Future of Defence: AI-Driven Surveillance and Digital Security Solutions

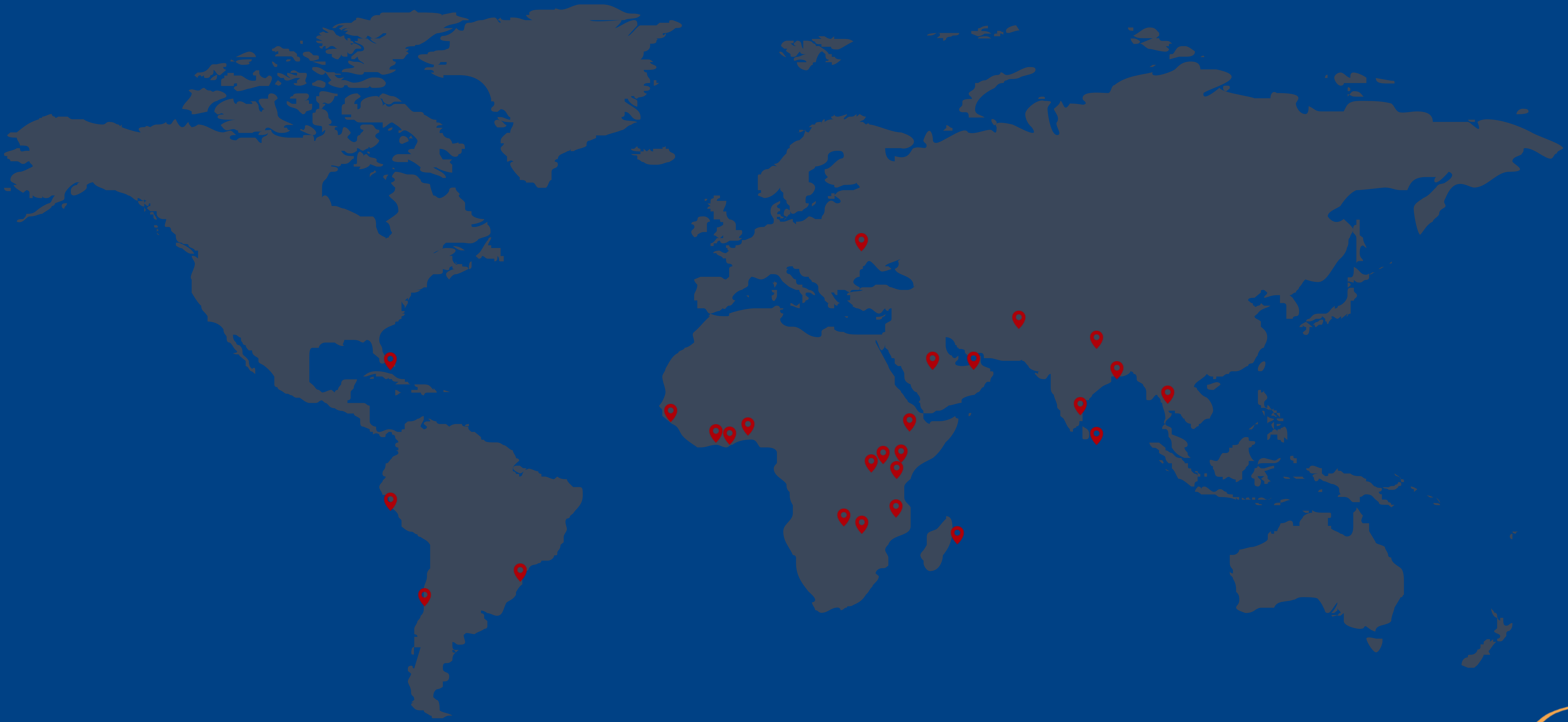
Solutions for Enhanced Defence with Integrated Command and control centers and Emerging Technologies

MSP MADRAS SECURITY PRINTERS

ABOUT MSP

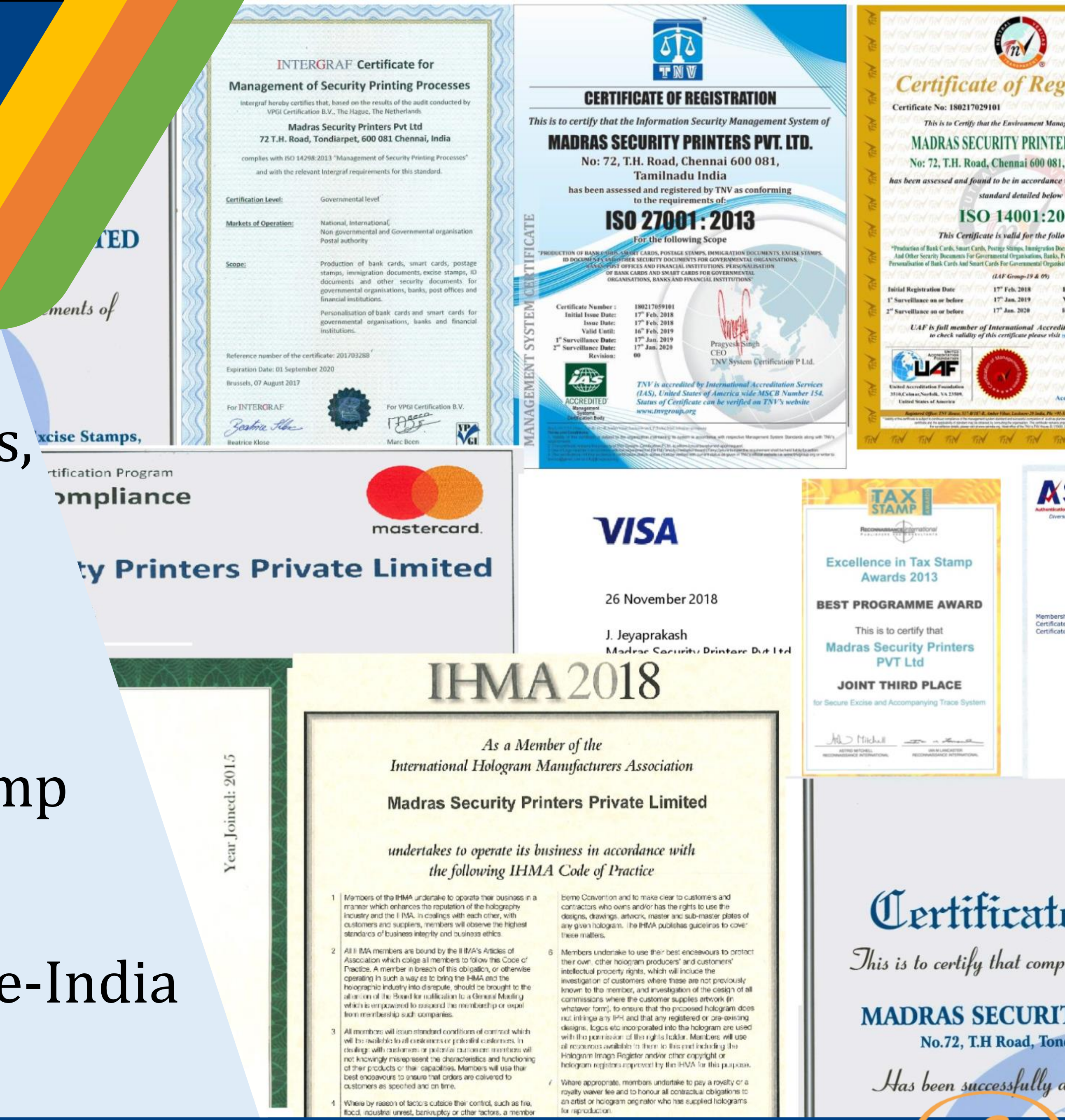
- Founded in 1976, Headquartered in Chennai and located PAN India
- Four Decades of experience in e-Governance, System Integration and other related products.
- Pioneer in establishing Data centers and Command & Control Centers
- MSP is certified to multiple ISO Standards & CMMI level 5
- 1000+ staff members, >200 in R&D

