AI & Tech

Counter Crime & Risk Concerns using tech & apps for

- Home Invasions
- Rape
- Smash & Grabbers
- And more……

IT'S HIM HUMAN INVESTIGATION MANAGEMENT

CAPSI CENTRAL ASSOCIATION OF PRIVATE SECURITY INDUSTRY

IFPO INTERNATIONAL FOUNDATION FOR PROTECTION OFFICERS KNOWLEDGE TO PROTECT

ISIO ISIO - International Security Industry Organization

SASA SECURITY ASSOCIATION OF SOUTH AFRICA

Introduction

Security personnel manage the flow and behaviour of people besides find crime and stop it, as well as, protecting sites and saving lives.

They are the ones that use the technology. The practitioners should consider two objectives namely,

- Their location: countering common (holistic) crime
- Field of Interest: countering distinct crime besides risk concerns

Besides all are involved in life impacting and deadly incidents, emergency management and investigations.

The focus could be on knowing the type of crime that they need to litigate or to reduce the collateral damage. Some look at websites and see technical information or visual pictures of crime displaying the technology at work.

They may see words or terms that the technical designers or system integrators use ***but*** that language may not attract attention of the security practitioners who are buying, using and/or selling the service. It would be helpful if the manufacturers, distributors and resellers talk to complete solutions for specific crime or issues in theatre that the practitioners have to litigate.

The issue here is that there is no one size fits all because one may require to integrate various technologies to litigate a particular crime or issue of concern. Consequently, this is a guidance booklet full of ideas by providing concepts for thought.

Note: We must keep in mind that certain technologies or brands and models of technologies that have been banned from government sites for good reasons. The practitioner must also consider the performance of such technology and the credibility of the manufacturer that needs to be considered. Both of the above could lead to profit loss besides reputational damage. Do check on other work by the author for reference links to laboratories for distinct reasons.

The future is here

There is a wide range of technologies available that are highly effective and producing predicted results. In other words, there is software that can evaluate the current position and predict issues of concern by testing outcomes when the risk escalates by certain percentages. Subsequently, there are also vulnerable scenarios that require innovative solutions besides upgrading existing apps that could be brought into session by adding them to a main controller (PSIM, VMS).

Amazingly there is a variety of technologies besides software apps that enhance and increase the operational scope of technologies. Having said such, we need to integrate them all together to serve a complete solution for crime fighting or upgrading to litigate the risk of concern.

For example, a control room needs to be classed as a restricted area. One could use one method or increase the level of security by adding an additional method (app). The same technology could be used to stop a kidnap in theatre. This displays the versatility.

Some ideas mentioned herein on 'apps' may not yet available today but rest assured because they should be shortly on the shelves. This technology sector is innovatively growing at a fast speed and therefore do visit media from time to time to find the latest or consult with silo experts.

The most important thing about AI is fully research and investigate the crime or concerns related to the location and/or field of interest for determining the SPI. *(Situation, Position, Implications) (Kirsten J, 2015) which will dictate the technological requirements.*

What is the situation in the location and field of interest?

Expand the situational awareness into the criminal methods and human behaviour for discovering criminal intention by considering that, security manage the flow and behaviour of people besides find the crime and stop it – protect sites and save lives.

Then research and investigate all technologies and their capabilities to identify the crime and stop it – protect sites and save lives.

Know and talk to the crime

There are IT manufacturers, System Integrators or Installers that may be unaware of what the market requires or what the end user is looking for.

View the statistics of the crime in the location or a field of interest. The stats could point one to discover the biggest fears such as stalking, home invasions, kidnapping, rape and murder. There is also local gangs or organized crime that could highjack company assets or services for human trafficking, drug smuggling or any other illegal activity.

It is the security practitioners that are using technology and equipment. The security sector's thought pattern must be comprehended and in relation to the location or field of interest.

The words 'anti-tailgating' or man-down does not justify the terms or describe the importance of using such technology. *Therefore, on the re-sellers' websites the words should be* – **Counter the Crime!** such as counter-rape, stalking, kidnapping, or the appropriate crime the location or for a vertical sector (field of interest).

This also applies to other issues related to a vertical sector. For example, **counter**-corruption, counter workplace-violence, counterterrorism, besides others.

Each sector has its unique issues but could use the same technology as other sectors for unique purpose. Critical infrastructure protection, border security, ports and harbours, cargo, prison security, food and energy security to mention can use the same apps for generic crime for their unique needs with small additions.

