# AI & Technology

## Merging Technologies and Workforce for Security Criminology-Risk Investigation Management

## 2024

### What is it? How it works? How to get the most out of it!

This edition is themed on the current threat along with its tailing threats

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

SASSA SECURITY ASSOCIATION OF SOUTH AFRICA

# Dedication

To all practitioners in the security industry regardless of title and rank on the frontlines handling life impacting and deadly incidents -Thank you for your service!

**Important Notes:**

- This is a living document that will update regularly because the speed of innovative technologies and content analytics and new equipment being launched.

- Naturally new crime or criminal intent must be discovered besides evolving issues uncovered.

- This work contains suggestions for technologies and software that are currently in use and others that could enter the market shortly.

- We cover a wide range of examples, whereas one may see something and not consider such as relevant. Do read all the examples because thought based on something seen before could inspire a solution for another situation.

- Today we are fortunate to live in a moment in time when we can access video clips that explain easily on how things work. You will find in this work a mixture of knowledge on topics along with descriptions of technologies and equipment. The reader may wish to know more and therefore we highly recommend making use of the wide range of internet powered video clips that can be searched for on 'YouTube' or such like.

- Also note that this booklet is written in NLP format, meaning that certain words or ideas are re-phrased or repeated because certain principles and formulas apply to more than one methodology. This methodology fosters human instinct by increasing retention levels . This is important for practitioners in this field need to react instinctively because they do manage life impacting or deadly incidents.

# Index

# Contents

This AI (Artificial Intelligence) work speaks to,

What we thought we knew in 2019 will not be the same in 2020 and beyond. The motivations for crime, the types of crime and the amount of crime is beyond comprehension resulting from the active biological threat and its tailing threats. Added to the mix in 2022, the second economic meltdown stimulated by the Russian Ukraine saga triggered AI and technology innovation again into AI playing an important role in energy and food security.

The practitioner needs to out-think and outsmart perpetrators by using AI intelligence (as in content analytics, equipment, technologies, and reporting software) besides human intelligence (workforce) to uncover new crime and evolving copycat crime. Furthermore, AI & technologies will save lives *because of the reaction response speed* to identify, alert and appropriately assist which are primary factors.

# AI for crime is used in all fields

This booklet is based on a research philosophy and investigative methodology that has uncovered new crime, discovered evolving copycat crime besides opportunities (methods) to mitigate or limit the level of collateral damage of the threats.

This is the fourth industrial revolution whereas all sectors are venturing into using artificial intelligence besides new technologies. Regardless of the field of interest, crime will be found one way or another in any profession and job function. *The crime committed could involve using manpower and with/or technology* and could be discovered and managed by using the same methods.

To comprehend the narrative (big picture), the user of artificial intelligence (AI) tools should think in a specific way using critical thinking (security styled). The process of thinking out-and-in-the-box and back out the box again is required to know what stimulates criminal behaviour and to follow the pattern for comprehending the width, depth and scope of the tools required.

There is initial data inserted by technology or humans into the 'system' that is recording data, analysing and filtering the data. [It] could identify relationship bridges between people with people or people with things and is also capable to flag incidents of concern and actioning or deploying solutions automatically. Technologies could sound alarms, send messages to the manpower on the ground, or remotely activate machines and equipment for example, robotics, drones. or opening emergency exists or locking down sites.

# Introduction

AI and technology is not a one size fits all kind-of-thing. However, there are complete solutions for certain applications, but there are conditions or needs that must be purposely addressed. Therefore, one must consider distinct goals based on 'self-researched' projects and objectives.

A particularly important consideration is that IT people cannot simply design software without consulting specialist security practitioners. A good example is a pandemic. It is the security practitioners that are doing the work on the ground by using technology and the workforce to take temperature, manage the behaviour and flow of people besides ensuring hygiene protocols are adhered to. Furthermore, they have to find the crime related to the threat besides protecting the integrity of the site for profit protection.

Initially, the manufacturers or system integrators quickly promoted 'covid compliant' plugins such as mask identification and to monitor social distancing. The security practitioners have specific issues to contend with in relation to their objectives and therefore views the needs differently to the IT sector because this is related to biological threat security. Some of these technologies that is mentioned could be also used to counter crime e.g., counter rape, kidnapping, corruption. Consequently, the security industry requires specific or use current apps for different purposes and for specific objectives.

It therefore stands to reason that one must be familiar with the threat in theatre and what is best to use. This is means that having knowledge of security, criminology-risk and investigation methodologies besides human behaviour is imperative.

Consequently, we define the users and focus on critical thinking out-and-in the box by bonding and bridging narrative research [digital management platform to see the big picture] with situational awareness [Technologies] *using investigative methodologies* [soft skills driven] by the workforce.

# Already using AI and technologies

The use of AI and other technologies is already in session in the security sector but could be underutilized:

Partially relevant technology and skills: There may be companies that have CCTV integrated with detection software, such as, facial recognition, object monitoring, license plate recognition and alarm systems that send out quick messages or video pictures and can record incidents. The emphasis must be on the comprehending the reporting of data easily which could be best understood with *a visually presented platform that would serve to see who or what is associated to a threat or an incident.*

A particular note is that there are people that have purchased incident reporting or investigation management software by buying the bells and whistles. If one did a survey, they would find that not all buyers are happy with their results. There are people that may lay the blame squarely at the feet of the software providers which may not the case. There are distinct skillsets that are required to use such technology besides comprehending the analysis.

According to the research outcomes in all the author's work, not all people are a good fit for specific job functions that relies on extracting *accurate and authentic* information therefore, even if they may have the required knowledge, they would need to have character traits besides the skill set best suited for crime or security criminology-risk investigation. There is a distinction between the two.