Presence Across Globe



Certificates & Awards

- Certified to various ISO standards, ISO 9001, ISO 20000, ISO 27001, CMMI Level5, RuPay, VISA & MASTERCARD
- Member of International Tax Stamp Association, ICMA, IHMA & ASPA
- Awarded by Tax Stamp Forum & e-India



TED

ments of

xcise Stamps,

INTERGRAF Certificate for
Management of Security Printing Processes

Intergraf hereby certifies that, based on the results of the audit conducted by VPGI Certification B.V., The Hague, The Netherlands

Madras Security Printers Pvt Ltd
72 T.H. Road, Tondiarpet, 600 081 Chennai, India

complies with ISO 14298:2013 "Management of Security Printing Processes" and with the relevant Intergraf requirements for this standard.

Certification Level:	Governmental level
Markets of Operation:	National, International, Non governmental and Governmental organisation Postal authority
Scope:	Production of bank cards, smart cards, postage stamps, immigration documents, excise stamps, ID documents and other security documents for governmental organisations, banks, post offices and financial institutions. Personalisation of bank cards and smart cards for governmental organisations, banks and financial institutions.

Reference number of the certificate: 201703288

Expiration Date: 01 September 2020

Brussels, 07 August 2017

For INTERGRAF
Beatrice Klose

For VPGI Certification B.V.
Marc Been

TNV

CERTIFICATE OF REGISTRATION

MANAGEMENT SYSTEM CERTIFICATE

This is to certify that the Information Security Management System of

MADRAS SECURITY PRINTERS PVT. LTD.
No: 72, T.H. Road, Chennai 600 081,
Tamilnadu India

has been assessed and registered by TNV as conforming to the requirements of:

ISO 27001 : 2013

For the following Scope

"PRODUCTION OF BANK CARDS, SMART CARDS, POSTAGE STAMPS, IMMIGRATION DOCUMENTS, EXCISE STAMPS, ID DOCUMENTS AND OTHER SECURITY DOCUMENTS FOR GOVERNMENTAL ORGANISATIONS, BANKS, POST OFFICES AND FINANCIAL INSTITUTIONS. PERSONALISATION OF BANK CARDS AND SMART CARDS FOR GOVERNMENTAL ORGANISATIONS, BANKS AND FINANCIAL INSTITUTIONS"

Certificate Number :	180217059101
Initial Issue Date:	17th Feb. 2018
Issue Date:	17th Feb. 2018
Valid Until:	16th Feb. 2019
1st Surveillance Date:	17th Jan. 2019
2nd Surveillance Date:	17th Jan. 2020
Revision:	00

Pragyesh Singh
CEO
TNV System Certification P Ltd.

IAS ACCREDITED
Management Systems Certification Body

TNV is accredited by International Accreditation Services (IAS), United States of America wide MSCB Number 154. Status of Certificate can be verified on TNV's website www.tnvgroup.org

Certificate of Reg

Certificate No: 180217029101

This is to Certify that the Environment Mana

MADRAS SECURITY PRINTE
No: 72, T.H. Road, Chennai 600 081,

has been assessed and found to be in accordance
standard detailed below

ISO 14001:20

This Certificate is valid for the follo

"Production of Bank Cards, Smart Cards, Postage Stamps, Immigration Doc
And Other Security Documents For Governmental Organisations, Banks, P
Personalisation of Bank Cards And Smart Cards For Governmental Organisa

(IAF Group-19 & 09)

Initial Registration Date	17th Feb. 2018
1st Surveillance on or before	17th Jan. 2019
2nd Surveillance on or before	17th Jan. 2020

UAF is full member of International Accredit
to check validity of this certificate please visit

UAF United Accreditation Foundation
United Accreditation Foundation
3510,Colmar,Norfolk, VA 23509,
United States of America

Registered Office: TNV House, 517-B/187-B, Amber Vihar, Lucknow-29 India, Ph: +91-

rtification Program
ompliance

mastercard.

ty Printers Private Limited

VISA

26 November 2018

J. Jeyaprakash
Madras Security Printers Pvt Ltd

TAX STAMP

Reconnaissance International

Excellence in Tax Stamp Awards 2013

BEST PROGRAMME AWARD

This is to certify that
Madras Security Printers PVT Ltd

JOINT THIRD PLACE

for Secure Excise and Accompanying Trace System

ASTRID MITCHELL
RECONNAISSANCE INTERNATIONAL

IAN M LANCASTER
RECONNAISSANCE INTERNATIONAL

AS
Authentication
Divers

Membersh
Certificate
Certificate

Year Joined: 2015

IHMA 2018

As a Member of the
International Hologram Manufacturers Association

Madras Security Printers Private Limited

undertakes to operate its business in accordance with the following IHMA Code of Practice

1 Members of the IHMA undertake to operate their business in a manner which enhances the reputation of the holography industry and the IHMA. In dealings with each other, with customers and suppliers, members will observe the highest standards of business integrity and business ethics.

2 All IHMA members are bound by the IHMA's Articles of Association which oblige all members to follow this Code of Practice. A member in breach of this obligation, or otherwise operating in such a way as to bring the IHMA and the holographic industry into disrepute, should be brought to the attention of the Board for notification to a General Meeting which is empowered to suspend the membership or expel from membership such companies.

3 All members will issue standard conditions of contract which will be available to all customers or potential customers. In dealings with customers or potential customers members will not knowingly misrepresent the characteristics and functioning of their products or their capabilities. Members will use their best endeavours to ensure that orders are delivered to customers as specified and on time.

4 Where by reason of factors outside their control, such as fire, flood, industrial unrest, bankruptcy or other factors, a member

Berne Convention and to make clear to customers and contractors who owns and/or has the rights to use the designs, drawings, artwork, master and sub-master plates of any given hologram. The IHMA publishes guidelines to cover these matters.

