detection in compliance zones

Robotics in Guarding

- Robots are being deployed in high-risk or sensitive areas such as:
- Banks, data centers, and defense factories
- Night patrolling in IT parks and logistics hubs
- Thermal imaging robots for hazardous environments

These robots come equipped with:

- LIDAR-based navigation
- Thermal and night vision cameras
- Audio alert systems
- 2-way communication

Automation Tools

- Access control systems integrated with biometric and RFID verification
- Automated visitor management systems with mobile OTPs and facial scanning
- Autonomous patrolling bots in warehouses and large complexes

5.3 IoT & Smart Surveillance

IoT in Private Security

Internet of Things (IoT) enables connected security devices to share real-time data with control centers, enhancing responsiveness and coordination.

Applications:

- Smart alarm systems connected to control rooms via GSM/Wi-Fi
- Environment sensors for smoke, gas, flood, and movement detection
- Wearables for guards to transmit location, status, and incident alerts
- Geo-fencing enabled patrolling with violation triggers

Smart Surveillance Systems

- Integration of IP cameras, AI analytics, and cloud storage
- Real-time streaming to mobile dashboards and central control centers
- Use of edge computing for on-device analysis, reducing reliance on centralized servers

Indian Context

Smart cities like Bhopal, Pune, and Surat have implemented IoT-based surveillance grids with CAPSI-certified agencies providing last-mile human monitoring and response.

5.4 Drone Integration in Guarding Services

Why Drones?

Drones offer unmatched aerial surveillance capabilities in large campuses, industrial estates, border zones, and perimeters where human patrol is inefficient.

Applications in PSI

- Perimeter security and patrolling of remote or large facilities (e.g. solar parks, SEZs)
- Event surveillance during large public gatherings
- Intrusion detection using night vision and infrared drones
- Disaster response: Assessing security risks post-calamity from a bird's eye view

Drone-As-A-Service (DaaS) Model

CAPSI supports the development of DaaS partnerships where drone service providers work with private security agencies for:

- Scheduled drone patrols
- Real-time visual feeds
- Automated alerts via AI analysis

Policy & Compliance

Compliance with DGCA's Drone Airspace Map, NPNT (No Permission No Takeoff) protocols
Training of drone pilots under DGCA-approved institutions

5.5 Cybersecurity: Zero Trust, Threat Detection, and Incident Response The Cybersecurity Imperative

As PSI agencies begin handling digital infrastructure (CCTV networks, access logs, drone feeds, etc.), cybersecurity becomes integral to operational integrity.

Zero Trust Architecture (ZTA)

- The Zero Trust model ensures that:
- Every access attempt is verified
- Devices are authenticated before being granted access
- Micro-segmentation protects different parts of surveillance networks

Threat Detection & SIEM

- Security Information and Event Management (SIEM) systems analyze logs from security devices and raise alerts for:
- Malware attacks
- Unauthorized access
- Suspicious file transfers
- CAPSI recommends managed SIEM services for mid-sized PSI firms that lack in-house cybersecurity teams

Incident Response Protocols

Every PSI agency must maintain an Incident Response Plan (IRP) that includes:

- Reporting hierarchies for cyber breaches
- Client alert protocols
- Digital forensics readiness

CAPSI Task Force is preparing IRP templates for sector-wide adoption

Training Initiatives

- Guard-level Cyber Hygiene Programs
- Manager-level Digital Risk Handling Workshops
- Tech team hands-on cybersecurity courses through Rashtriya Raksha University (RRU) and private partners

Conclusion

The adoption of emerging technologies is not optional—it is a strategic necessity for the Private Security Industry to stay relevant in the face of rising physical and cyber threats. AI, robotics, IoT, drones, and cybersecurity frameworks will become the new pillars of guarding, and CAPSI is leading the charge in building a roadmap for responsible, affordable, and scalable adoption.

By embracing these technologies, India's PSI will not only enhance its service delivery but will also emerge as a strategic ally to law enforcement, government agencies, and national cybersecurity frameworks.

Chapter 6: Creating Centers of Excellence (CoEs) in AI & Cybersecurity for PSI

Overview

To future-proof India's Private Security Industry (PSI) and keep pace with the exponential evolution of cyber threats and AI-led disruptions, CAPSI envisions setting up five state-of-the-art Centers of Excellence (CoEs) in collaboration with CyberPeace Foundation, Microsoft, Palo Alto Networks, IBM Security, Fortinet, and prominent academic institutions. These CoEs will be regional hubs for hands-on training, research, and deployment of real-world security solutions using licensed technologies and global best practices.

Purpose of CoEs

- Empower PSI Professionals with next-generation skills in AI, cybersecurity, threat intelligence, and digital forensics.
- Train Trainers and Commanders to implement advanced SOC (Security Operations Center) practices.
- Bridge the Skill Gap between manual guarding roles and AI-enabled, digitally empowered protection forces.
- Enhance National Preparedness by aligning private security with national cyber defence objectives.
- Engage Clients and Stakeholders through live demonstrations, cyber drills, and managed services.

Roles of Key Institutions

CAPSI (Central Association of Private Security Industry)

- Strategic Leadership in setting vision and standards for PSI modernization.
- Policy Advocacy with the government for funding, incentives, and formal recognition of AI/cybersecurity skilling.
- Operational Governance and rollout of training programs across PSI companies.
- Partnership Development with global and Indian technology leaders.

CyberPeace Foundation

- Hosts India's Most Advanced SOCs and cyber range environments.
- Provides Cybersecurity Awareness Modules for PSI staff, clients, and civilians.
- Supports Research & Threat Monitoring through its Cyber Threat Intelligence labs.
- Collaborates on Joint Training Programs for both entry-level and leadership tracks.