*AI considered differently*

There is crime in all industries and professions. The needs and desired outcomes could differ. In the field of security criminology-risk investigation, we have global threats in theatre that could impact all sectors and job functions besides unique crime related to a distinct field of interest.

Furthermore, in the conceptional framework *of any investigation* certain considerations and protocols are suggested herein to ensure that all-the-truthful information must be considered because of the fact that the AI and technologies are only as good as the users. One has to check with laboratories to ensure that the technology is fit for purpose to avoid reputational damage.

It is not the weapon, that is the problem – it is the person that uses the weapon therefore, the focus is finding the person, or the people involved. Having said such, the contradiction is when an object is moved or disappeared then by finding and tracing the object would find the person of concern. At the end of the day – it is the 'habitual' (behaviour) and actions (pattern) of people (their modus operandi) that needs to be identified.

[1] *MOST IMPORTANT PRINCIPLE (Juan Kirsten 2018)*

Security success depends on the **level of situational awareness** of the **people** (decision-makers) on the ground and their **reaction speed**.

- *To know the true situation,* one must get to know the nature of the beast intimately. To know the situation the person needs knowledge and a continuous flow of information.
- In conventional investigations, reaction speed is timeous as in; for the right reason, at the right time and under the right conditions, actions are taken When the situation could lead to a life impacting or deadly outcome then decision-making and reaction speed must be super-fast. This is when technology could excel over people.

Both the human and technology can comply with the formula

- *Level of Situational Awareness*

The person and/or the technology must capture the information. The users should know security and criminology-risk intelligence to select and set the protocols for the technology. In other words. they tell the technology what to look for.

- *Decision-Making*

The person or the machine (pre-programed instruction) makes decisions when the pattern of information changes.

- *Reaction speed*

The situation will dictate the reaction speed

[1] Juan Kirsten2018/2021, Critical Thinking the X-Factor in security criminology risk investigation

# Principles

- Security success depends on the *level of situational awareness* of *the people on the ground (all are decision-makers)* and *their reaction speed*.
- Know SPI(Situation – Position – Implications)
- *There is a difference between crime investigators* that are only summoned after the fact *and the security criminology/risk investigators* that must *find the crime before the fact* to limit or mitigate the damage so to speak.
- Practitioners use technology and manpower for being in a constant state of situational awareness (investigation mode) because they are managing life impacting and deadly incidents*. This in-turn impacts on the appropriate timing of reaction speed.*
- The biggest nightmare is not knowing what is truly happening on the ground right now under one's own nose.

  Subsequently, practitioners must rely on discovering a person of interest and to find who else is involved using soft skills (critical thinking/security styled. Technology assists by consulting the incident reporting's to find and flag issues of concern by identifying and following the pattern (modus operandi).

# The point of AI is machine learning and machine doing.

Machine learning's objective is to get all the information (data from various resources) then searches for that information that pre-programmed either cancels the alarms or actioning (machine doing) which is reporting besides it could activate counter measures using technology, equipment or notifying specific people.

In other words, one can imagine that a person already has a picture of specific animals in their head. They also have a picture of a person. AI could have the same pictures in their database (memory). So, when it sees an image walking or crawling it could distinguish what it is and then react with pre-programed instruction.

If the AI identifies a bird and has no image of it in its database (memory), then it will record the incident and issue alarm. Then the programmer would instruct the AI that when it sees a bird again then it must activate specific instructions. This is how it learns when it identifies a threat that it has not seen before - it alarms the threat until it learns how to react. This dictates that some manufacturers state that they need a few days or weeks on site to tailor the AI for a project.

# AI can Profit Protect

AI can be used to protect profit depending on the devices used because,

- it reduces the expenses related to check false alarms
- could summon specific people besides the number of people saving money.
- could direct people saving time and money or re-directing a larger portion of the budget to use more 'human investigators' for gathering intelligence and to identify other forms of crime

**Find more** on issues related to economic meltdown of the pandemic and war between Russia and Ukraine on how AI can be used for profit protection (page 39)

# AI can save lives

Every minute counts when a person has a heart attack or stroke. When AI picks up someone on the floor or trying to call then the appropriate people could be messaged immediately saving time.

**Find more** in the booklet AI for security emergency management.

# HUMINT Human Intelligence

# You are the hypothesis.

*The instrument is only as good as the user*

[2]Dr Raj Ramesh in his 5-minute video clip demonstrates AI [Artificial Intelligence] theory and relating to mimicking HUMINT [Human Intelligence].

## Knowing the nature of the beast intimately

Let us consider that you want to design a ‘’POLICE ROBOT’’ A robot gets programmed to do certain things. So, one has to think by way of considering how it would move, what information would be needed, how it will remember, it would report its progress besides secure the evidence and what action must be taken, when where and how.

*Critical Thinking Situational Awareness*

Critical Thinking the X Factor in Criminology, Security and Risk Vol 3 uses a person as the hypothesis and refers to identifying the crime (action), crime culture (behaviour) and criminal framework (pattern) (J Kirsten 2018)

When considering the complete and truthful nature of the beast then one could consider the basic formula of what a person needs to hear, see, touch, move (movement) and talk.

Taste and smell may not be required for distinct scenarios unless there was a scenario that required taste and smell. In that case one would use technology that could analyse liquids or extract particles out to the air to analyse.

It is also paramount to know how ‘it’ (the beast) moods (behaves)

This basic formula gives direction on how AI works. The human brain cannot distinguish between reality or fantasy. Humans acquire knowledge from learning, experiencing and then reacts accordingly which could be impulsively (instinct) or at a pre-planned pace.