6 Members undertake to use their best endeavours to protect their own, other hologram producers' and customers' intellectual property rights, which will include the investigation of customers where these are not previously known to the member, and investigation of the design of all commissions where the customer supplies artwork (in whatever form), to ensure that the proposed hologram does not infringe any IPR and that any registered or pre-existing designs, logos etc incorporated into the hologram are used with the permission of the rights holder. Members will use all resources available to them to this end including the Hologram Image Register and/or other copyright or hologram registers approved by the IHMA for this purpose.

7 Where appropriate, members undertake to pay a royalty or a royalty waiver fee and to honour all contractual obligations to an artist or hologram originator who has supplied holograms for reproduction.

Certificate
This is to certify that comp

MADRAS SECURI
No.72, T.H Road, Ton

Has been successfully

MSP

Why Choose MSP?

- A 48-year-old Company Specializing In Comprehensive E-governance Solutions.
- A Trailblazer In E-governance, With A Wealth Of Experience In Managing IT System Integration, Extensive Databases, And Delivering Solutions For Citizen-centric Projects.
- Comprehensive Secure IT Solutions provider for Government Departments, Public Sector Units (PSUs), And Large Enterprises.
- Turnkey solution providers for designing and Implementing various civil, active, passive components .
- Established command and control centers for various project.
- Holds Certifications In Multiple ISO Standards.

VALUE PROPOSITION

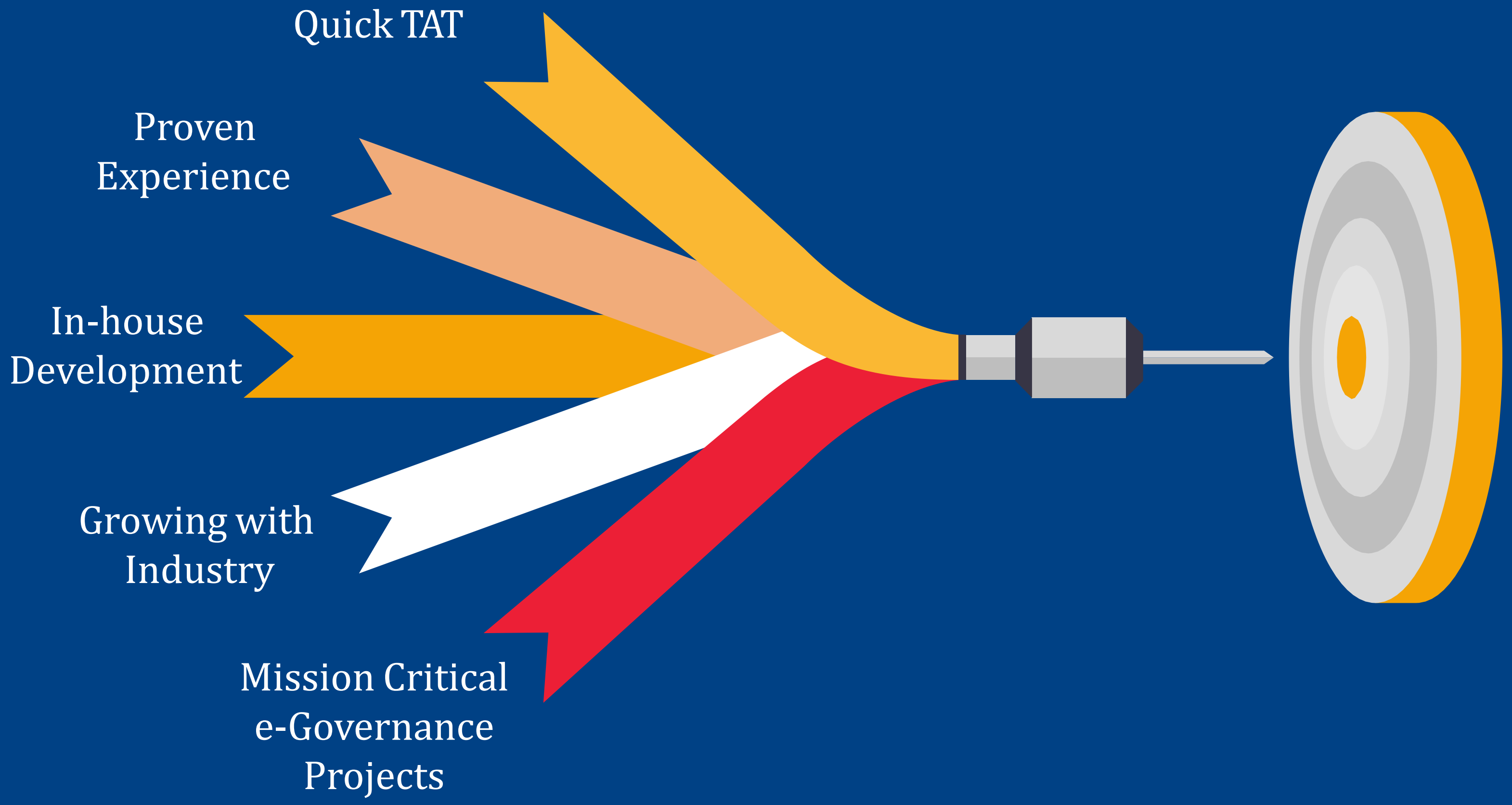
🟨 **Quick TAT**
Implemented projects in time

🟧 **Proven Experience**
Successfully implemented several projects across the Globe