Global Tech Partners (e.g., Microsoft, Palo Alto, IBM, Fortinet)

- Provide Licensed Tools and Cloud Access for real-time threat emulation, monitoring, and sandbox testing.
- Design Industry-Relevant Courseware for endpoint protection, AI in threat detection, and Zero Trust architectures.
- Deploy Expert Faculty and Mentors for immersive training programs and mentorship.
- Ensure Global Certification Pathways for skilled PSI personnel.

CoE Locatio	Special Focus	Primary Partners	Key Functions
Delhi NCR	AI-Driven Threat Detection & Zero Trust	Microsoft, CyberPeace Foundation	Executive skilling, M365 Defender & Sentinel, Zero Trust labs
Hyderabad	SOC-as-a-Service & Forensic Research	CyberPeace Foundation, IBM Security	SOC simulation, forensic analysis, threat intel, red-blue team training
Bangalore	IoT Security & Autonomous System Protection	Palo Alto Networks, Fortinet, IISc	Smart surveillance, drone security, OT/ICS lab setups
Mumbai	Financial Services Security & Risk Mgmt	Symantec, Check Point, NSE Academy	Financial sector security practices, phishing/ransomware mitigation
Kolkata/ Guwahati	Citizen & Border Zone Digital Security	Indian Army Veterans Network, CyberPeace, Regional Tech College	Community portal development, border security awareness, vernacular content labs

Suggested COEs to be set up by CAPSI

Program Highlights at CoEs

- **AI + Human Training Modules:** Structured dual-track education for frontline guards and command-level officers.
- **Certification-Backed Curriculum:** Co-created with partners; includes both CAPSI and international endorsements (e.g., CompTIA, ISC2).
- **Hands-on Labs & Virtual Cyber Ranges:** Real-world threat detection, forensic simulation, red teaming, and blue teaming exercises.
- **Client Immersion Workshops:** Training senior security officers of major client organizations in SOC integration and AI-led security policy implementation.
- **Innovation Hackathons:** Annual events to co-create innovative security solutions using AI/ML, CV, NLP, and Blockchain.

Strategic Benefits

- **Holistic Capacity Building:** From guards to CXOs, across urban and rural PSI deployments.
- **Trust Building with Clients:** Demonstrating PSI's ability to safeguard digital and physical assets.
- **Global Positioning:** Making India a net exporter of private security talent equipped with AI/cyber expertise.
- **Employment and Entrepreneurship:** Creating new roles like "AI Security Analyst", "Drone Threat Investigator", "Cyber Protection Officer" within PSI firms.
- **Continuous Research:** CoEs will drive whitepapers, threat reports, and best practices contributing to India's cyber resilience posture.

Next Steps for Implementation

- MOU Signings with CAPSI, CyberPeace Foundation, and all tech partners.
- Launch of Pilot Training Batches (Q4 2025) in Delhi and Hyderabad.
- Onboarding of Instructors from industry, academia, and security agencies.
- Release of CoE Portal for registrations, content delivery, certification tracking.
- Annual CAPSI AI & Cybersecurity Conclave to showcase CoE outcomes and forge global alliances.

To address the growing cybersecurity threats and capitalize on AI-led opportunities, CAPSI can establish five Centers of Excellence (CoEs) across India in partnership with CyberPeace Foundation and global technology leaders like Microsoft, IBM, Palo Alto Networks, and Fortinet. These CoEs will serve as national hubs for advanced skilling, research, and real-time threat simulation for Private Security Industry (PSI) personnel, senior managers, and client organizations. Each center will focus on specific domains—ranging from AI threat detection and SOC operations to IoT and financial sector security—delivering certified hands-on training, deploying licensed tools, and fostering innovation through hackathons and immersive labs. Operated under CAPSI's strategic leadership and supported by CyberPeace's SOC infrastructure, the CoEs will build a digitally empowered PSI workforce, elevate industry standards, and position India as a global leader in AI-driven private security.

Chapter 7: Case Studies, Initiatives, and Pilot Programs

As the Private Security Industry (PSI) in India transitions from traditional manpower-heavy operations to technology-augmented guarding services, CAPSI has taken proactive steps to design, test, and scale pilot programs that integrate AI, cybersecurity, and digital tools into PSI workflows.

This chapter outlines the key initiatives, case studies, and pilot programs undertaken by CAPSI and its partners, reflecting the industry's readiness to adopt next-generation technologies. These pilots are designed not only to demonstrate feasibility but also to provide proof-of-concept models for nationwide scaling.

7.1 AI-enabled Guarding: CAPSI Pilot Batch (50 Personnel)

Objective

To demonstrate the practical use of AI tools and digital systems in enhancing the capability, efficiency, and accountability of private security guards.

Program Highlights

- **Participants:** 50 selected guards/officers from different states underwent training on AI-enabled monitoring tools, bodycams, facial recognition devices, and mobile reporting systems.
- **Location:** The pilot was rolled out in collaboration with two large gated communities in NCR and a manufacturing zone in Pune.
- **Tools Used:**
 - a) Body-worn cameras with real-time streaming and facial recognition
 - b) Mobile patrol app with geo-fencing and route adherence alerts
 - c) **AI-based attendance and shift-reporting software**

Outcomes:

- Incident detection accuracy improved by 30%
- Reduced response time by 40%
- Guards reported improved morale and confidence due to digital empowerment
- Clients expressed satisfaction with transparency and real-time updates

Scalability:

Based on the results, CAPSI plans to roll out this model to 1,000 guards over the next 12 months, creating a framework for "AI-Augmented Guarding Services" as an industry standard.

7.2 Cybersecurity Awareness Modules by CyberPeace Foundation

Objective

To equip private security personnel—especially those handling digital surveillance infrastructure—with the basic understanding of cyber hygiene, data protection, and threat detection.