[2] Dr Raj Raemsh What is Artificial Intelligence? In 5 minutes. https://www.youtube.com/watch?v=2ePf9rue1Ao

AI capable of mimicking Humans

- Seeing: CCTV Video
- Feeling: Motion and Intrusion detection
- Listens: Gunshot detection software or audio recording
- Evaluating: Measuring distances and heights to restrict vehicle entry besides measuring speed using radar
- Following: Tracing and Tracking (GPS, RFID, etc)
- Remembering: Memory containing Video, Audio and all Reporting
- Analysing and Decision-making: Filtering out false alarms & flagging issues of concern and activates programmed instructions.
- Talking (asking for help): making sounds as in alarms or sending texted messages
- Confronting: Using the counter measures by using relevant means be it technology. equipment and/or manpower

Using this simple formula of imaging oneself in the AI's shoes, then one could comprehend the narrative framework and what one would need, be it, in the form of technology and manpower.

The first step then is to truly know what one has to contend with by knowing intimately the full and truthful nature of the beast and its behaviour.

- What is it? Describe the project brief in detail
  Keep in mind the list of the current threats: E.g., Active Biological Threat or a War, then the crime related to the outcome of the threat being the economic meltdown.

  All the following gives an outline in the work below:
- How does it work?
- What can affect it?

What is needed?

- Technology
- Manpower

Where will it be used?

Why will it be used?

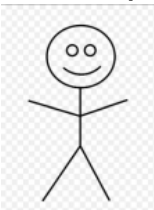
Identify, Investigate, and Manage all the outcomes by the reporting!

> **Important Note:** There must be no bias whatsoever and in any sense of the word towards technology or a person. Technology could have recently been improved or people could have issues that change their baseline.

# Nature of the Beast

AI is all about data capture for machine learning and machine doing. AI initially could just be learning and could progress into deep learning to comprehend patterns. Comprehending the narrative and its framework is by reading the patten of behaviour.

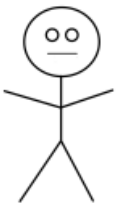
## [3]Reading Patterns - Baseline Principle



It is not the weapon that is of concern – it is people that commit crime, terror and havoc. There is a saying that people are creatures of habit (patterns). In investigation, people use interviewing skills to discover information that will uncover the truth. They may use specific skills to read people (behaviour & actions). So, when one knows the reaction pattern of a person, then one could know what not to do or purposely do something or say something for specific reason to extract information.

To discover a reason for concern would be when the *baseline/pattern changes*. In the world of investigation, the habitual habit is the baseline of a person's behaviour and actions. When the base-line pattern changes then it would require further and deeper investigation.

To feel the power of this method, have a conversation with a person. Begin with simple non-intrusive questions and watch their physical reactions and listen to their verbal tone to discover how they naturally react which is their baseline.



Their baseline would change for any reason be it, a thought that flew into their mind, or perhaps when they do not answer a question and then they may simply not react, or when they changed subject. All what you see and hear will then give guidance in comprehending the big picture.

[3] Critical Thinking the X Factor in Criminology, Security and Risk Vol 3 Juan Kirsten 2020/1

The same applies when looking at reports, data or video feeds to comprehend the big picture when we look for patterns emerging or the change in patterns to identify and find the source by comprehending the implications because of the change and those involved.

*The first step is knowing the complete and true nature of the beast!*

This begins with the first brief of the AI project where the level of situational awareness is paramount.

Do not be surprised when you are only provided with partial information to build and use the robot (AI). It is possible that the project author may not be fully aware of what they clearly want. Be quite clear that you need all-the-truthful information for the brief. You then could use a critical thinking methodology, distinct skills besides security and criminology-risk knowledge ([4]HIM Tool) to extract reliable and usable information to clarify the situation, know the position that one is in besides the implications of what is required.

Then considering the landscape of where, what, how and why the AI would be used. The security practitioner may want a simple guarding system that is solely based for guard control management which would include a reporting system.

Another practitioner in the same field would like to extend the parameters and would like to know relationship interactions that the guard would experience as in who are they meeting with, for how long, and where. Obviously, they would want to know the 'why' and would to be warned as soon as an issue of concern is identified. If this is the case, then they may need 'recorded evidence-based' technology that could produce video footage, access control tracing and route tracking or other evidence capturing tools mentioned later in this doc.

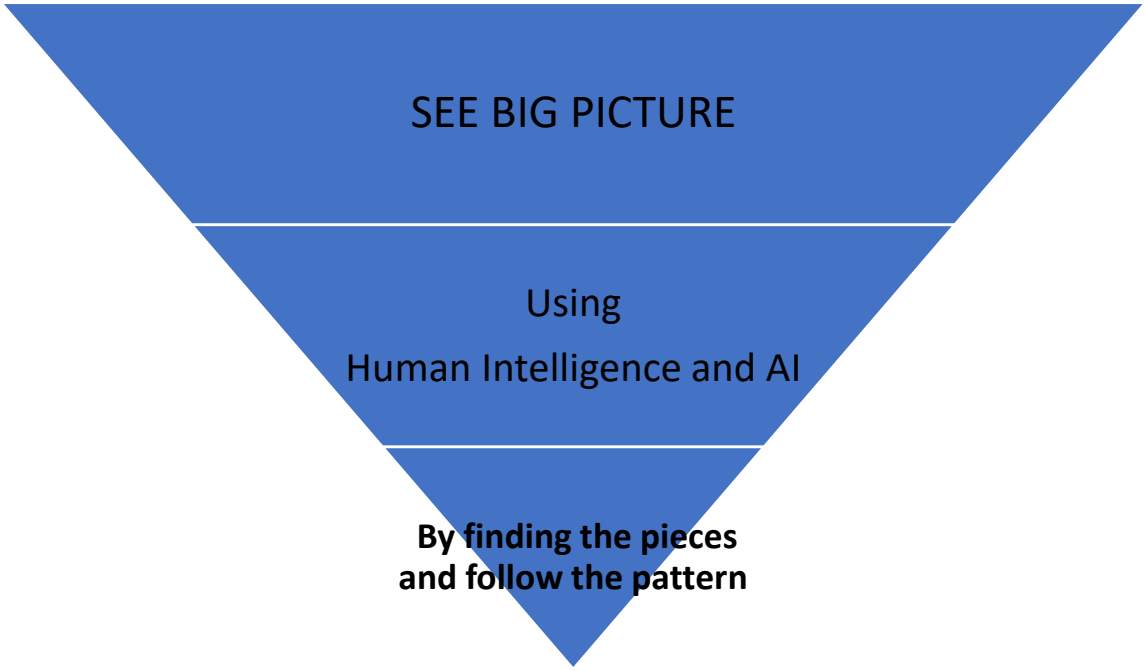
Therefore, the user must know the nature of the crime, criminal behaviour, criminal methods and cultural crime in order to be able to identify such (situational awareness), then comprehend the necessary technology to use and what is required from that technology and the manpower.