This is not a one size-fits all type of solution. One must then appreciate that banking on only one technology may not litigate the crime. There is a difference between protecting the site and litigating the crime. Focusing on litigating the crime will in-turn protect the site.

[1]**PSIM** (physical security information management) & **VMS** (video management) systems triangulates devices and methodologies together to counter crime and risk concerns. Subsequently, a variety of solutions needs to be used at the same time to find the crime and stop it or protect sites and save lives. It may be appropriate at this stage to stress that PSIM and VMS is also used for incidents. Investigations and emergency management because practitioners are involved in all three.

The following is world-wide but varies in percentage, therefore, check stats in your location.

Most importantly, regardless of the technology selected one must keep 'compliance' in mind by acknowledging the importance of including encryption of 'Security' and Technology for 'Evidence Gathering' besides the integrity of the data or access. This can be done with standards such as 'Triple Des' or 'AES 256'. There could be other scenarios that require 'Time Stamping' for several reasons as well as for governance management.

Also, keep in mind that certain brands or models of the brands could be banned from government sites for good reason. There are investigative journalists with laboratories that not only test technologies but also investigate the credibility of companies.

[1] View the difference of PSIM & VMS in Critical Thinking X Factor

Counter Generic Crime

Rape	Stalking
Kidnaping	Home invasions

Software Apps such as video analytics and/or sensors be used for higher level security. The following could be used separately or in combination with others to reduce the level of collateral damage or litigate the crime.

- Facial recognition and pairing of approved people when escorted (only approved people may escort specific people). Therefore, only approved people should be on the premises. Unknown people must be flagged and removed off site.
    - Facial recognition database could contain people disallowed by court order.
    - For specific sites include facial recognition database of wanted, or missing people
- Tailgating detection for *all and <u>both</u>* entry and exit points so that both one can monitor what or who is coming in or what and who is leaving (apps for people with object detection)
- Apps to identify Man-down, aggressive behaviour detection, etc.
- Emergency recognition (verbal or visual: word or hand-sign)

    The following vertical sectors require the same above for perimeter security
- Virtual perimeter alarming that has a wide range of sensors. For example, motion detection as well as appropriately positioned pressure pads
- Anti-tailgating of people or vehicles of any type.
- LPR (License Plate Recognition) connected to database of stolen cars besides approved vehicles*. When there is no license plates then software should declare emergency and activate procedures.*
- Technology that can detect explosives
- Object Monitoring (Weapon detection or active assailant/vehicle)
- Gunshot Detection
- Drone Detection and counter drone technology
- Detection of perpetrator/s crawling on mission (man-down besides crossing virtual perimeter boundary) or crawling on-site under the laser beams or radar.
- Detecting any object dropping from the sky within the site.

For Correctional services, prisoners or officers could use GPS tracking bracelets or other devices within the perimeter that can be tracked using CCTV apps.

Medical Related sites

Mental Institutions

Drug and Drink Rehabilitation Centres

Hospitals

Child and Elderly care centres or recreation centres or parks.

Include apps to Identify

- Identify Man-down, crawling or *having a seizure*
- Identify Falling off bed or slipping
- Indecent exposure
- Wheel-chair toppling

For maternity and avoiding child-kidnapping include

- Mother to child RFID tagging
- Facial recognition pairing of approved people : Only allowed staff or parents allowed into areas. Unidentified people must be disallowed with immediate alert to response personnel.

Biothreat security

When people are desperate then they are capable of anything. It could be used to identify infected people so to ensure they enter a specific entrance and to monitor any form of aggressive behaviour. This alert could then despatch security staff that are appropriately PPE protected to manage violent behaviour. Also, the software is to prevent the desperate from entering through the backdoors or goods such as oxygen cylinders

- Anti-tailgating at all entrances and exits
- Detect aggressive behaviour or man down
- People counting per zone
- Flow of people
- Counter corruption using anti-tailgating in-and-out along with detection of people with people or people with objects.

Special Protection Centres

Social Welfare places of safety

Witness protection

Courts of Law

All the technology and apps mentioned in the generic crime section besides the 'restricted area scenario (see next page)' and also include the following:

- Include facial recognition database of registered sex offenders, wanted people, missing people or pictures of specific people that have been issued with restraint orders by a court of law.
- RFID or GPS bracelets could be used for all scenarios that can monitor the walking direction along a virtual perimeter and alarm triggered when breached. CCTV could also be activated to determine the intention or behaviour of a person on concern besides the direction they are taking.