Program Partners

- CyberPeace Foundation: India's premier cyber safety think tank
- CAPSI Cybersecurity Task Force

Module Structure:

- Module 1: Introduction to Cyber Threats in PSI (CCTV, access control, and mobile apps)
- Module 2: Cyber Hygiene & Digital Discipline
- Module 3: Social Engineering & Phishing Awareness
- Module 4: Reporting Protocols & Handling Data Breaches

Mode of Delivery:

- Bilingual (Hindi & English) online videos and live webinars
- Post-training certification
- Mobile-first learning interface with periodic alerts and updates

Key Impact:

- 500+ guards trained in 3 months
- 85% guards scored above 70% in digital hygiene practices
- Enhanced trust of clients in PSI's cyber-readiness

Future Plan:

Mandatory inclusion of cybersecurity module in all CAPSI-affiliated training programs with a "Cyber Responsible Guard" badge.

7.3 IITM Pravartak – Advanced AI & Cybersecurity Course Design**Overview**

In collaboration with IIT Madras Pravartak Technologies Foundation, CAPSI has initiated the co-design of India's first advanced AI & cybersecurity skilling curriculum tailored for Private Security professionals and supervisory staff.

Structure of the Program:**Foundational Track:**

- AI concepts and ethical usage
- Basics of cybersecurity and Zero Trust Models

Intermediate Track:

- AI for surveillance analytics
- Network and endpoint security for surveillance setups

Advanced Track:

- Integration of AI with drones, robotics, and IoT
- Real-world simulations of cyber incident response

Delivery Model:

- Online & hybrid sessions
- Weekend labs in Chennai, Hyderabad, and Delhi
- Final certification jointly issued by CAPSI & IITM Pravartak

Significance:

This program will bridge the knowledge gap between traditional PSI practices and future-ready skillsets, creating a cadre of “AI & Cybersecurity Officers” within the private security ecosystem.

7.4 Community Portal & App – CAPSI Connect Rollout**Vision**

To build a centralized digital ecosystem for PSI professionals, trainers, clients, and technology partners to connect, share knowledge, access tools, and seek help.

Features of CAPSI Connect:

- Profile-based dashboard for security guards, supervisors, and trainers
- Daily updates on industry trends, training videos, and alerts
- Helpline integration for legal aid, cyber complaints, and safety issues
- Chat groups & forums for discussing on-ground incidents and tech use cases
- Marketplace for tech vendors offering CAPSI-approved AI tools, bodycams, and patrol devices

Pilot Usage Data (as of April 2025): (experimental target audience)

- Over 5,000 downloads across Android/iOS
- 1,200+ daily active users
- 75% positive feedback on training content
- 15+ posts in the peer knowledge-sharing community

Future Enhancements:

- Integration with attendance and compliance management tools
- Launch of AI-based helpdesk chatbot
- Vendor evaluation and procurement tools with ratings

Conclusion

These initiatives reflect CAPSI’s commitment to transforming India’s PSI into a tech-empowered, future-resilient industry. By combining pilot programs, strategic collaborations with academia and cyber institutions, and real-world deployment, CAPSI is actively demonstrating what the future of private security in India should look like: digitally skilled, cyber-aware, and AI-augmented.

As these pilots scale and feedback is integrated, these models can be standardized and recommended to Government bodies, ensuring support in form of policy, recognition, and investment.

Chapter 8: Strategic Recommendations to Enable the Ecosystem

To achieve accelerated, responsible, and secure adoption of AI and cybersecurity across India's Private Security Industry (PSI), a multi-dimensional enabling ecosystem must be established. This ecosystem must balance innovation with regulation, promote scalable skilling and certifications, create robust public-private partnerships (PPPs), and ensure access to appropriate technology stacks and funding mechanisms. This chapter outlines the roadmap for building such a foundation, drawing upon best practices from global counterparts, including countries like the USA, UK, Israel, and Singapore.

8.1 Regulatory Imperatives: Standards, Certifications & Incentives

Need for Uniform Standards

India's PSI currently lacks nationally defined standards around the use of AI tools, cybersecurity frameworks, and digital surveillance in private guarding services. This regulatory gap exposes the industry to risks including:

- Inconsistent technology deployment
- Privacy breaches
- Non-compliance with data protection laws (e.g., DPDP Act)

Recommendations

- Establish CAPSI-CERT-IN-AI Working Group to issue baseline cybersecurity & AI usage guidelines for PSI
- Adopt NIST Cybersecurity Framework and ISO/IEC 27001 compliance for PSI tech vendors
- Define standard operating procedures (SOPs) for AI-driven video surveillance, drone usage, and real-time tracking systems

Smart Certification Models

Introduce tiered certification (Basic, Intermediate, Advanced) for:

- Security Guards using AI-enabled tools
- Supervisors responsible for cybersecurity protocol adherence
- Tech vendors providing AI/Cybersecurity solutions to PSI

Incentivization Framework

To accelerate adoption:

- Offer tax exemptions or procurement preference for licensed companies meeting tech-readiness and cybersecurity criteria
- Provide monetary incentives or cost-sharing grants for AI pilot projects within PSI companies

8.2 Capacity Building: Skilling 500+ Officers via Smart Certification

Strategic Need

India has over 10 million PSI personnel, but only a fraction are digitally literate or trained in AI tools or cybersecurity protocols. To mainstream these technologies, skilling of 500 senior officers and trainers as "change agents" is critical.

