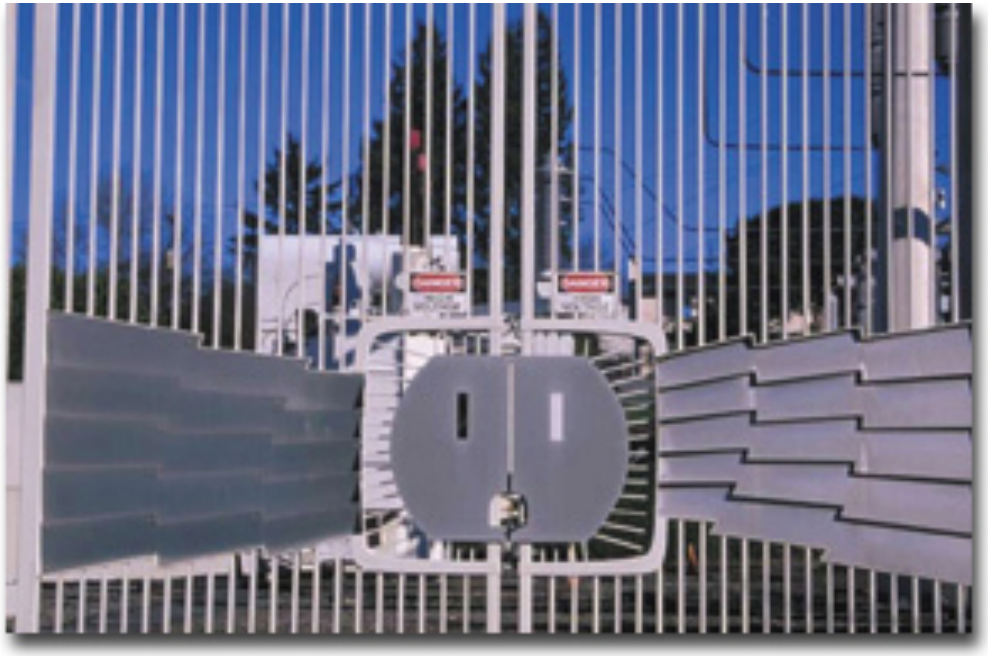
# Goals of Physical Security

1. Deter
2. Delay
3. Detect
4. Assess
5. Respond



Physical security technology is comprised of barriers, entry and search controls, intrusion detection, alarm assessment, and testing and maintenance

Systems along with organizational practices and procedures – respond to unauthorized activity

# Cyber crime case studies

Russian bank robbery:

Hackers steal £650 million in world's biggest bank raid.
Russian based hackers spent the last two years orchestrating the largest cybercrime ever uncovered.

As much as £650 million is thought to have gone missing after the gang used computer viruses to infect networks in more than 100 financial institutions worldwide.

Virus was injected from a computer within Bank network. Difficult to ascertain how hackers physically reached the bank network

# Russian bank robbery

How it happened?

The hackers managed to infiltrate the bank's internal computer systems (mostly by physical access thru social engineering) using malware, which lurked in the networks for months, gathering information and feeding it back to the gang.

The illegal software was so sophisticated that it allowed the criminals to view video feeds from within supposedly secure offices as they gathered the data they needed to steal.

# Mexico bank robbery

The cybercriminals began by gaining entry into an employee's computer through spear phishing, infecting the victim with a malware.

They were then able to jump into the internal network and track down administrators' computers for video surveillance. This allowed them to see and record everything that happened on the screens of staff who serviced the cash transfer systems.

# Mexico bank robbery

1) When the time came to cash in on their activities, the criminals used online banking or international e-payment systems to transfer money from the banks' accounts to their own. In the second case the stolen money was deposited with banks in China or the United States. The experts do not rule out the possibility that other banks in other countries were used as receivers.

2) In other cases cybercriminals penetrated right into the very heart of the accounting systems, inflating account balances before pocketing the extra funds via a fraudulent transaction. For example: if an account has $1,000, the criminals change its value so it has $10,000 and then transfer $9,000 to themselves. The account holder doesn't suspect a problem because the original $1,000 is still there.

# Mexico bank robbery

- These attacks again underline the fact that criminals will exploit any vulnerability in any system. It also highlights the fact that no sector can consider itself immune to attack and must constantly address their security procedures.