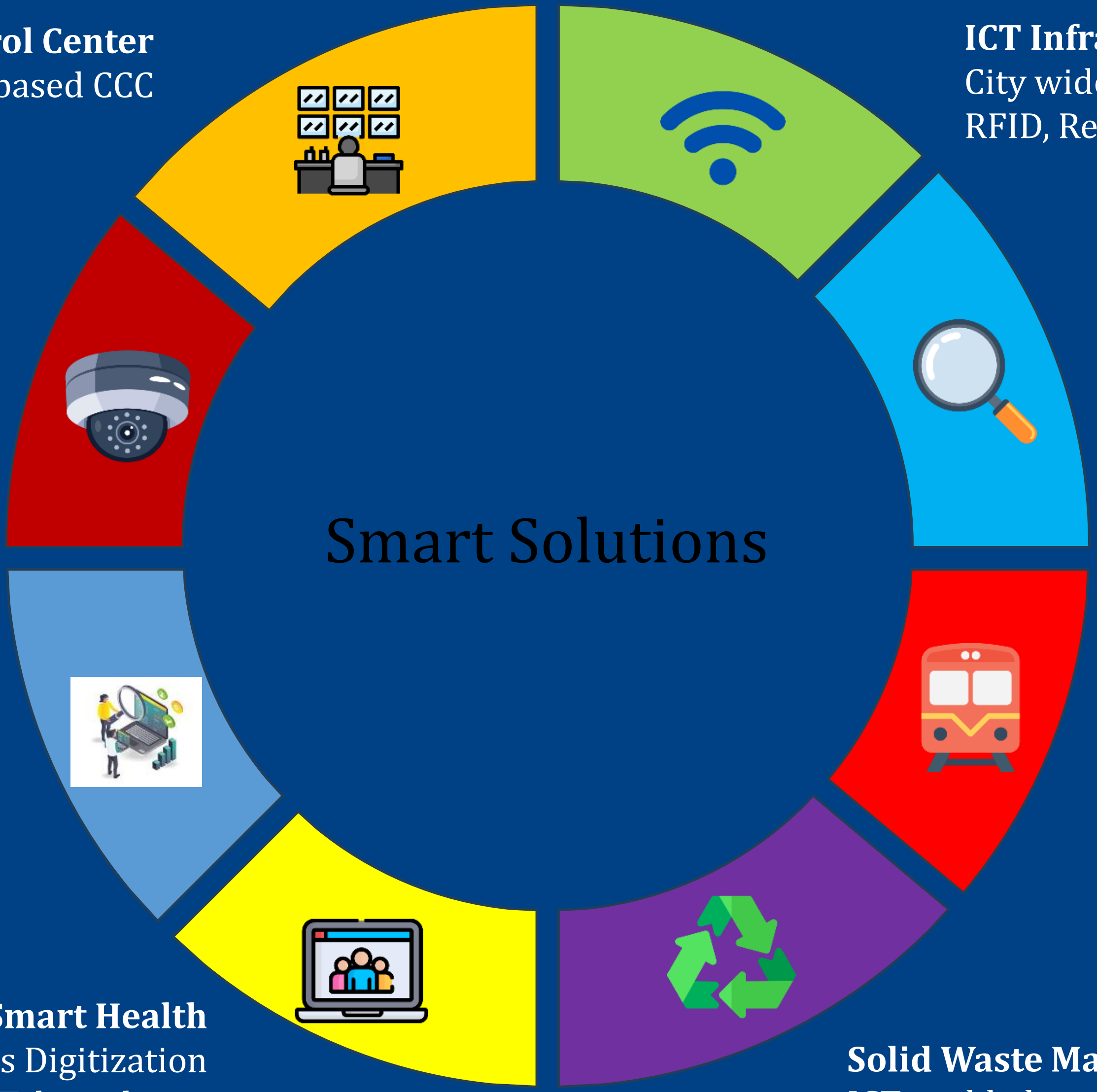
🟧 **In-house Development**
High Security Printing Plant and Software development under one roof

⬜ **Growing with Industry**
More than 4 decades in the industry, evolved with the industry

🟥 **Mission Critical e-Governance**
Involved in Mission Critical e-Governance Projects in India and Across Globe



MSP's SMART SOLUTIONS



Smart Solutions

Command & Control Center
AI based CCC

ICT Infrastructure
City wide OFC backbone
RFID, Readers, CCTV & Public Wi-Fi

Smart Surveillance Smart Cameras
Smart video analysis Smart Monitoring

Smart Track & Trace
QR Code Based Track and Trace System for Excise Department across the country for the various products

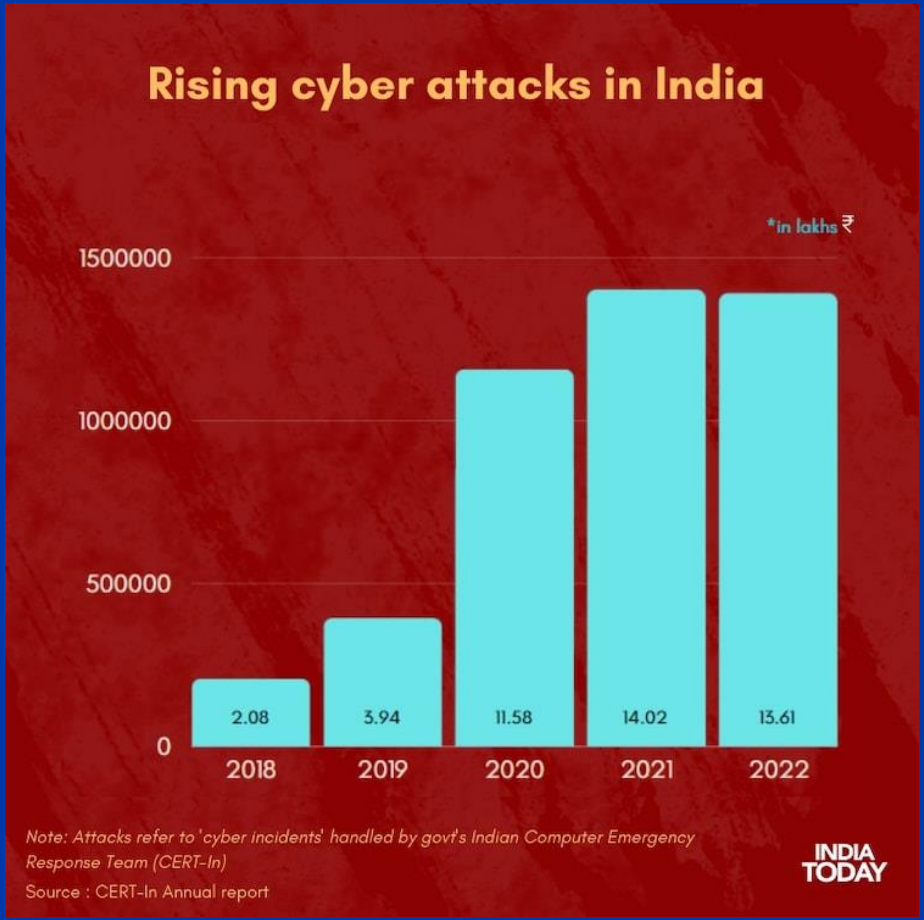
NOC and SOC solutions
Network Monitoring
Vulnerability Management

Smart Traffic Management
Adaptive traffic management Solar wireless traffic controllers

Smart Health
Health and wellness centers Digitization of medical records Telemedicine Access Electronic Card Emergency Services

Solid Waste Management
ICT enabled waste collection system Smart bins
Bio composting

Introduction to Surveillance and Cybersecurity in Defence



Rising cyber attacks in India

Note: Attacks refer to 'cyber incidents' handled by govt's Indian Computer Emergency Response Team (CERT-In)

Source : CERT-In Annual report

India's vulnerability to cyberattacks

India has witnessed a massive surge in cyberattacks in the last five years with the Home Ministry's National Cyber Crime Reporting Portal registering about **15 Lakhs complaints** this year. 85 per cent of the complaints related to online financial fraud.

Surveillance and cybersecurity are pivotal in mitigating threats such as

- ✓ Espionage
- ✓ Cyber warfare
- ✓ Terrorism in the digital age.

Data source:https://www.indiatoday.in/business/budget/story/budget-2024-cybersecurity-artificial-intelligence-projects

WHY IT MATTERS FOR NATIONAL DEFENCE?