Phased Skilling Strategy

Phase	Target Group	Focus Areas	Delivery Model
Phase 1	100 CAPSI Master Trainers	AI/Cybersecurity basics, ethical tech use	Online + Residential
Phase 2	200 Supervisors	Hands-on with patrol tech, AI cameras, threat detection tools	Virtual Labs, MOOCs
Phase 3	200 Officers	Integration into guarding operations, policy design	Blended with practical modules

Creating Change Agents to Transform PSI

Smart Certification Features

- AI-powered test modules for skill validation
- Digital badges for LinkedIn profiles & employment portfolios
- Registry of certified professionals maintained by CAPSI for industry visibility

Benchmarking Global Practices

- UK SIA (Security Industry Authority) mandates digital training for all license holders
- Israel includes AI-centric risk training in military-to-PSI transitions
- Singapore's SkillsFuture supports AI-Cyber micro-credentials for gig security workers

8.3 PPP Models: Govt-CAPSI-Tech Collaboration

PPP Pillars

- Public-private partnerships are essential for driving innovation while maintaining accountability. CAPSI proposes a 3-way collaboration among:
- Government agencies (Ministry of Home Affairs, Ministry of Skill Development & Entrepreneurship, (MSD&E), RRU, MeitY)
- CAPSI-led industry task forces
- Tech companies offering AI, drone, cloud, and cybersecurity solutions

Model Initiatives

- Smart Guarding Pilot Zones – Jointly funded by Skill India, implemented with Tech Mahindra & Drone Federation of India
- Digital Surveillance Sandbox – In partnership with CERT-IN, DRDO and NASSCOM, testing AI-based threat detection tools in Tier 2 cities
- Women in AI Guarding – Targeting women PSI recruits with digital skill kits and cyber awareness, supported by CSR arms of large PSUs

8.4 Tech Stack: Open Source, Cloud Platforms, AI Vendors

Rationale

Cost-effective, scalable, and secure tech adoption is key for PSI. Preference should be given to interoperable open-source tools that can be adapted for the diverse needs of private security operations.

Component	Tools/Vendors	Remarks
Video Analytics	OpenCV, YOLOv8	Open-source models for facial, movement detection
Threat Detection	Snort, Suricata, OSSEC	Cyber intrusion detection for control rooms
Cloud Storage	AWS, Azure, Zoho, GCP	Encrypted storage for CCTV data
Field Apps	CAPSI Connect, OpenHIM	Custom Android apps for patrol and reporting
AI Training Simulators	Unity3D + GPT agents	Simulated AI training for real-world scenarios

Recommended Stack for Tech Adoption

Vendor Evaluation Framework

- Security compliance certifications (ISO 27001, SOC2)
- Indigenous development and localization
- Support for Hindi and regional languages
- Adherence to DPDP Act & NCIIPC guidelines

8.5 Funding Ecosystem: CSR, RRU Skill India, MeitY

Funding Requirements

To scale AI and cybersecurity adoption across India's PSI, CAPSI estimates an initial corpus of INR 50 Cr (~USD 6 Million) over 3 years, covering:

- Curriculum development
- Pilot infrastructure
- Certification programs
- Awareness campaigns

Potential Sources for funding initiatives are given below.

Source	Contribution Type	Remarks
CSR Funds (PSUs, Tech MNCs)	Grants for training & digital tools	Align with Schedule VII of Companies Act
NSDC	Co-funding skill certification & infrastructure	Can accredit CAPSI Academy as training partner
MeitY	Grant-in-aid for cybersecurity awareness & tech pilots	Under Digital India initiatives
Skill India	Support for content development, e-learning platforms	Standardized modules for PSI
State Governments	Land, training centers, and subsidies	Particularly in high PSI employment zones

Potential Funding Options for CAPSI initiatives

Global Benchmark

- US DHS funds private security digital transformation under "Protective Security Coordination"
- UK leverages Home Office funding for digital upskilling of guarding professionals
- EU Horizon Programs co-finance AI and cybersecurity pilots in private sector guarding, especially for airports, events, and border monitoring

Conclusion

For India to position its Private Security Industry as a globally competitive, AI-enabled, and cyber-resilient force, it must invest in a comprehensive enabling ecosystem. A balanced combination of forward-looking regulation, skilled manpower, tech accessibility, partnerships, and financing is essential. CAPSI stands ready to anchor this transformation, aligning industry priorities with national security and technological advancement imperatives.

Chapter 9: CAPSI's AI & Cybersecurity Task force driving Transformation

In January 2025, the Central Association of Private Security Industry (CAPSI) established a national task force focused on integrating Artificial Intelligence (AI) into the private security sector.

Introduction: CAPSI AI & Cybersecurity Task Force – Securing the Future of India's PSI

As India's Private Security Industry (PSI) transitions into the digital age, the convergence of physical and cyber threats has created an urgent need for adaptive, technology-driven responses. Recognizing this paradigm shift, the Central Association of Private Security Industry (CAPSI) has constituted the AI & Cybersecurity Task Force to spearhead innovation, capability building, and resilience within the PSI ecosystem.

This Task Force is envisioned as a national think tank and execution body that will:

- Define the cybersecurity framework relevant to PSI companies, professionals, and their clients.
- Accelerate the adoption of AI-powered security technologies, integrating surveillance, threat detection, and rapid response systems.
- Create a future-ready workforce by recommending curriculum, certifications, and training aligned to global cyber and AI standards.
- Foster collaboration between global cybersecurity firms, Indian PSI players, training institutions, and policy makers.

The CAPSI AI & Cybersecurity Task Force will serve as a bridge between traditional security protocols and the emerging tech-enabled security paradigm, helping transform India's PSI into a globally benchmarked, cyber-aware, AI-enabled industry. Through strategic partnerships, actionable policy recommendations, and cutting-edge research, this task force aims to safeguard not just the physical, but also the digital frontiers of Indian enterprises.