- Underlying importance of Watch on employees, zone restrictions, proper screening of every staff for unwanted use of USB drive etc…

- USB Killer video ...
- https://www.youtube.com/watch?v=pstHYmlZM9I

# Global bank robbery case

- The hackers were then able to get into the internal network and track down administrators' computers for video surveillance.
- Once the hackers become familiar with the banks' operations, they use that knowledge to steal money without raising suspicions, programming ATMs to dispense money at specific times or setting up fake accounts and transferring money into them.

ATM spits money

https://www.youtube.com/watch?v=XmRoyvBTbTc

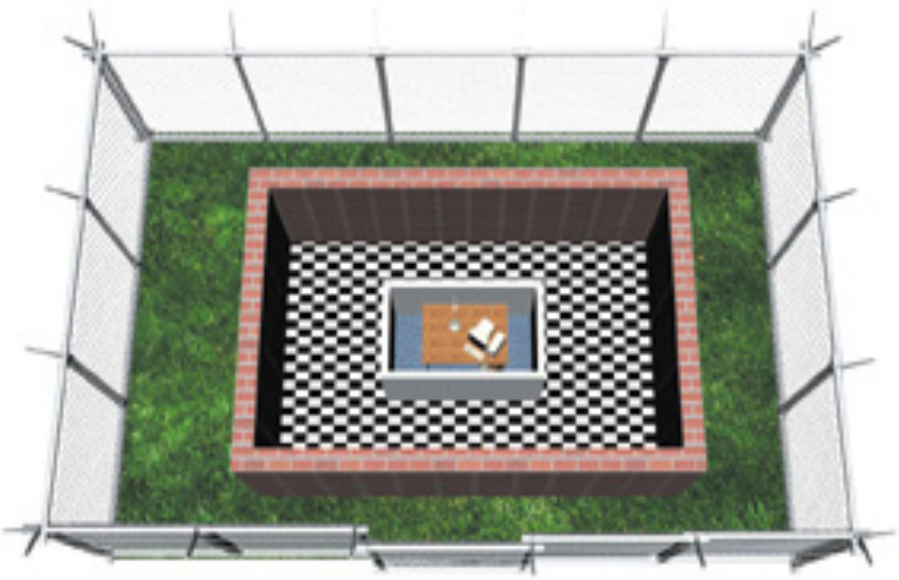
# Visuals on bank robbery hacking events

Here are some of the video links on the global bank robberies executed through breach in  the perimeter security & cyber security…..

Data center in Crosshairs
https://www.youtube.com/watch?v=WO9vzcsGTnM ,
Hackers steal millions – kaspersky view
https://www.youtube.com/watch?v=vQZjwOTGCFI ,
Watch this hacker break into a company
https://www.youtube.com/watch?v=PWVN3Rq4gzw
How Hackers get bank account details
https://www.youtube.com/watch?v=8EpbpLZgHHs ,
Detecting cyber attacks in Data centre
https://www.youtube.com/watch?v=9bOQayv77lc ,
Rapidly detect and prevent cyber attacks
https://www.youtube.com/watch?v=8mBgPCXLE3o ,

# Layered Defense Model Subtopics

- *Perimeter and Building Grounds*
- Building Entry Points
- Inside the Building -- Building Floors/Office Suites
- Data Centers or Server Room Security
- Computer Equipment Protection
- Object Protection



# Section Objectives

Understand the ‘layered’ approach to physical security, from the outside perimeter to the inside of the building

Describe boundary protection

List perimeter intrusion detection systems

Describe controls used inside the building

List the key controls for data center or server room security

https://www.youtube.com/watch?v=8g0NrHExD3g

# Centralised Security Operations Centre of an enterprise

**Perimeter Monitoring Solutions**
- Geo-sensors based monitoring
- Microwave fencing
- RF based Intrusion Detection
- Video Motion Detection

**Video Analytics Solutions**
- FRS based Doors / Gate mgmt
- Visitor Management(Biometric)
- VIP / Blacklisted identification
- Video based Zone violation alert
- People count for ICE scenario

**IOT based sensors**
- 4-in-One sensor
- Wirelsss cameras
- Door open sensors
- Sirens/Smoke detector

**Remote feeds with Cyber security**
- Remote login / access using BVP as additional layer of security
- MOBIMASS T&A
- Fixed line BVP based roster admin
- Exception Management