The big picture must be completely understood before one could fathom the non-tangible skillsets (specific skilled practitioners) and tangible tools (technology & equipment) that will be required to make up the AI System.

[4] HIM Tool www.human-investigation-management.com

# Triangulation Research

Triangulation research is bringing all the pieces together: technology, equipment, electronics, human input, data, using various methods of investigation to get the big picture. Then appropriate solutions or protocols can be implemented.




## AI is Puzzle Building

Wondering if people still build puzzles which comes in a box with a picture printed on lid of the box. In this AI day and age, in professions to get the big picture we have to be *situationally aware* of the puzzle and the individual pieces, meaning we need intelligence from people besides the technology and equipment which are both inputting and reporting information.

(*situationally awareness requires knowledge and thinking method)

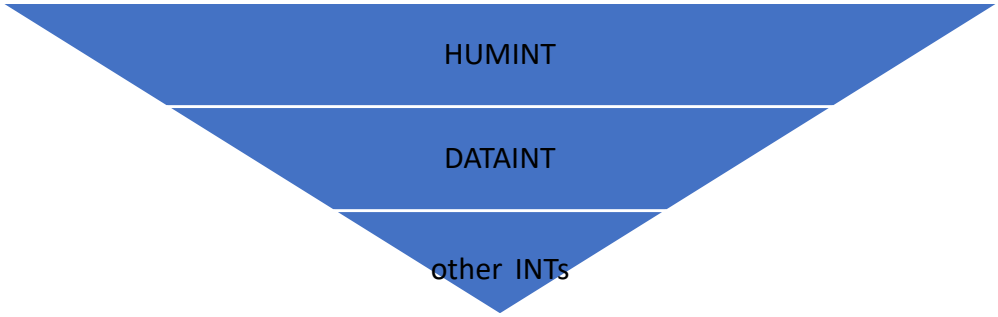
- We know that each piece of the puzzle is cut into different shapes
- We must *follow the pattern to locate* the pieces
- Each piece is meaningful because if there are missing pieces then we will not get the big picture

finding missing pieces

## we need investigation intelligence as in,

- what to know
- where to find
- how to use
- and why to look for each piece.

## Consider relevant methods and tools




## TECHINT with relative software


We could use visual recognition technology [5][PSIM] or use other investigation methods with technology that can match relationships to each other besides and being notified when actions are identified.

## Environmental intelligence


Considering that we could be working in a room that does not have good lighting at certain times during the day or could need to work at night which means that the lights must come on automatically by using light sensors (Electronic Intelligence ELINT)

[5] PSIM (Physical Security Investigation/information Management) systems

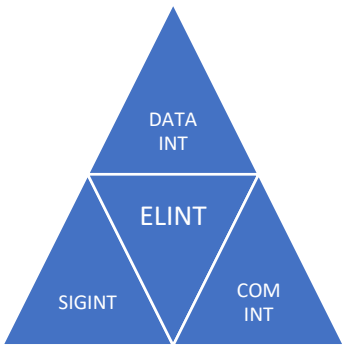
People provide information HUMINT


Different Investigators may need to be summoned to give their input because they may specialize in different fields and use different methods

We need relevant professionals or information gatherers such as

- People that see all colours because there could be people that are colour blind
- Artists and architects that understand design
- We may know that there could be a motor car in the picture, so we need to identify such and would require car enthusiasts, car salespeople and mechanics
- Finally, a carpenter or a metal worker that can make a frame to hold the picture

There are triangles within triangles meaning that other scenarios may need to be included or unique and again require different things. For example, we may need to use the puzzle as part of a presentation. So, we need a presenter that has a good voice, learned in their location or field interest. This person knows their subject matter and is capable of using the technology and equipment.




# Triangulating tangible and non-tangible information to automate systems.

In the security sector there is a wide variety of equipment, technology and manpower that need to contribute, insert and/or report information.

Considering qualitative research for AI, we may have the objective of gathering information from observation, interviews with people and from group discussions on new findings.

*This work emphasises focusing on triangulation research* of and in; investigation, data, theoretical, environmental and multiple methodologies ([6]Dezin,Norman 1978).

The reason being, is that technologies contribute in diverse ways for investigation. Such as, cctv access control or perimeter security could alarm an incident and record such, using recording devices when interviewing a suspect that is analysed resulting in clues that give direction for investigation, object monitoring, or tracing and tracking technology is used then to finally achieve the objectives

## PSIM, VSM Incident or Investigation Management Systems

Using the principle 'security success depends on the level of situational awareness (technology and manpower on the ground) and reaction speed, then we use technologies for PSIM [Physical Security Information/Investigation/Incident Management] or VSM [Video Management Systems]. Visually on screen we can see the ''whole picture'', so the question is 'what do we need to determine?''. Suggest, the reader research 'YouTube' to know about PSIM and VMS Systems.