Key Pillars identified by the task force:

1. Creation of National Centers of Excellence (CoEs)

To institutionalize continuous innovation and skilling, five Centers of Excellence (CoEs) will be established in collaboration with global technology and cybersecurity leaders. These CoEs will serve as:

- Skill Enhancement Hubs for PSI personnel, senior managers, and command-level staff.
- Technology Adoption Incubators for piloting and deploying cutting-edge security solutions.
- Cyber-Physical Research Centers focusing on AI, threat simulation, ethical hacking, digital forensics, and smart surveillance.
- Industry Collaboration Forums for PSI companies, clients, regulators, academia, and technology providers.

Location	Focus Area	Partner Organizations
New Delhi NCR	AI-Driven Surveillance and SOC Training	CyberPeace Foundation, IBM, Honeywell, Hikvision
Hyderabad	Cybersecurity Operations & Incident Response	Microsoft, CyberPeace, Palo Alto Networks, Tech Mahindra

Location	Focus Area	Partner Organizations
Mumbai	Maritime & Infrastructure Security	Cisco, Fortinet, Indian Navy (Liaison), L&T
Bengaluru	Smart City & Critical Infrastructure Security	Bosch, Accenture, TCS, ISAC Foundation
Pune	Manufacturing & Industrial Asset Protection	Siemens, Kaspersky, Automation Anywhere

Focus areas to be Double clicked. through COEs

2. AI-Driven Cybersecurity Integration in PSI Services

- Given the rise of cyber-physical threats, PSI organizations must integrate AI into the core of their operations. Key initiatives include:
- Deployment of AI-based Monitoring Tools in command centers to detect anomalies, intrusion, perimeter breaches, and behavioural deviations.
- Collaboration with AI Security Firms for facial recognition, drone analytics, vehicle tracking, and autonomous patrolling.
- Training Guards and Supervisors to operate tech-enabled systems, use hand-held AI scanners, and respond to cyber threats.

Outcome Goal: Make cybersecurity and AI knowledge foundational for 1 million PSI personnel by 2027.

3. Integrated Electronic Surveillance and Smart Guarding

- Standardize the use of smart cameras, biometric access controls, AI motion detectors, and drones in all high-risk zones.
- Promote smart patrolling with live geo-fencing and real-time reporting through integrated mobile apps.
- Digitize incident logs, visitor management, and guard tour verification systems.

4. Skilling and Career Progression

- Mandatory Cyber & Tech Certification for all PSI recruits within 6 months of induction.
- Introduce Dual Career Tracks: traditional guarding and tech-enabled roles such as SOC analyst, drone operator, cybersecurity assistant, etc.
- Collaborate with RRU and global edtechs for multilingual and hands-on training content.

5. Client Awareness and Technology Enablement

- Conduct industry-wide awareness sessions for top clients in BFSI, pharma, retail, logistics, manufacturing, and energy sectors.
- Offer Cyber Risk Readiness Audits and Tech Adoption Scorecards to help clients benchmark and modernize their PSI infrastructure.
- Co-develop AI-integrated emergency protocols and threat drills.

6. Policy and Standards Leadership

- Work with regulators like MHA, NASSCOM, BIS, and RRU to draft India's PSI Tech Guidelines 2026.
- Promote adoption of Ethical AI Standards, Data Privacy Norms, and Responsible Surveillance Policies.
- Ensure PSI firms comply with international security standards (ISO/IEC 27001, GDPR, etc.)

7. Innovation Ecosystem and Start-Up Acceleration

- Create an innovation sandbox for security startups to co-develop next-gen products with PSI companies.
- Launch an annual PSI Tech Challenge to fund innovations in AI surveillance, biometric security, and autonomous systems.
- Incentivize Indian MSME product companies to partner with CoEs for domestic solutions.

Conclusion

India has the talent, demand base, and ecosystem readiness to lead the next global revolution in private security services. Through an integrated roadmap focused on Centers of Excellence, AI adoption, cyber-physical integration, skilling, and collaborative innovation, the PSI can transition into a future-proof, globally respected force. CAPSI, together with strategic partners like CyberPeace Foundation and global tech leaders, will play a critical role in executing this ambitious, yet achievable, roadmap by 2027.

Chapter 10: Proposed Roadmap 2025–2027

Towards Global Leadership in Technology Adoption in Private Security Industry (PSI)

Overview

India's Private Security Industry (PSI), employing over 10 million personnel and is standing at the brink of a massive transformation. Driven by the intersection of technological evolution, changing threat dynamics, and increased demand for integrated physical-cyber security, the roadmap from 2025 to 2027 outlines a path for India to emerge as a global leader in technology-enabled PSI services. This roadmap focuses on enabling PSI organizations to evolve from traditional guarding operations to intelligence-led, AI-powered security solutions that safeguard physical and digital assets.

In this report, we outlined strategic interventions, key milestones, outcome expectations, and KPIs to guide the transformation of PSI into a digital-first and future-ready industry.

10.1 Vision 2027: India as a Global Leader in Tech-Driven PSI

The vision is to:

"Position India as a global hub for tech-enabled private security services by 2027 through robust skilling, strategic partnerships, AI & cybersecurity integration, and global-standard regulation."