ID Sensors, Camera and IOT sensors

Remote locations feeds and alerts

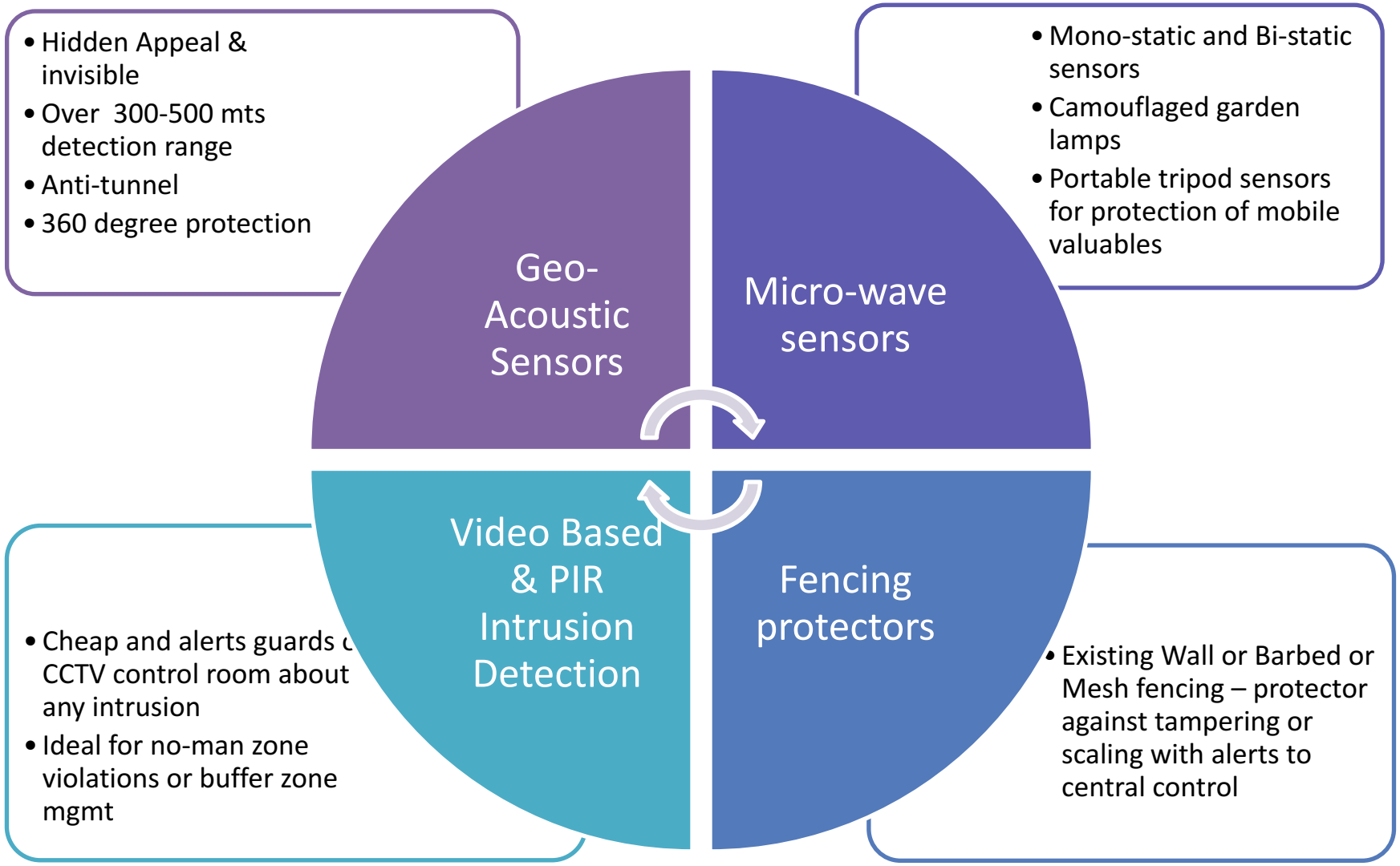
Physical Inspections & Visuals

Analytics, Alerts, Search & Forensics

**Physical + Visual Inspection**
- Beat / Patrol Minder
- UAV sorties with pictures
- RFID based Asset Tracking
- RFID based Vehicle entry / exit tracking

**Alerts + Analytics & Forensics Layer**
- Intelligent Video Search Application
- Trigger Alerts
- Analytics & Forensics (Cyber + Mobile tools)

# Perimeter Solutions Overview



Second Line of Protection

***Security At the building/Factory / Unit***

# People

Disgruntled employee / former employee

Moonlighter

Marketing, sales representatives, etc.