Restricted areas

Restricted areas e.g., AI protecting info & company secrets

Security control rooms, IT and research centres, to give an idea.

One should consult with a silo expert on the cyber security. The restricted area or room must have a formidable security system to ensure it is only in attended by specific people.

Furthermore, no device can enter the zone or leave the zone without permission.

Include specifically both technologies

- Facial recognition of approved people allowed in the area
- Object Monitoring to find any object entering or leaving the area.
- Anti-tailgating both on entry and exit

Counter Corruption and avoid reputational damage

Use required and appropriate 'generic crime' above and ensure to include,

To identify taking a bribe from people jumping the queues (time set doors to be opened, where should people be standing, and where are they forming a queue elsewhere. Know which queue enters site first).

****(Alarmed when wrong queue enters site first, and which door is entered into. Who is allowed to open the doors and who opens the door must be known)?****

- Object monitoring. Pairing face recognition with allowed objects could reduce false alarms especially at *unloading or loading docks.*

- People counting, virtual perimeter and anti-tailgating (entry and exit):

- Obviously, the facial recognition of allowed people however with disallowed objects entering or leaving the site is criminal.

Mob attacks and Armed theft

Smash & grab theft or armed attacks

Riots

Small armed attack teams

Sites or stores have experienced smash and grab mob-theft or small armed groups depending on location. This is when people enter together, thieve openly and all walk out together.

Use crowd formation detection application with people counting that could manage access to a specific number of people at any one time. If more than the allocated number are trying to enter, or suspicious people wearing head gear (motorcycle helmets) then access could be denied and if necessary, defended by door locking mechanisms with appropriate alarms and alert messages despatched.

- Include the Video Analytics as per generic crime mentioned in the beginning. However more in-depth crowd behaviour detection could assist for example, man-down or crawling.
- Facial recognition alarming when identifying facial covering, masks and motorcycle helmets (AI can distinguish between medical mask and full facial mask to limit false alarms)
- Object monitoring, weapon detection and gunshot detection

Emergency Management

There are situations where the public will go into panic mode and panic buy goods. The sites need to manage the flow of the population besides their behaviour. Include apps for,

- People counting and Traffic flow of people
- Aggressive behaviour detection
- Seismic (earth-quake regions) or gunshot detection and opening exits automatically
- Virtual perimeter breaching or object alarming if emergency exits are blocked
- Emergency recognition (verbal or visual: word or hand-sign)

Vertical Sectors

Hotels, Entertainment venues and other such like sites and following through into Critical Infrastructure security especially of the mass-transit hubs one has to consider the following,

Open or closed shopping centres

High-risk sites during specific threats (crime related to biological threat or to an economic meltdown)

- Include relevant suggestions mentioned in the generic crime section and commercial sector.
- Emergency management apps (view the security emergency management booklet)
- Point of note is to include behaviour detection to determine if aggressive or violent behaviour at specific locations and which staff are involved.

Profit Protection

AI can be used for profit- protection because of the crime related to a global threat that impacts the economy, or crime related to the location or field of interest.

- False Alarms: Attending to false alarms costs money. AI (artificial intelligence) saves the client money because the technology is able to read and distinguish between a false and positive alarm.

Also, AI can

- People counting to notify appropriate people to respond in appropriate numbers thus not wasting money on irrelevant people that also cost money in transportation besides for their time.
- perpetrators could be stopped before the crime is fully realized or caught quickly saving money and anxiety.
- reducing the percentage of budget for loss prevention
- AI could identify an individual perpetrator or mob formation and could activate counter measures to reduce the collateral damage and related costs.
- Using AI provides the opportunity to increase the number of security investigators that are focused on looking for crime or managing aggressive and violent behaviour and stopping it.

Other scenarios

Examples

For cities and neighbourhoods

Definition: *Active Vehicle Assailants*

Similar technologies mentioned can assist the AI system. Having said such, each scenario may demand distinct software applications detecting any object. For example, a car can be detected driving at a high speed (radar detection) which may trigger a deterrent of some kind (e.g., boom) being activated automatically to prevent a planned attack on a venue or on a crowd. Obviously, the tech must distinguish between government vehicles and private vehicles.