This involves:

- Creating a digitally skilled PSI workforce
- Implementing AI and cybersecurity solutions across guarding operations
- Launching a national digital ecosystem for PSI stakeholders
- Driving innovation through Public-Private Partnerships (PPP)
- Making India a net exporter of PSI knowledge and solutions

10.2 Key Milestones (2025–2027)

Year	Key Focus	Milestones
2025	Foundation & Early Adoption	<ul style="list-style-type: none">- Train 500 officers under Smart Certification Program- Launch CAPSI Connect 1.0 app & Community Portal- 5 AI & cybersecurity pilot programs in Tier 1 & Tier 2 cities- Establish AI-Cyber Task Force within CAPSI- Issue national PSI-AI-Cybersecurity Best Practices whitepaper
2026	Scale & Regulation	<ul style="list-style-type: none">- Certify 5,000 PSI professionals in AI & cybersecurity- Onboard 100+ PSI agencies to CAPSI Connect- Develop National Tech Adoption & Surveillance Standards for PSI- Launch Digital PSI Skilling Hub with NSDC- Integrate drones and AI tools in 10 city-wide guarding deployments
2027	Global Positioning	<ul style="list-style-type: none">- Export India-developed AI Guarding solutions to 5 countries- Global PSI Skilling Alliance with CAPSI as anchor- 1 lakh personnel digitally certified- Launch CAPSI International Research & Training Center- Represent India at global PSI-Tech summits (UK, Dubai, Singapore)

Key Milestones to Measure Progress

10.3 Target Outcomes by 2027

Outcome Area	Target 2027	Strategic Benefit
Employment	1 lakh digitally skilled PSI personnel	Future-proof PSI jobs, reduce attrition
Upskilling	AI/Cyber training for 50,000 security guards	Quality-of-service enhancement
Agency Readiness	1,000 PSI companies tech-ready	Industry-wide tech compliance
Policy Enablement	National PSI-Tech Code	Clear governance and legal framework
Exports	5 Indian PSI-Tech solutions exported	Global brand value for Indian PSI
Entrepreneurship	1000+ tech-savvy PSI entrepreneurs	Boost to MSMEs in security-tech sector

Targeted achievements by 2027

10.4 Strategic Programs in Roadmap

A. Digital Skilling & Smart Certification

- Partner with RRU, IITM Pravartak, CyberPeace Foundation
- Use a mix of MOOCs, live online classes, and hands-on simulators
- Three levels of certification: Digital Guard, Digital Supervisor, Tech-enabled Officer

B. AI & Cybersecurity Tech Adoption

- Promote adoption of drone patrolling, computer vision CCTV, AI command centers, and threat detection platforms
- Incentivize agencies that meet digital readiness benchmarks with CAPSI TechSeal

C. Platform & Portal Launches

- CAPSI Connect: A national app-based interface for field force coordination, reporting, certification, and training
- PSI Digital Registry: A government-accessible verified database of certified PSI professionals and agencies
- AI Surveillance Standards Repository: Managed by CAPSI in collaboration with CERT-IN

D. Global Partnerships

- Exchange programs with UK SIA, US DHS, Israeli Security Startups
- Invite UN, ILO, and other bodies to certify Indian skilling models
- Collaboration with NASSCOM and DRDO for indigenous tech adoption

10.5 KPIs to Measure Impact

To ensure accountability and continuous improvement, a detailed KPI framework will be tracked annually:

Category	KPI	Target by 2027
Skilling	No. of certified guards, officers	1,00,000 personnel
Tech Integration	AI/Cyber tools deployed by PSI firms	1000+ firms
Agency Tech Rating	PSI Tech Readiness Scorecard adoption	5000 agencies
Employment	New jobs through AI/Cyber skilling	2,00,000 incremental
Export Readiness	Indian PSI-Tech products exported	5+ countries
Platform Adoption	CAPSI Connect app users	1 million users
Women Empowerment	Women trained in AI-based PSI roles	25,000 trained women
Ecosystem Development	Active partnerships with academia, industry	100 MoUs signed

Proposed KPIs to be tracked

10.6 Risk Mitigation & Success Factors

Risks

- Resistance to change among traditional PSI employers
- Data privacy concerns with increased surveillance
- Cyber threats to AI-driven platforms
- Fragmented implementation due to regional disparities

Mitigation Strategies

- Regional training hubs with language support
- Strong data governance via DPDP Act compliance
- Incident Response Teams and cyber awareness sessions
- Centralized monitoring through CAPSI Tech Council

10.7 CAPSI's AI Task Force: Driving Technological Transformation

In January 2025, the Central Association of Private Security Industry (CAPSI) established a national task force focused on integrating Artificial Intelligence (AI) into the private security sector. Led by Srinivas Mahankali, an expert in digital transformation technologies, this task force aims to modernize India's private security ecosystem by leveraging AI to address critical challenges such as rising security threats, operational inefficiencies, and the urgent need for upskilling personnel.

Key Objectives:

- Identify potential AI applications for security systems within 60 days.
- Pilot AI-driven surveillance and threat detection in key areas over the next six months.
- Draft ethical guidelines for AI integration within 90 days.
- Train 500 security personnel on AI tools within a year.

This initiative envisions significant advancements in security operations, including predictive analytics, biometric authentication, and intelligent surveillance systems. The integration of large-scale networks of IoT devices, drones, and CCTV systems is set to redefine India's private security landscape.

10.8 Launch of Nari Rakshak Teams (NRT) & Women Safety App

On March 7, 2025, during the International Women's Day celebrations, CAPSI, in collaboration with ASIS International, New Delhi, launched the Nari Rakshak Teams (NRT) and a dedicated Women Safety App. Developed under the leadership of Wg. Cdr. Sonika Tanwar (Retd), the app is designed to enhance women's safety and security. The launch event included a live demonstration showcasing its features and functionality, emphasizing CAPSI's commitment to women's safety and empowerment in the security sector.

10.9 Training 2 Lakh Drone Warriors

In a significant move to harness drone technology for improved surveillance and security operations, CAPSI announced a comprehensive training program to develop 2 lakh Drone Warriors from the private security sector. This initiative aligns with the training standards and parameters set by the Directorate General of Civil Aviation (DGCA) and underscores CAPSI's commitment to equipping security personnel with essential skills to operate drones effectively, ensuring a high standard of safety and security across various environments.