Purchasing agents, buyers, subcontract administrators

Consultants

Vendor/Subcontractor

Clerical

Applicants, Visitors, Customers

# Common device that can be Disastrous …

Mini and Micro Electronic devices

https://www.youtube.com/watch?v=l8YpTOv7Q2A (LAN Turtle)

https://www.youtube.com/watch?v=v723HK_qR-4 (Bash bunny)

USB drives

https://www.youtube.com/watch?v=sbKN8FhGnqg (rubber ducky)

External hard disks

Hidden cameras

Mobile phones with camera

Personal laptops / tablets

Intelligent espionage & leakage devices

Plug BOTs etc.

# Physical Security Checks

Normal Metal Detectors are not enough to detect micro-electronic threats

Detection of prohibited electronic devices (including voice recorders, mobile telephones, SIM-cards, digital memory devices), as well as firearms;

Detection of improvised explosive devices (IED electronic control systems) in hand luggage and on the “operator’s” body, in the complex technogenic interference from the city environment;

Detection of covert eavesdropping electronic devices

https://www.youtube.com/watch?v=5GnMj5cus4A

What all did you observe ?

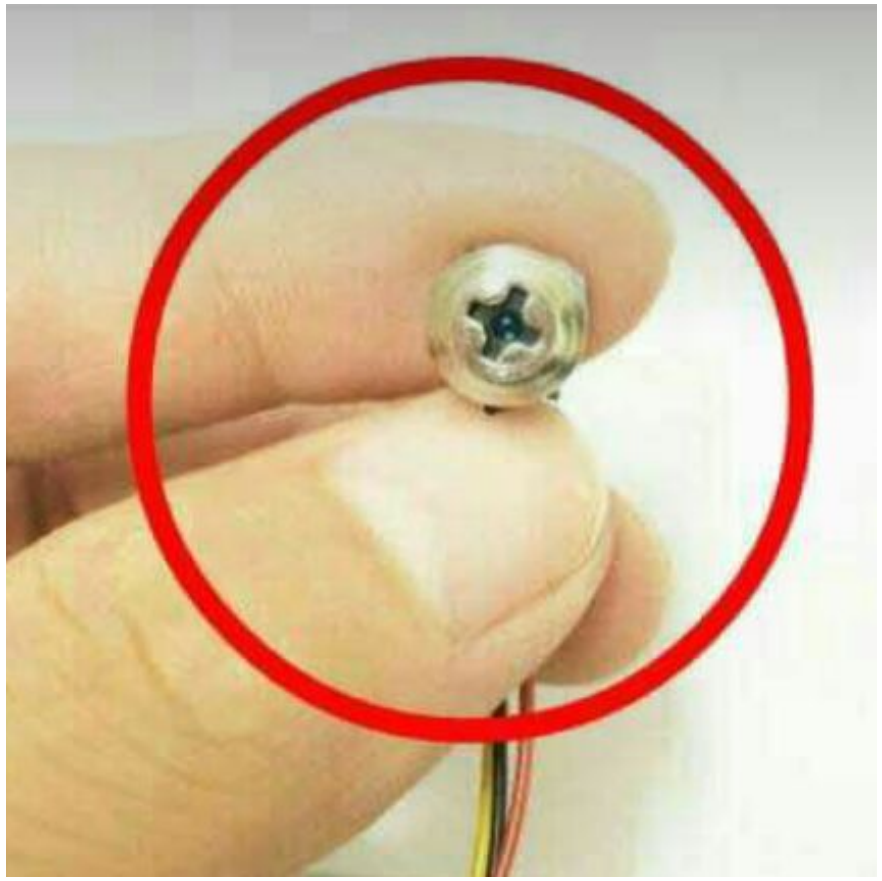
# Multifunction Detection Device

A new generation multifunction counter surveillance device, designed for detection and localization of all major types of eavesdropping devices.