Disruption of Critical Infrastructure

Military communication networks, command and control systems, and logistics.

Impact:

Paralysis of military operations during crises.

Disrupted supply chains for critical resources and ammunition.

The NotPetya cyberattack in 2017 crippled systems globally, including logistics companies vital for military operations.

Espionage and Data Theft

Classified defence data, including blueprints of weapons, strategies, and troop movements.

Impact:

Loss of strategic advantage over adversaries.

In 2022, Chinese hackers reportedly targeted Indian power grids near Ladakh, possibly to gather intelligence during border tensions.

Data source :https://visionias.in/current-affairs/monthly-magazine/2024-06-22/security/technology-absorption-in-defence

WHY IT MATTERS FOR NATIONAL DEFENCE?

Sabotage of Weapon Systems

Smart weapons, drones, missile defence systems, and naval fleets.

Impact:

Hacking into weapon systems could render them inoperable or redirect them.

Vulnerabilities in automated weapon systems like UAVs (drones) could allow adversaries to seize control during deployment.

Cyberattacks on Strategic Assets

Nuclear facilities, satellites, and space operations.

Impact:

- Breach in satellite communication could disable reconnaissance and surveillance systems.
- Sabotaging nuclear facilities could lead to national security disasters.

The Stuxnet virus, which targeted Iran's nuclear program, demonstrated how cyberattacks can cripple sensitive infrastructure.

Data source :https://visionias.in/current-affairs/monthly-magazine/2024-06-22/security/technology-absorption-in-defence

MSP

RECENT CYBERATTACKS

In 2024, **cyberattacks were increased by** 33% from 2023, Among which defence sector was the primary target.

May 2024: Other country hackers targeted India's government, aerospace, and defence sectors using phishing emails disguised as official defence communications which leads to compromise of sensitive data.

November 2022: **The ransomware attack on AIIMS** Delhi crippled operations for weeks. Although not directly a military attack, it exposed vulnerabilities in critical national systems, which can cascade to military dependencies.

Volt Typhoon Attack on U.S. Infrastructure (2024) other countries targeted U.S. critical infrastructure, including communications and energy, by hijacking small office/home office (SOHO) routers.

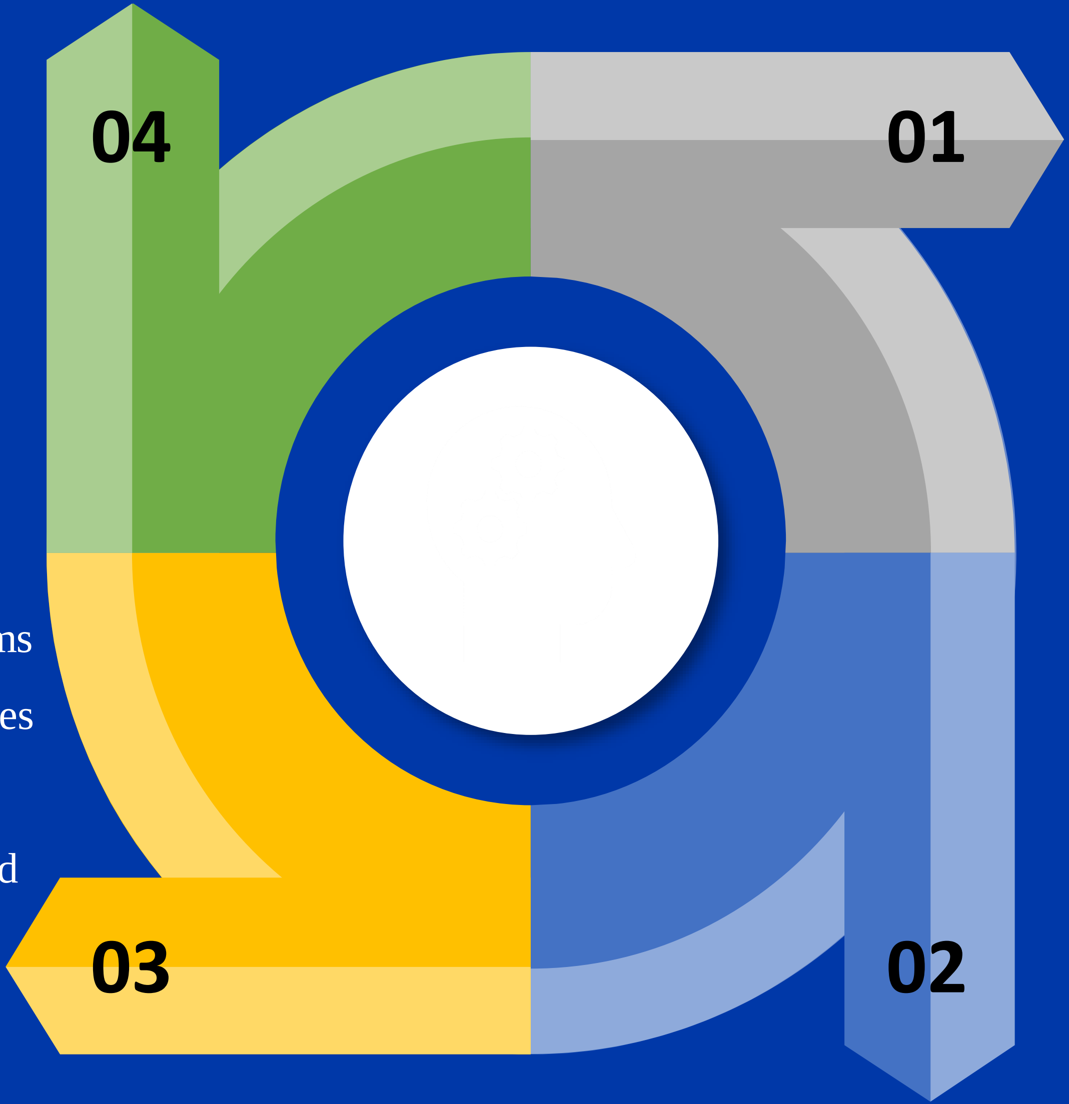
The recent **global disruption caused by a Microsoft Windows software** update glitch serves as a stark reminder of the vulnerabilities in our interconnected digital infrastructure.

Ongoing Threats: Other countries cyber-espionage activities have been linked to targeting India’s strategic assets and networks. In one instance, hackers compromised power grids to map vulnerabilities.

Data Source :

- ✓ *https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents*
- ✓ *https://www.crn.com/news/security/2024/10-major-cyberattacks-and-data-breaches-in-2024-so-far*
- ✓ *https://www.drishtiias.com/daily-updates/daily-news-editorials/strengthening-india-s-cyber-defence*

DIGITAL BATTLEFIELD



Modern warfare increasingly involves cyberattacks alongside traditional methods, affecting not just military but also civilian infrastructure.

Nations like China, the US, and Russia are investing heavily in cyberwarfare, creating an arms race in cyberspace.