Protecting urban security or large properties

Definition: *Finding Assets or Assailants in large sites*

To identify, search and find assets or people on large sites could take hours and even days. These sites could be industrial sized premises or huge hectors of farmland. There could be instances that could result in deadly consequences. This is when the remedy demands fast reaction speed. Sensors are positioned that could automatically trigger the deployment of drones that may have software that could detect motion, thermal detection of humans and animals. *The drone* could identify a person or animal and track besides sending out messages that could contain video footage, pictures and GPS location. The same technology could be used when the sensor trigger is a gunshot or is alarm activated when a fire alarm is activated. *There are already drones* that automatically deploy to scout a certain area for a period of time that return to their landing dock and recharge automatically.

Counter Drone and Drone Security

There is technology that can interfere with any form of wireless control of any device besides the GPS controlling of the drone. There are also encrypted technology and devices that can retain the security integrity of a site or the drone.

Using AI for investigation

It is not the weapon that is the threat – it is a person/people. Identifying specific human behaviour is imperative. It is also possible to find a person of concern using weapon identification. Combining both simply states that all issues is aggressive and violent behaviour. The Investigation process is to find a person of interest and determine if they are committing crime voluntarily or under duress by working in concert with others. Subsequently, match people with people or people with objects to uncover the actors and comprehend the criminal methods that are being used.

This could be by identifying the change in pattern from the baseline. This could relate to people's behaviour or missing objects besides identing unaccountable objects entering the scene, for example a bag or suitcase not accompanied by someone. The person could be identified that has carried that bag or suitcase by rewinding the video clips of different cameras in various locations until the person that has placed the item is identified.

At any time appropriate technology is used for legitimate evidence gathering and safeguarding the evidence.

Reporting systems are vital

Incident or investigation management software therefore is key to look for a particular incident that will then points to a criminal method which could be a copycat, or a newly innovative criminal method being used.

This booklet outlines only specific examples of scenarios in demonstrating the depth and width of what types of motivations and types of crimes that are coming into theatre, which should be considered for AI management.

To out-think and outsmart criminals one should acquire certain skills to master the skill-craft. There are other *booklets in the HIM Tool such as security criminology-risk investigation and master investigator critical thinking investigation that provide methodologies to apply the skills and knowledge to reach the objectives.*

Guidance Project Sheet

- Describe the full and complete nature of the beast (crime or concern) in a location of field of interest (Define it)
- Consider the vulnerability landscape and what could impact the mood (behaviour) of the beast (how it sees, talks, moves and behaves)
- Consider the environmental issues or conditions of relative issues that could impact, for example: Geography, Climate, Location, or Audience (people).
- List the information resources that can provide relative information.
- What has to be considered to locate a person of concern or the people involved? (e.g., culture, criminal behaviour, criminal methods, etc)
- What technology is required for where and why?
- What is required in the incident or investigation software to identify flags of concern?
- What knowledge and skillsets should an analyst or distinct staff possess?
- How will the incident/investigation information be stored securely?
- Who must be kept in the loop or specially informed for distinct reason?
- And how fast must they be informed and how must they be informed?

Project Sheet Conclusion

Practitioners must work out what is best for themselves according to their own learning curve or field of interest whereas other steps or different steps could be sequenced.

As stated before – this is not a one size fits all kind-of-thing for numerous reasons besides the crime related to the location or fields of interest besides other considerations for example, environmental conditions.

Concluding

An example of one app is therefore could be used to reduce the risk or litigate many things, displays that people need to relate to app to the crime or fear of incident related.

- All buildings or homes that house people and at all entrances and exit points to *reduce crime related to home invasions, kidnapping, stalkers, rapists, & murders*
- Mental institutions, rehabilitation centers, nursing homes, retirement villages and schools to *ensure safe containment*. (Position outside going in and inside going out)
- *Restricted area security:* that may hold intellectual property or contain any other valuables.
- *Avoiding reputational damage* because of corruption. When people are being let into a site by entering before others (day/*time stamped*) which could be by using people counting within a line and an app to monitor the direction of their walking and entering the site.

Note: This version could be updated from time to time because of novel issues discovered or recent innovations suggested. Subscribers to HIM will be informed (View below the version date)

The booklets referred to in this work 'Security Operational and Protocol Guide for Managing Biothreats, Critical Thinking the X Factor in Criminology, Security and Risk (Vol3), Security and Criminology Investigation Management(Vol4), Critical Thinking in Investigation(Vol5), to which all are endorsed by various organizations. Authored by Juan Kirsten for HIM Human Investigation Management.