**Detects**

- Radio microphones;
- Telephone transmitters;
- Radio-stethoscopes;
- Concealed video cameras equipped with a radio channel for transmission of information;
- Technical means or systems for spatial radio frequency radiation;
- Beacons of the systems used for moving objects monitoring (e.g. people, transportation means, goods etc.);
- Unauthorized radio stations, radio handsets, and also telephones with radio-extension;
- Radio modems and digital wireless access systems;
- Devices transmitting intercepted information by AC 220V mains lines and capable of operating at frequencies up to 30 MHz

# New types of threats are coming



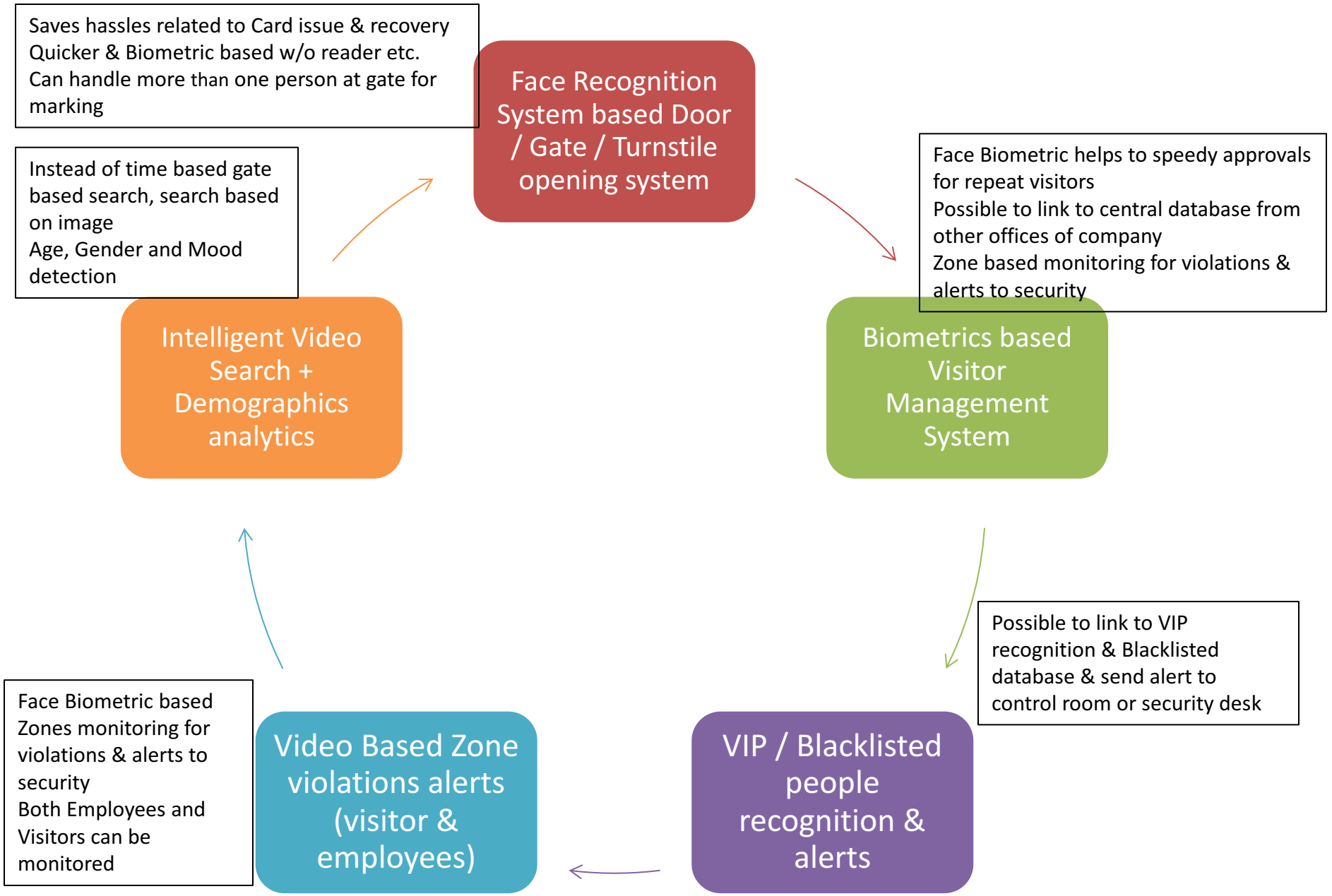
# Various Counter-Terrorism & Counter-Intelligence Devices

Cellular Jammer – small area / sterile zone protection

Cellular Signal Suppressor – used as means of protecting confidentiality durir negotiations by impeding the operation of mobile telephones and obstructing certain digital communications channels (Wi-Fi, Bluetooth, WiMax).