In modern warfare scenarios, ICCC platforms equipped with robust surveillance capabilities offer strategic advantages by monitoring battlefields, tracking enemy movements, and preventing infiltration.

Cyberattacks can paralyze economies or undermine public confidence in government systems.

NEED FOR CYBERSECURITY SYSTEMS

Proactive Threat Detection

✓ Surveillance systems continuously monitor networks, endpoints, and physical environments for anomalies that may signal cyberattacks.

✓ Intrusion Detection Systems (IDS) analyze network traffic to detect unauthorized activities such as brute-force attacks or data exfiltration attempts.

Compliance with Regulations

✓ Many industries are governed by strict cybersecurity regulations (e.g., GDPR, HIPAA, PCI-DSS).

✓ SOCs ensure adherence to these standards by implementing the necessary security measures.

Incident Response and Recovery

✓ In case of a cyberattack, immediate response is critical to limit damage.

✓ SOCs provide expertise and tools to contain, investigate, and recover from security incidents by predictive analysis.

NEED FOR PHYSICAL SURVEILLANCE SYSTEMS

Incident Response and Forensics

- ✓ By integrating with physical surveillance measures, ICCCs can provide a unified security posture, addressing threats comprehensively.
- ✓ Surveillance records are critical in forensic investigations to trace the origin of cyber incidents.

Capturing real-time data

- ✓ Capturing real-time data allows security teams to quickly assess and mitigate breaches.
- ✓ Physical surveillance acts as a complementary measure to digital monitoring by identifying and mitigating suspicious activities in real time

Physical Security Integration:

✓Cyberattacks often have a physical component (e.g., insider threats or tampering with hardware). Surveillance cameras and sensors in secure areas provide an additional layer of defence.

✓Surveillance cameras and sensors in secure areas provide an additional layer of defence by deterring unauthorized access and detecting suspicious activities.

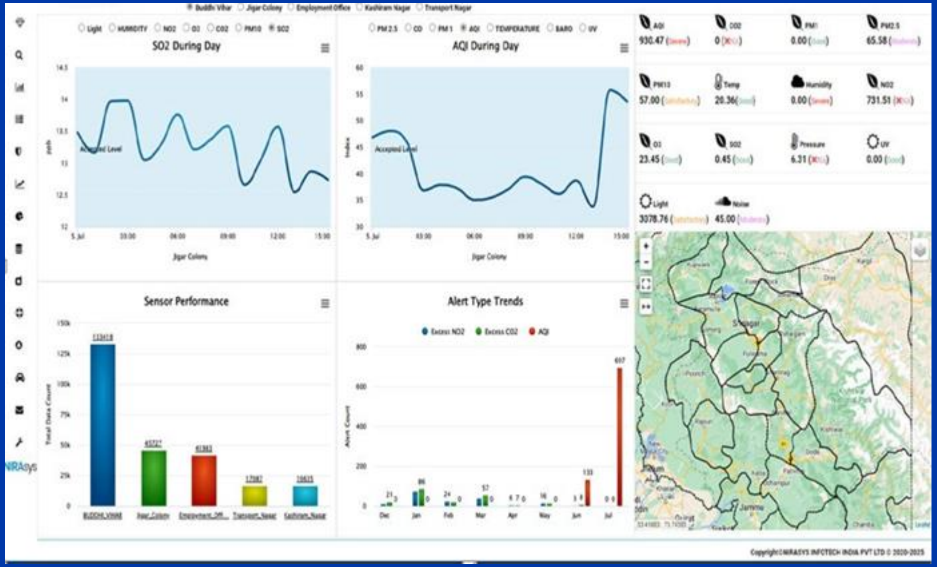
PHYSICAL SURVEILLANCE

Physical Surveillance can be strengthened with the help of Integrated Command and control Center (ICCC) by incorporating

- ✓ AI based Video Analytics
- ✓ Perimeter Surveillance
- ✓ Real-Time Monitoring and Analysis
- ✓ Facial Recognition and Biometrics

MSP

ICCC (Integrated Command and Control Centers)



- ✓ Acts as the nerve center, consolidating data from various sources (video feeds, IoT devices, sensors).
- ✓ Provides a unified dashboard for monitoring, analysis, and real-time decision-making.
- ✓ AI-driven anomaly detection and event prioritization.
- ✓ Seamless integration with legacy and modern surveillance systems

ICCC can be widely used for

Urban Surveillance: Monitoring public safety in smart cities.

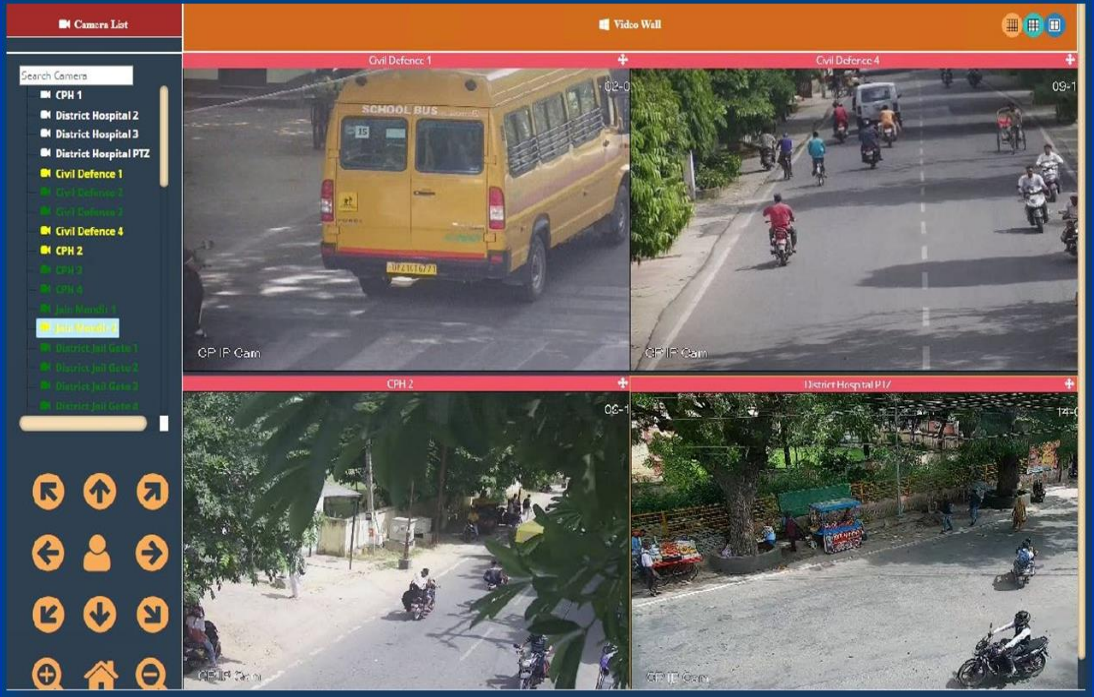
Military Operations:

- ✓ Monitoring and surveillance of designated zones
- ✓ Identifying and responding to the threats

This Reduces response time by **50%** in critical situations and Improves resource allocation through predictive analytics.