## Intelligence Sources

*First and foremost, the person must know security criminology-risk investigation. Comprehending Criminal Intelligence and Criminal Intent Analysis* dictates that a person must know the thinking pattern required to identify the crime and criminals by sourcing information using technology and manpower. Intelligence can be obtained from all available sources because partial information may be provided from one medium or from a multitude of others.

We then converge by triangulating relative intelligence sources such as:

- HUMINT Human Intelligence
- COMINT Communications Intelligence
- DATAINT Data Intelligence
- TECHINT Technical Intelligence
- ELINT Electronic Intelligence
  There is also OSINT (Open-source Intelligence) and SIGINT (Signals intelligence) but for this work we focus and title the above.

[6] Denzin, Norman 78
https://books.google.co.za/books?id=UjcpxFE0T4cC&printsec=frontcover&dq=online+purchase+Norman+K.+Denzin+McGraw-Hill,+1978&hl=en&sa=X&ved=2ahUKEwik__aFvYHtAhUSiFwKHQD-BfQQ6AEwAnoECAgQAg#v=onepage&q&f=false

# Requirements

# Human Intelligence

- Non-Tangible Tools

Relevant knowledge: The knowledge of crime in the location and field of interest is paramount. If one does not know that a crime exists, then one cannot look for it. It is vital to know where to look and who to mix with, that can provide reliable information.

*The use of Critical Thinking* (Security Styled) for Criminology-Risk Situational Awareness dictates that an open and wide thought patten is required to comprehend the depth, width and strength of the intelligence system. Furthermore, it is a method of thought that can identify or make something that has never been used or seen before with the knowledge known at that time. The critical thinking situational awareness (out-and-in the box and out again) must incapsulate criminology, security, risk and investigation in order to strategically select the technology, equipment and to purposely layer manpower by skillsets.

## Investigation Intelligence methodology

Technology and equipment designers are IT specialists that may not be security criminology-risk investigators. *AI solutions requires both intellects* for the selection of equipment or technology to be relevant.

This is when different investigators use their methodologies and derive outcomes. *Therefore, the practitioner must have investigative intelligence*!

*For AI, Triangulating Investigation* is the foundation formula from beginning to end to comprehend the landscape for selecting the appropriate and relevant technology and equipment or experts to gather all the truthful information.

Different 'silo-expert-investigators' (e.g., open-source intelligence and Avsec investigators) will derive different results, therefore the same applies to using technology whereas each technological tool has its distinct benefit and could be utilized differently for various scenarios. Therefore, putting all together and triangulating the information gathered from the workforce and technology will provide a better overview and insight of issues being flagged.

- Investigate all technologies, all types of equipment and the authenticity of such.
- Apply different yet appropriate security criminology-risk investigative philosophies and methodologies to achieve the mission and objectives.

## Environment Intelligence & Awareness

Broad-based thought on Environments must be considered.

Environments must be considered for technology because information gathered can impede or support the collation of vital information. An example is in using technology or equipment, whereas temperature detection taken outside would be quite different than taken indoors.

*Cultural awareness*

There are cultures where the cultural behaviour may dictate clothing criteria. This could mean that facial recognition may not be effective. Do keep in mind that all cultures do live in polarized neighbourhoods besides in open neighbourhoods therefore it is advisable to have a private room which is manned by 'same-sexed' persons to ensure that the veil is lifted for identification.

*Emotion Awareness*

*Emotion detection* could be identified for suspicious or violent behaviour. This could be one person or a suspicious mob besides angry people collecting together possibly arming themselves with objects as weapons. Software could be used to identify such. There are also '*real-time'* CCTV operators that could be trained by renowned specialists on identifying suspicious behaviour.

*Emergency environmental awareness*

Within a mall or building, the traffic flow of people can be countered or monitored. This information can be used by the emergency managing officers whereas they could plan and manage the internal layout to ensure easy and fast escape if the venue is under threat.

## Keep in Mind

All the above on this page must be kept in mind when considering the *following* ***resources*** from tangible tools, such as DATAINT, TECHINT, ELINT, COMINT and SIGINT (Signal Intelligence).

# Artificial Intelligence

- Tangible Tools providing intelligence

As stated earlier in this booklet machine learning is through programmed instruction. This programmed information besides a continuous flow of information from devices is then building the brain-bank (memory) of the AI.

# Information Gathering Resources

## Data Intelligence (DATAINT)

AI depends on authentic and relevant data information. For specific applications there may be a fixed amount of data required for analytics or other applications that require a continuous feed of relevant or selective data.

*Objective*

The objective is to use technology and the people on the ground *to find the pattern* (modus operandi).

The type of data in various scenarios may require digital data to be captured, whereas evidenced based data can be drawn from videos, pictures or even logged computer activity. There also tons of date reported and provided by people using different devices.

When specific data is required from appropriate sources *for distinct purpose then specific actions can be activate, for example*:

- Equipment: information from equipment such as alarm systems, access control, perimeter security and such like, could be bridged with incident and investigation reporting software. This could be a method to assess the compliance of the equipment besides provide innovative ideas to resolve criminal intent.
- Software: video analytics, facial recognition, object monitoring, license plate recognition, tracing and tracking, violent behaviour
- Tracking equipment tech or software: Practitioners may have security officers being monitored with a verification system for compliance e.g., GEO fencing, GPS, RFID tracking to ensure routes are being authentically patrolled and should also be connected to incident reporting.
- The incident reporting of defensive actions*:* Automating defensive and protection equipment such as, door closures, deploying security smoke, pepper vapour spray or arming electrified fencing.

## Tech Intelligence (TECHINT)
## Technology

The software are the brains and therefore how one thinks (security criminology-risk) and interprets the incident reporting will dictate the inclusion of addons for technology required and software applications.