10.10 Government Support for Digital Growth and AI Adoption

The Union Budget 2025, presented by Finance Minister Nirmala Sitharaman, outlines a roadmap to bolster India's digital ecosystem, strengthen cybersecurity frameworks, and accelerate the adoption of emerging technologies like AI. These announcements signal the government's continued focus on leveraging technology for governance, economic growth, and skill development, while addressing gaps in digital access and data security.

10.11 Enhancing Cybersecurity Resilience

India's cybersecurity landscape in 2025 emphasizes the need for ongoing adaptation and vigilance due to the growing sophistication of cyber attacks. By boosting international collaboration, developing domestic cybersecurity solutions, and investing in AI-driven threat identification, India aims to create a more secure digital ecosystem. The resilience in the digital age will depend on the capacity to maintain an advantage in the cybersecurity domain as threats continue to evolve.

10.12 Conclusion

CAPSI's strategic initiatives from 2025 to 2027 reflect a comprehensive approach to transforming India's private security industry through technological integration, skill development, and collaborative efforts. By focusing on AI adoption, women's safety, drone technology, and cybersecurity resilience, CAPSI aims to position India as a global leader in tech-enabled private security services.

India has a rare opportunity to leapfrog into global leadership in AI-driven, cyber-aware private security services. With the right roadmap, strategic partnerships, and sustained investment, the Indian PSI can evolve from a manpower-intensive industry to a knowledge, skill, and technology-driven national asset.

This roadmap outlines where we need to go, how to get there, and how to measure progress. CAPSI is committed to driving this transformation as a national priority.

Glossary of Tech Terms

Artificial Intelligence (AI): The simulation of human intelligence by machines, particularly useful in tasks such as facial recognition, video surveillance analysis, and automated decision-making for security operations.

Machine Learning (ML): A subfield of AI where systems learn from data and improve their performance over time without being explicitly programmed. It is widely used in predictive security analytics and behavior analysis.

Zero Trust Architecture: A cybersecurity framework that assumes no entity inside or outside the network is inherently trusted. Every access request is verified, making it highly effective for preventing breaches in distributed and mobile security environments.

Internet of Things (IoT): A network of interconnected physical devices embedded with sensors and software, enabling them to collect and exchange data. In the Private Security Industry (PSI), IoT enables smart surveillance, environmental monitoring, and access control.

Drones (Unmanned Aerial Vehicles - UAVs): Aircraft systems without human pilots onboard, increasingly used in guarding services for perimeter surveillance, event monitoring, and emergency response due to their mobility and aerial vantage.

Computer Vision: A field of AI that enables machines to interpret and understand visual information from the world, such as CCTV footage or license plate recognition. It is key to automating surveillance and threat detection in real time.

Cybersecurity: The practice of protecting networks, systems, and programs from digital attacks. For PSI, it ensures that security infrastructure, digital tools, and sensitive client data remain secure and uncompromised.

Threat Detection: The process of identifying potential or actual cyber threats using automated tools, real-time monitoring, and AI. It is essential to prevent unauthorized access, data breaches, and operational disruptions.

Incident Response: A structured approach to managing and mitigating the aftermath of a cybersecurity breach or incident. It ensures rapid containment, investigation, and recovery to reduce damage and downtime.

Digital Twin: A virtual representation of a physical object, process, or environment. In PSI, it can simulate a facility for risk assessments, training, and predictive threat modeling.

Edge Computing: A technology paradigm where data processing occurs at or near the source of data generation, rather than in centralized data centers. It improves response time for critical applications like smart surveillance.

Public-Private Partnership (PPP): A collaborative model where government bodies and private sector organizations work together to deliver services or infrastructure. In PSI, PPPs are vital for co-developing and scaling training programs, technology pilots, and certification systems.

Annexure 2: Stakeholders Consulted

List of Stakeholders Consulted

The whitepaper preparation involved extensive dialogue with key stakeholders across government, academia, and private industry, including:

1. **Central Association of Private Security Industry (CAPSI)**
 - Chairman: **Kunwar Vikram Singh, Chairman, CAPSI**
 - Task Force Head: **Mr. Srinivas Mahankali**, Digital Transformation & Cybersecurity Expert
2. **Government Agencies & Bodies**
 - Ministry of Home Affairs (MHA)
 - Ministry of Electronics and Information Technology (MeitY)
 - Rashtriya Raksha University (RRU)
 - Skill India Mission
3. **Academic and Research Institutions**
 - **IIT Madras Pravartak Foundation** – Curriculum Development Partner
 - **CyberPeace Foundation** – Cybersecurity Awareness & Digital Safety
 - **NASSCOM FutureSkills Prime** – Reference for skill standardization
4. **Technology Companies & Startups**
 - AI solution providers (facial recognition, predictive analytics)
 - Drone service firms
 - Cloud platform vendors
 - Cybersecurity tool vendors (zero trust, endpoint protection)
5. **Private Security Agencies**
 - Guarding companies
 - Facility management companies
 - Event security and response teams
6. **Law Enforcement and Defence Representatives**
 - Retired officers from Police, CRPF, and Intelligence Bureau
 - Defence consultants on drone warfare and surveillance technologies

Annexure 3: CAPSI Initiated Training Programs

CAPSI has actively partnered with several organizations to roll out targeted skill development and pilot initiatives:

1. **CAPSI–IIT Madras Pravartak Advanced Training Program**
 - Focus: AI & Cybersecurity for Security Professionals
 - Duration: 12-week hybrid format
 - Modules: Drone surveillance, zero trust cybersecurity, computer vision
2. **CyberPeace–CAPSI Cybersecurity Awareness Modules**
 - Format: Online + Classroom sessions
 - Audience: 10,000+ frontline security guards across India
 - Themes: Digital hygiene, social engineering, phishing prevention