VIDEO ANALYTICS

IT Transforms passive video surveillance into proactive threat detection and uses AI to recognize patterns, objects, faces, and behaviors.



Key Capabilities:

- ✓ Behavior Analysis: Identifies unusual movement or loitering.
- ✓ Object Detection: Tracks weapons, drones, or suspicious packages.
- ✓ Facial Recognition: Matches individuals against watchlists.

This can be implemented in

- ✓ **Border Surveillance**: Identifying unauthorized crossings.
- ✓ **Crowd Management**: Detecting threats during large gatherings.

It majorly reduces reliance on human monitoring by **85% and** Increases threat detection accuracy to **95%.**

MULTI-LAYERED SECURITY APPROACH

Combining surveillance systems with emerging technologies of ICCC creates a **multi-layered security approach**

Physical surveillance solutions

Cybersecurity solutions

Multi Layered Security Approach

01

Integrated Dashboards

AI consolidates data from disparate systems into a single interface for faster threat assessment and decision-making

02

Cyber-Physical Correlation

AI can correlate cyber threats (e.g., phishing attempts) with potential physical intrusions (e.g., unauthorized personnel near data centers), offering a complete threat profile.

03

Machine Learning Models

AI-powered predictive models can identify potential vulnerabilities based on historical attack data and evolving threat patterns

04

Post-Attack Analysis:

AI can automate forensic investigations, identifying the root cause and suggesting system improvements to prevent future incidents.

OUR EXPERTISE

MSP

01 Our in-depth knowledge and experience in deploying and managing advanced cybersecurity and ICCC systems.

02 We ensure adherence to global standards such as ISO 27001, GDPR, NIST, and others, reducing compliance risks.

03 Our systems enable continuous surveillance and cybersecurity monitoring, minimizing downtime and mitigating risks.

04 With AI and advanced analytics, we can quickly identify threats and alert authorities before they escalate.

05 We provide actionable insights through regular reports and dashboards, empowering better strategic decisions.

SAFE-CITY PROJECT – CASE STUDY- CHENNAI

- MSP Established a Secure environment in public areas and work locations by installation of surveillance cameras powered by AI.

We have successfully Installed :

- **5250 CCTV Surveillance Cameras at**
- **1750 Key Locations**

- The servers and storage system of surveillance data and analysis is housed in the Data Centre.
- The key components of this projects include
  - ✓ Integrated Command and control center
  - ✓ Data center and Data Recovery Center
  - ✓ Cyber Forensic Lab
  - ✓ Security Operation Center

AI BASED - ANALYTICS AVAILABLE FOR SAFE CITY PROJECT
CASE STUDY - CHENNAI

- Camera Tamper
- Chain/Handbag Snatching
- Crowd Detection
- Vandalism Detection
- Intrusion Detection

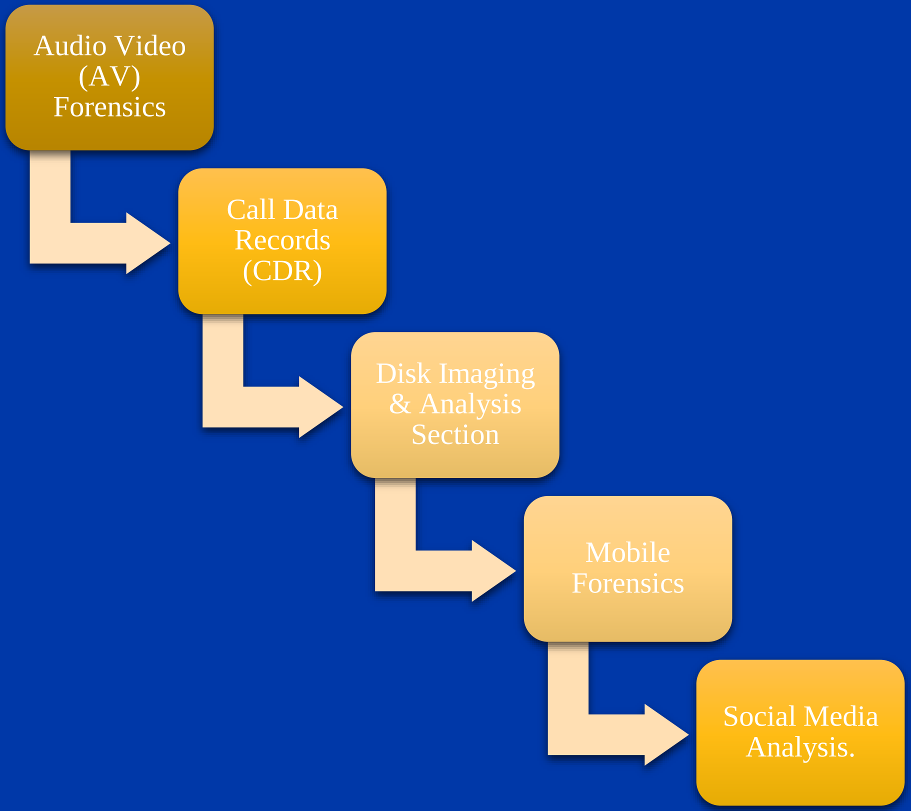
- Mobile Snatching
- Object Classification
- People Fighting
- Person Collapsing
- Strike/Hartal

- Suspected appearance
- Unattended Object
- Women Surrounded by Men
- Women/Infant Abduction
- Zone Monitoring

MSP

CYBER FORENSICS LAB

- ✓ Cyber Forensics Lab for investigating cyber crimes against women & other cyber crimes set-up at GCP HQ.
- ✓ A core team of police personnel formed who were already trained by System Integrator on Cyber Crime security certifications.
- ✓ CFL is equipped to handle