Each application 'addon' must be for distinct purpose and contain automated response mechanisms. The ***life impacting or deadly incidents*** that must be addressed such as in a person lying motionless on the ground or crawling. Reaction speed is vital.

Therefore, the software needs to *detect people in distress* and immediately despatch messaging to the appropriate people. This is obviously highly relevant to retirement villages, hospitals or any such like venue where there a high probability of such event.

Let us keep in mind that any site that hosts high human traffic volume that would require such, for example malls, shopping centres, or even for neighbour watch. To elaborate on the thinking, is when the practitioner knows that there could be a high probability of physical violence that could take place such as in a pub, a mental institution, a school, a hospital besides others. This is when the software must detect a violent episode.

An addon to the software to *identify and prevent tailgating meaning* that a person is trying to slip through behind a legitimate card or key holder. The software addon would be required for a higher level of security. An example, a person of concern could be someone trying to enter or exit undetected into an appartement building. *This person of concern* could be on mission to stalk, rape, rob, murder or kidnap.

*Facial recognition* by pairing approved escorts for people could be added on for anti-kidnapping or for witness protection (entry and exit).

The examples above display using apps to litigate relative methods of crime for a variety of reasons besides even more reasons for example, protection of an area holding high valuable good or even restricted areas containing intellectual property.

*And highly relevant to counter terror*

When the software identifies any of the above then it can alarm and despatch messages using various technological platforms, e.g., walkie talkies besides mobile phones *taking the necessary video footage for evidence capture and pushing messages.*

*The emergency management for disaster planning and counter terror*, or to comply with safety regulations one may want to monitor the human traffic flow on a site. They also need to constantly know the potential blockages that would inhibit the immediate evacuation of people. This scenario would use object monitoring or crossing the virtual perimeter ensuring a free and open pathway. Also, the software could ensure that that the exit doors are untampered with, and the outside is free of blockages.

Furthermore, practitioners would need to know quickly if a package or any object or item has been placed which is unattended for a brief period of time. For large sites there are apps to detect the route how the object travelled to its current location and with whom *however quantum computers to utilize such.*

*Adding additional Tools*

The software could provide heightened awareness by linking to access control systems  using access cards that have a photo of the user in the database. Facial recognition may need to detect masks for access control or deny access if the person is wearing headwear that hides the face.

There are software application plugins that speak for themselves by the descriptions of where and why they should be part of the AI system.

- Crowd formation identification (e.g., x number people and more)
- Weapon detection such as knives and batons
- Gunshot detection

## Be careful and research all relative implications

There are technology suppliers that attempt to ride on the ‘’threat of the day’’ and promote irrelative or partially relevant solutions. For example, it is not a clever idea to use sound alarms for people for certain scenarios that trespass specific rules because the sound can create panic.

The audience could also contain people that could be mentally unwell or paranoid for good reason. If the software is used for social distancing monitoring, then it would be used to inform the guard force on the ground to physically police the situation and not to create panic by using an alarm.

## Technology of concern: Always look for the risk factor

The first thing is to consider who can access the security system because it could contain certain intelligence of cases under investigation that must be kept secret. Specific users are granted 'relevant' access to part of the system that could be in the security team or from other departments.

There are AI systems that are partially or fully equipped systems with reporting and interfacing with machine alarm triggered pushed messages. With the speed on innovation all should be able to be updated especially because of *security enhancements*. Remember there are millions of hackers that are daily attempting to break into the programming systems.

There could be reputational damage or crime related to the technology or the users of such. When there is a rush to market of innovative technology or equipment, manufacturers could suffer reputational damage because their product is not thoroughly assessed or, is presented to the market using misleading information. It is important to use authentic equipment and technology in-case it needs to be used as evidence in a court of law.

*Dangers*

- Make sure that only authorized users have access for their field of interest which may not be all the tech and reporting systems.
- Double check the credibility and authenticity of the equipment.
- Keep in mind that IT criminals are in a constant state of finding methods to compromise the 'hardware or software. Therefore, ensure that encryption or relative is part of the solution.
- The motivations and new types of crimes for example, intellectual property theft, industrial espionage could need to be protected using various solutions.

## Communications Intelligence (COMINT)
## Handheld devices

The handheld devices be it a conventional smartphone, two way-radio that uses mobile networks or any other such device, will become 'the tool' of the trade for the workforce on the ground even more so.

The workforce that may use such technology could be lone workers or working alongside others on mission at the same time in the same theatre.

*Software*

There is a saying ''the software sells the box'', which is true in every aspect because it is what the software can do, that is important!

*Phones and body worn cameras could be used for rapid reporting and evidence gathering* by capturing video footage, taking still pictures, recording voice conversations or sending messages support quick and easy reporting systems which is necessary.

This technology is suitable for the guard force on the ground going right up the ladder through to forensic psychologists, intelligence analysts and chief investigators.

*Apps could be included Tracing and Tracking*: Emergency Panic button and location identification talks the importance for safeguarding the user of the device. The tracing and tracking abilities services may service a range of demands, for example, *assured site* for perimeter investigation.

## Electronic Intelligence (ELINT)

Electronics are part of life today and evolving at a fast pace to the extent by bridging integration with humans by remote controlling such. The clicking of the fingers or voice activation activates the automation of machines, and the IT and IoT (internet of things) increases the distance and range of remote control.

Sensors (ELINT) connected to this technology is used for issue alerts by way of alarm systems when intruders are detected or even by a flashing light when an object is identified by a metal detector or an x-ray machine.

Electronics can integrate with other mediums such as, with radar operated using an electronic controller (vehicle speed detector) with live viewing capabilities and can send reported messages. There are also electronic alarms that can be integrated with drones and could be automatically activated for perimeter security to identify and trace people, fires or any other reasons.