Hidden Camera Detector – using hand-held device to detect any type of lenses , pin-hole cameras etc.

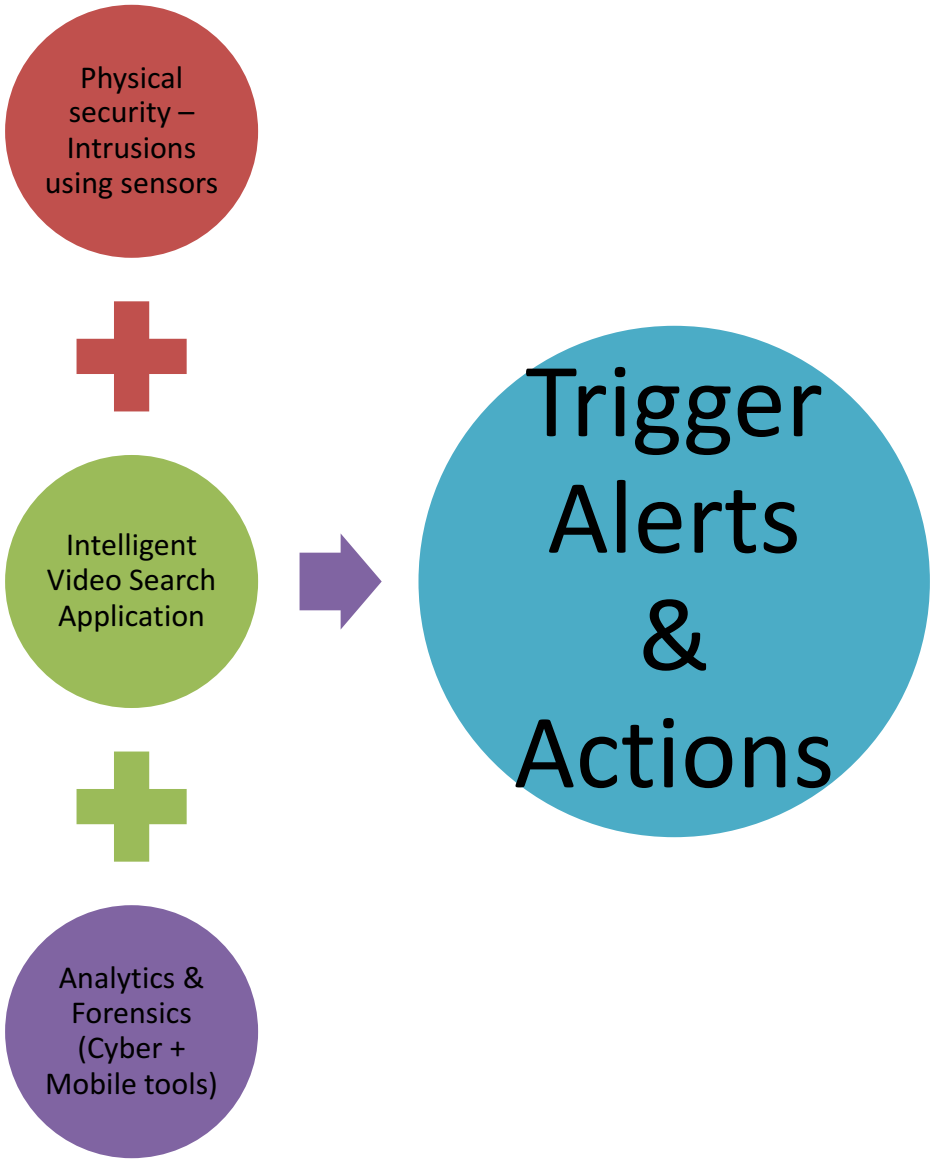
# Video Analytics Based Security



# Other IOT Sensors

# INSIDE building with back-end command & control systems

# Alerts + Analytics & Forensics Layer

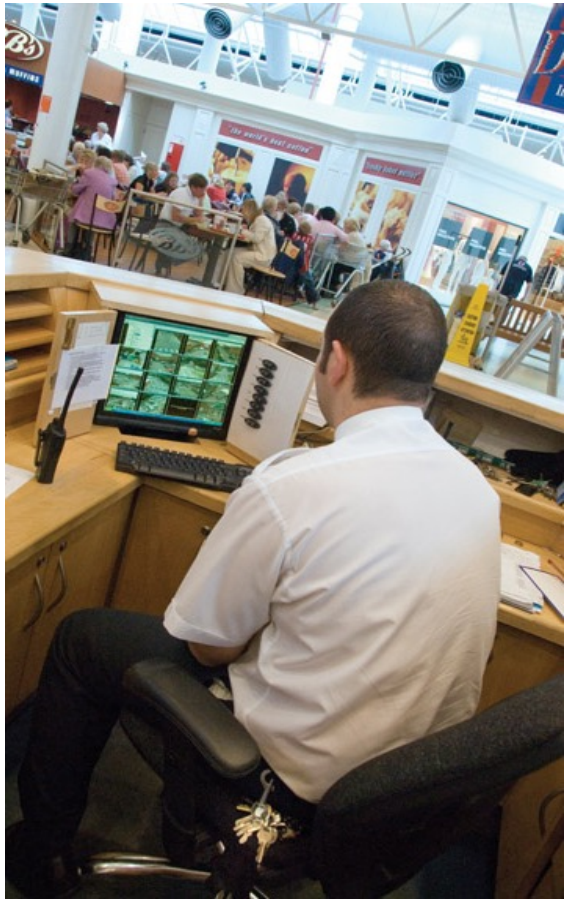


# The challenge

Video surveillance is a booming business, and installations become larger and larger with lot of recordings – but not used till an ‘event’ occurs

Several Studies, concluded that personnel can only watch one monitor for 20 minutes before losing focus, so the purpose is lost, if alerts are not generated automatically

And how do we turn video surveillance from a reactive tool to a pro-active instrument?



# Video Analytics with Identification of Blacklisted people & VIPs

Install a good set of cameras at the entrance of the prison and give a feed to the "Video Analytics" engine installed in the control room

State police and other central agencies can give the list of 'wanted criminals' as well as VIPs along with photographs

It can give a lot of demographic inputs as well as identify the VIPs and Blacklisted people by comparing the list of photos uploaded

It can also identify the prisoners movement, if any thru the gate and record the movement automatically

# Intelligent search app

Large installations have multiple cameras & stored for a period

In order to find a specific event or person, many hours of video material from several channels has to be manually inspected.

This costly and time-consuming process

This Quick Intelligent Search app cuts down costs and time drastically using intelligent processing of multiple video recordings

# Command & Control Centre

It is a must to react to alarms and alerts

It must cover all zones – Perimeter to Interiors ….

Must have security cover / back-up

Must be secured itself with good intelligent systems

# Command & Control Room

Conceptually, a command center is a source of leadership and guidance to ensure that service and order is maintained

The Control room is the most important area within the company premises as it controls various activities taking place within the enterprises.

Hence the Control Room should be the State of the Art Technology and should have advance devices to perform the day to day activities and record security breaches & action taken to prevent as well as avoid such incidents in future.

Most important is to alert the security men on duty whenever an action is required.

Also, generate MIS and specific reports to Management team for improving security and safety.