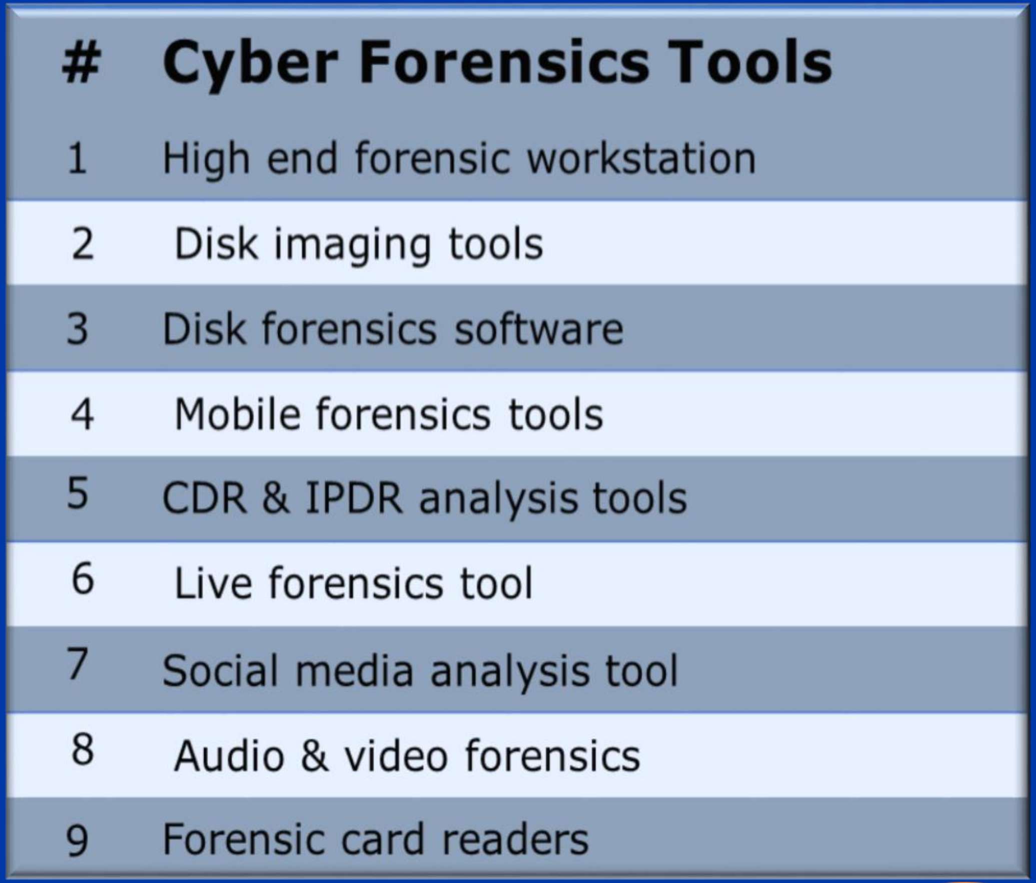
Audio Video (AV) Forensics

Call Data Records (CDR)

Disk Imaging & Analysis Section

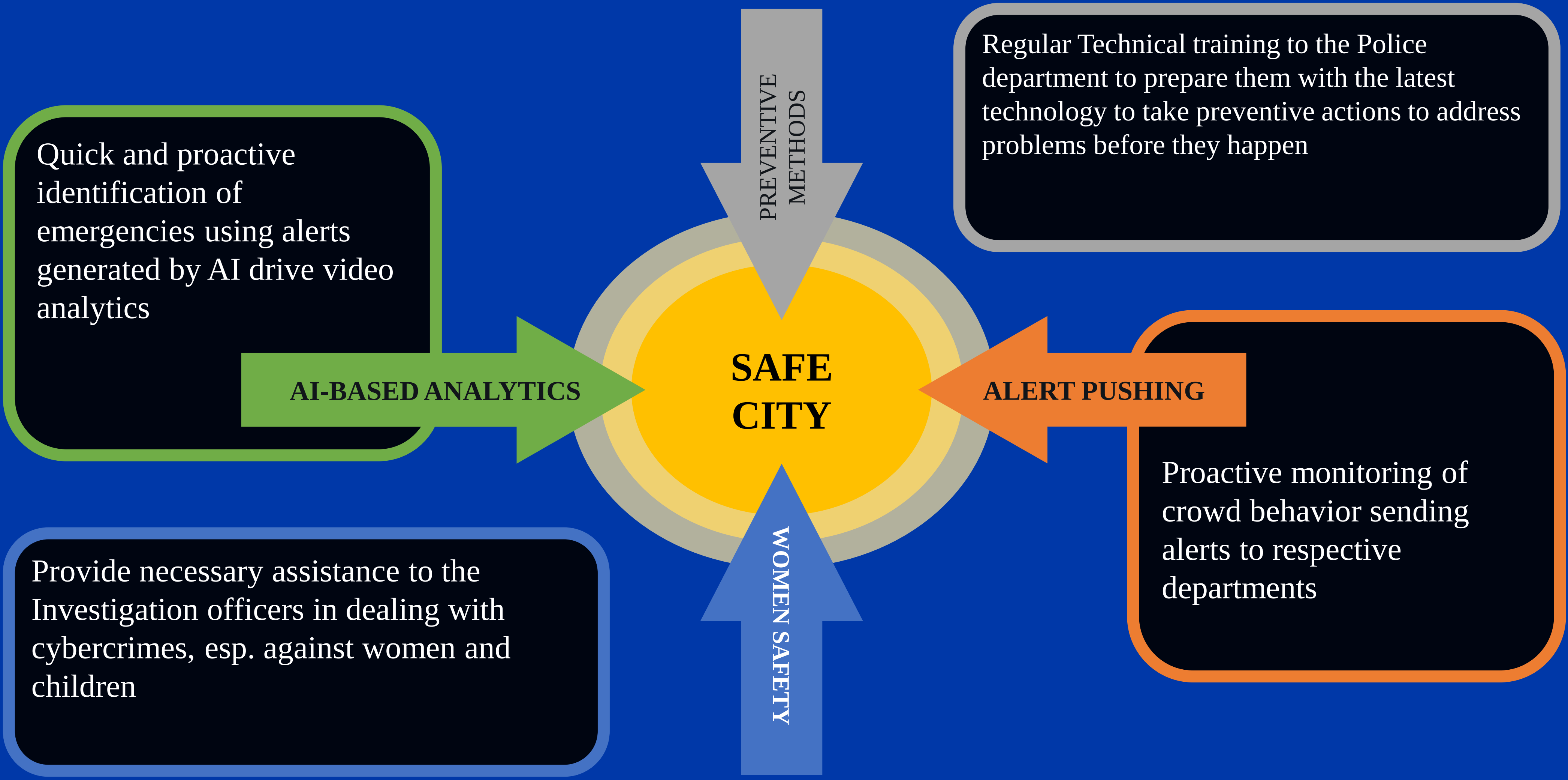
Mobile Forensics

Social Media Analysis.



#	Cyber Forensics Tools
1	High end forensic workstation
2	Disk imaging tools
3	Disk forensics software
4	Mobile forensics tools
5	CDR & IPDR analysis tools
6	Live forensics tool
7	Social media analysis tool
8	Audio & video forensics
9	Forensic card readers

KEY FEATURES



SAFE CITY

AI-BASED ANALYTICS

Quick and proactive identification of emergencies using alerts generated by AI drive video analytics

PREVENTIVE METHODS

Regular Technical training to the Police department to prepare them with the latest technology to take preventive actions to address problems before they happen

ALERT PUSHING

Proactive monitoring of crowd behavior sending alerts to respective departments

WOMEN SAFETY

Provide necessary assistance to the Investigation officers in dealing with cybercrimes, esp. against women and children

Contact Us

MSP SYSTEM INTEGRATION DIVISION

72, T.H. Road, Chennai – 600 081, Tamil Nadu, India
+91 44 2591 6086, +91 44 2591 5549

customerrelations@madrassecurityprinters.com

www.madrassecurityprinters.com