This technology applications are vital for a variety of reasons because we do need to follow the beast as it moves. The sensors that can be attached to such technology could indicate if a vehicle has had a collision or been stolen, a person that has just been highjacked or computers or any device for that matter containing valuable information that are being moved or being stolen besides devices that could ensure confinement (for whatever reason), for example ankle bracelets.

There are thousands of reasons why this type of technology could be used for distinct or for various purposes. These technologies could be reporting from time to time or real-time.

The triggering of an alarm and message sending the information to the AI controlling platform contributes information for machine learning and machine doing. The reporting system could give valuable information and evidential proof of the fact which could be highly relevant for any investigation or project risk management.

# Monitoring & reporting systems

The data extracted from all devices can be downloaded into incident reporting and investigation management software that should be integrated into the platform of the system. This is a vital component for investigation, vetting and compliance.

All practitioners know that data collection (intelligence) is paramount. The electronic realm can contribute pertinent information besides activating machine automation.

All technologies should have or be connected to incident reporting that serves as evidence of the fact. This data could provide valuable input for managing manpower. We can go deeper by using *crime or incident investigation software* for distinct purpose.

- The protocols that dictate the type of data from people or technology should be based on'' *all* the truthful information''.
- All the people involved in collecting and inserting the data at all levels must insert or code the information correctly.

The analyst could educate and/or experienced to find the unknown besides the known, therefore, what was thought irrelevant could become relevant.

Therefore, all data must be inserted. The analyst must be knowledgeable on the crime culture, and criminal methods in their location or field of interest.

Consequently, the equipment/tech is only as good as the users in acquiring the information, understanding the information and knowing what to identify to comprehend the patterns (modus operandi).

## Digital and Reporting Security

The information gathered may be required to build a case and therefore the evidence needs to be securely stored as well as copies made and stored elsewhere [7](Kirsten J 2019).

Keep in mind that the information contained on these technological devices is of high value in the protection of assets or the lives of people. Security protocols must be followed in every sense of the word.

In today's world of device hacking, cyber *infiltration* or *video footage manipulation*, it is imperative to ensure that whatever equipment or technology is used there must be prominent levels of encryption.

Furthermore, the password protection could be monitored to ensure that privileged users are the only ones to use such. These usernames and passwords find themselves being placed on other devices such as mobile phones which are just as porous and insecure as any main frame computer and deserve the respect for top level encryption.

## Authenticity, Installation and Usage

It is wise to comply with the technical instructions. Use authentic equipment because if the evidence must be presented then it will not serve the case at hand if the criteria is compromised, and evidence presented is denied.

- Practitioners and investigators know that they must have staff correctly trained on using the equipment and technology. *They also should know* (because of biological threat security) *where to check* to ensure that they are using authentic equipment.

Furthermore, the technology or equipment must follow the installation criteria and the correction usage of such especially when the evidence must be recorded or presented. *This is vital to avoid reputational damage.*

[7] Referencing Master Investigator critical thinking investigation (Kirsten, J)

# Triangulating the reporting of Tangible Resources

The technology sends reports to a central storage system and platform to be examined and analysed. The platform could present a visually presented or printed version of regular or irregular incidents.

The investigators would then analyse and consider what silo experts to involve that have their own theories or methods to comprehend the narrative.

There also could be security criminology-risk investigators that may use specific software that would extract specific information from the platform to discover and obtain evidence for building their case, perhaps to find new crime or uncover new issues of concern.

## Theories & methods

Once we have the intelligence information gathering framework integrated, we then have to analyse the information gathered from people by merging theories and methodologies.

These theories and methodologies assist in finding and identifying specific issues that impact the bigger picture

# Theoretical Intelligence

Multiple threats demand silo experts that use theories or different technologies that are based on their unique theories that will produce specific results. This means that each technology that is relative must be considered, be it for information gathering, incident or emergency management besides investigations.

Specialists in technologies use their distinct theoretical methods and investigative methodologies to obtain the necessary information for the incident reporting, crime investigation software or to predict risk.

## Multiple threats

Knowing intimately the threats in theatre could point the analyst to find an associated pattern of crime to look for.

With a pandemic or a war there is crime related besides crime related to outcomes such as, the economic meltdown.

This is where AI must excel. The problem with any emergency related threat is the reaction speed in managing such. *The faster the reaction speed to limit or mitigate the collateral damage - the better*.

When one intimately comprehends the threat then consider AI to assist.

- Consider the flow and behaviour of the population
- Research the type of crime and criminal methods that could be used
- Keep in mind the outcomes of the threat related to protect the profits because of the tailing threats.

# Methodology Intelligence

## Reporting and Investigation Management

Both machine and human providing or acting on the information results in part or as a whole, meaning that, an AI project could be by running totally on algorism or in-part could be reliant on the continuous human input.

Repeating the following reinforces *the importance that when people provide the reporting or information* then consider the following,

- A person may think that an incident is not important or something within the incident was not relevant and therefore did not add it to the reporting. Something that may not be relevant now could become truly relevant in the future. Everything must be reported. This is especially important and therefore use all means to remind the team.
- *Also keep in mind that people* lie, hide or volunteer information for a variety of reasons and therefore specific knowledge for governance management for such is needed to ensure a more secure data input.

Summarizing: By triangulating all the data obtained from all modes for intel gathering by using equipment, technology software and people on the ground reporting then one can comprehend the big picture. The software then serves for analysis and investigation that could also produce newly discovered knowledge by comprehending the threat and for designing protocols that could be used for distinct purpose.

Consistent monitoring of the reporting will inform on the behavior of the beast with which one is contending. This may point to technology considerations or other means to mitigate or limit the level of collateral damage.

All incidents are reported *regardless of their perceived value*. *Once the incident re-occurs* then one can conclude a pattern has begun. This incident must be immediately analyzed as to value the importance of such and also to be assessed with solutions considered.