# Layered Defense Model Subtopics

*Perimeter and Building Grounds*

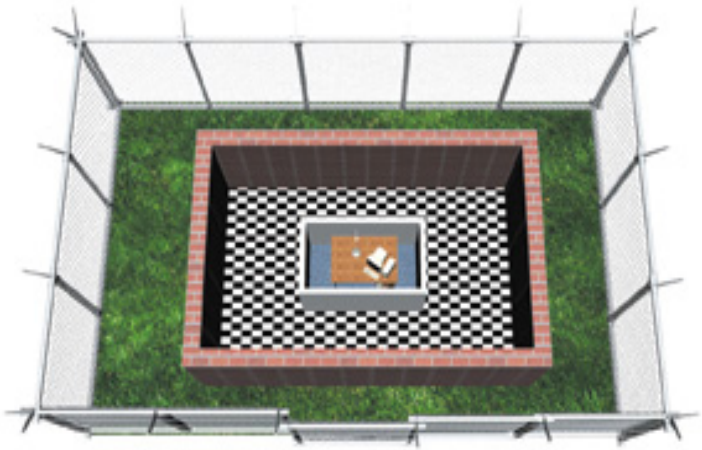
Building Entry Points

Inside the Building -- Building Floors/Office Suites

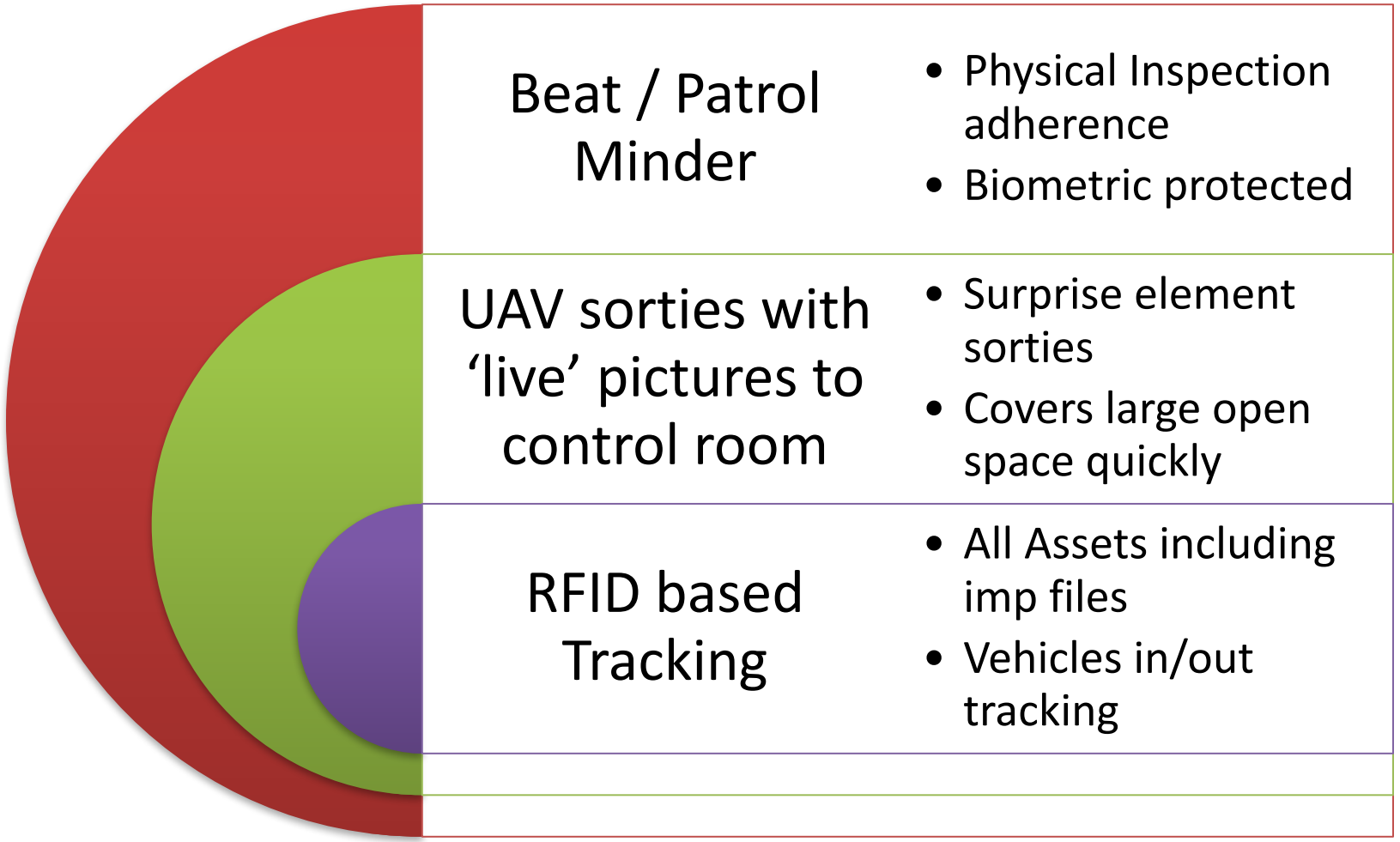
Data Centers or Server Room Security

Computer Equipment Protection

Object Protection



# Physical + Visual Inspection



# Object Protection

Objects are placed inside security containers such as safes, vaults, or locking file cabinets.

- Should be theft-resistant and fire-resistant.
- Steel containers with a locking device.
- Create good lock combinations, change them frequently, and monitor the distribution.