3. **Drone Warriors Program**
 - Objective: Train 2 lakh private security guards in certified drone operation
 - Collaboration with DGCA and drone startups
 - Training Partner: Security Sector Skill Development Council (SSSDC)
4. **Women Safety Initiative**
 - App Launch: **Nari Rakshak Teams (NRT)**
 - Safety App for SOS alerts, location tracking, quick response
 - Event Partner: ASIS International, New Delhi Chapter
5. **CAPSI Connect – Digital Community Platform**
 - App & Portal for members
 - Features: Learning modules, updates, collaboration, reporting system
6. **MoUs Signed (2024–2025)**
 - IIT Madras Pravartak (Curriculum Development)
 - CyberPeace Foundation (Cyber Literacy)
 - Leading Drone Training Academies (Skill India certified)
 - NASSCOM (For alignment of curriculum with FutureSkills Prime)

CAPSI Governing Council

1. **Kunwar Vikram Singh** - Chairman
2. **Sh. Mahesh C Sharma** - Secretary General
3. **Sh. Vishwanath V Katti** - National President
4. **Sh. C Pal Singh** - National Honorary Director General
5. **Sh. Vikram Mahurkar** - National Vice Chairman
6. **Sh. Anil Puri** - National Vice President
7. **Sh. Capt. V.P. Singh (Retd.)** - National Vice President
8. **Sh. Sudhir Bhasin** - National Vice President
9. **Sh. Sanjeev Paul** - National Vice President
10. **Dr. Raj Kumar Tyagi** - National Vice President
11. **Col. Sanjeev Kaul** - National Joint Secretary
12. **Capt. Ashok Kutty** - National Secretary
13. **Sh. R. Srinivasan** - National Secretary
14. **Sh. Gurdeep Singh Arora** - National Secretary
15. **Sh. Vipin Oberoi** - National Secretary
16. **Sh. Venu SR Pariat** - National Secretary & North East Incharge
17. **Sh. Ajit Singh** – Treasurer
18. **Maj. Prashant Rai** - National Secretary
19. **Capt. Nalini Ray** – Regional Vice President
20. **Sh. Manjeet Cheema** - Regional Vice President

Board of Governors & CAPSI Advisors

1. **Lt. Gen. Rajinder Singh (Retd.)** - Former Director General of Infantry
2. **Sh. M. L. Kumawat, IPS (Retd.)** - Former Director General-BSF; Former Vice Chancellor for SPUP
3. **Lt Gen AB Shivane (R)** – Former DG-Mechanical Forces, Indian Army; Strategic Advisor to the Chairman, CAPSI
4. **Lt. Gen. Shokin Chauhan (Retd.)** - PVSM, AVSM, YSM, SM, VSM Former DG Assam Rifles
5. **Sh. Anil Pratham IPS (R)** - Former DG of Police, Gujarat, Advisor, CAPSI
6. **Sh. C Pal Singh** - Former IG Police (Punjab)
7. **Dr. Keshav Kumar IPS (R)** - Former DG of Police, Gujarat
8. **Sh. B.S Sial, IPS (Retd.)** - Former DG Police, Karnataka
9. **Sh. Bhagwan Shankar, IAS (R)** - Advisor, CAPSI
10. **Maj. Gen. Narpat Singh Rajpurohit**, VSM Army veteran
11. **Sh. Pawanjit Singh Ahluwalia** - Chairman & Managing Director, Premier Shield Pvt. Ltd.
12. **Sh. B. R Lohia** - Chairman & Managing Director, Eagle Hunters Solution Ltd.
13. **Sh. Rupal Sinha** - Global President, BVG India Ltd.
14. **Sh. Praveer Bagchi** - Former Chairman to Ex - Prime Minister's & Follow-up Action Programme; Ex-Advisor, IBM (India & South Asia)

AI & Cyber Task Force Team

1. **Shri Srinivas Mahankali**
2. **Prof. (Dr) Surabhi Pandey**
3. **Shri Lalit Kalra**
4. **Shri Bimal Puri**
5. **Shri Anil Puri**
6. **Col Rahul Chauhan**
7. **Ms Vrinda Kapoor**
8. **Shri Baljeet Malhotra**
9. **Lt Cdr Satyabir Singh**
10. **Shri Abhijit Gudikandula**
11. **Ms Malathy Singh**
12. **Shri Anuj Nigam**
13. **Ms Shobha Ramesh**
14. **Ms Shalini Verma**
15. **Shri Harun -ul -Rashhed Shaik**
16. **Maj Vineet Kumar**
17. **Ms Antara Jha**
18. **Mr Saravana Malaichami**
19. **Maj Sadhna Singh**

This whitepaper, "Guarding the Future: AI & Cybersecurity in India's Private Security Revolution,"

Explores the transformative role of Artificial Intelligence (AI), Cybersecurity in reshaping the Private Security Industry (PSI) in India. With over 10 million security personnel, the industry stands at a pivotal juncture, requiring urgent modernization to address rising physical and digital threats. The document analyses global trends, case studies from countries like Singapore, Israel, and the US, and maps a clear strategy for India's security ecosystem. It outlines actionable steps for capacity building, digital skilling, and policy alignment, while highlighting CAPSI's pivotal role in leading this transition. From community platform launches and AI- powered training to collaborative initiatives with premier institutions like IIT Madras and CyberPeace Foundation, offering a blueprint for a secure, intelligent, and future-ready security infrastructure in India.

The CAPSI AI Task Force drives innovation by integrating AI, Cybersecurity, and emerging technologies to modernize and future-proof India's Private Security ecosystem.

CENTRAL ASSOCIATION OF PRIVATE SECURITY INDUSTRY

276, Sultan Sadan, Lane No.-3, West End Marg, Saidullajab,
New Delhi -110030, India

Tel :- +91 11 40820070

Email: info@capsi.in, Web :- www.capsi.in