*The various methods of gathering information* and comprehending the narrative framework [HUMINT (Human Intelligent) ] is outlined *in the author's other works* that will provide guidelines of 'crime' outcomes for triangulation research. (Security criminology risk investigation besides Critical thinking the master investigator)

- The analyst may need specific software in the reporting from the tangible resources to comprehend the narrative. When the system is reporting then it could match people with people or people with things on specific dates or places to follow the pattern by relationship building.
- They analysts may require Video Search addon applications: For example, by using applications to find distinct issues such as *video search technology*.
- There are 'addon' applications that can monitor, and video search a particular area, be it a pathway for example that can find a person/people or object/s on a particular day or activity for a period of time. This addon application for video footage or picture search is a necessary investigation tool.
- Addons for specific sounds or verbal confrontation detection may be required to comprehend the narrative.

Outcomes

- Knowing the true nature of the beast, AI must be realized as a living entity and living in-time with the daily innovation of technology or discoveries in intelligence gathering.
- Furthermore, must be programmed purposely to identify crime and criminal behaviour.
- Knowing that there is a difference between applications for incident reporting and criminal investigation software. Incident investigation software should be used for security investigation along with applications that display relationship trees (relationship connections with between people, people with objects or people involved in the same incidents).
- Then the practitioner needs to drive the concept with real time monitoring that produces alerts against flagged issues of concern
- When the patterns of crime and criminal behaviour identifies issues in theatre then appropriate and relative technology can be re-introduced taking the issues of concern into consideration.
- The practitioner then designs protocols to reduce the levels of collateral damage by selecting the technology, equipment or the layering of the workforce appropriately for the threats in theatre.

# Scenarios using the AI technology.

## Species of Beasts

When considering the *complete truthful nature of the beast* then one could consider the basic formula of what a person needs to hear, see, touch, and move (movement). Taste and Smell may not be required *unless drugs or explosives need to be identified*. *One must also consider how the beast moves in order to layer the workforce by character traits and skillsets*.

## Threats in theatre impact the selection of tools

The pandemic experienced and the economic meltdown also due to war has contributed much to the knowledge and stressed the importance of managing the *social movement* of people besides managing the *behaviour of people* and entry control to any site. Security manages aggressive and violent behaviour and therefore experience like impacting and deadly outcomes

### Scenario: Pandemic Control gave insights

*Definition: Active Biological Threat:* A method of transmission: *The eyes are just as porous as the mouth*. This is important to know because any volatile interaction could be a deadly outcome. Someone could shout and/or spit into another's face. Ensure *staff wearing eye protection wear <u>when they are alerted to address</u> the aggressive threat before the person enters the site.*

#### Environment

*People:* The audience are desperate, scared and could be over emotional so use a gentle approach.

*Tech:* Electronic thermometers can be used taking the environmental conditions into consideration which is giving the person time to climatize with extreme temperatures. For thermal imaging or fever cameras ensure that the are installed and utilized correctly. Below find specific reference points of note.

## Methodologies

### Appropriate Intelligence TECHINT and ELINT

There are various technology providers climbing on the bandwagon with those that are not providing the correct solutions for a specific application. There are also providers that are driving product with false information. This is due to technology designers that are uneducated and unaware of the characteristic traits of the threat and therefore highlight attention to specific unrewarding benefits or use wording that misinforms the buyers.

IPVM (technology testing group) is highly recommended to evaluate the brand performance  be it cctv technology thermal imaging and non-contact temperature detection besides other technologies.

There is also in your location, the Ministry of Health or departments aligned to them that set the criteria and standards for equipment and technology besides the installation and usage of such. The standards must be utilized in the security protocols for an active biological threat.

*Links to view*

IPVM (http://www.IPVM.com) FDA (www.fda.gov/medical-devices/general-hospital-devices-and-supplies/thermal-imaging-systems-infrared-thermographic-systems-thermal-imaging-cameras)

Note: There are manufacturers claim that their thermal imaging cameras or fever detection cameras are able to read temperatures and/or can view faces through masks. It is best to check the technology advances relating to knowing which technology is effective for reading masks (https://ipvm.com/reports/face-masks).

**Most importantly,** the technology protocols for installation can be located in all the above-mentioned websites and must be followed as prescribed.

***Masks, facial shields eyewear protection must be purposely detected*** *and flagged when they are misplaced on a person's face, especially when the person experiences any form of aggressive or violent behavior. As stated earlier, the eyes are just as porous as the mouth. This then can identify a person and situations that could are at or could become high-risk.*

Loophole: *if cultural attire is worn*, then it may not be able to read faces or temperatures. With distinct cultures the temperature must be taken by the same sexed person to avoid aggressive behavior.

Speed of development: This field is developing at such a fast pace, so it makes sense to keep watch on the progress of facial recognition or any devices used to measure temperature.

## Purposely use for biological threat security

As mentioned, the security industry **is managing the flow of people and the behaviour of people** besides ensuring that they sanitize. The technology must then be able to identify the above which could use trespassing over virtual boundary lines.

Verbal, aggressive behaviour or violent behaviour could be identified that could be recorded and relevant practitioners could be automatically notified using messaging system. There are apps coming into the market that can detect if a crowd being formed, people hitting each other, detecting people screaming, to mention but a few reasons. This should paint a picture of what would be required for specific purpose but then these are everyday threats now.

*Keeping in mind the crime related to the threat to avoid tailgating* with appropriate software or specially designed doors that are technology driven to not only ensure that people are not standing close but and most importantly to stop criminal intent associated to the threat which is *corruption or receiving anything through the backdoor.*

## Trace and Track internally to find crime

As mentioned earlier - in countries there may be legalities of privacy, so this needs to be explored. Human Resources could provide a list of people *that are on sick leave and may know the reason they are sick.*

*Reasons being*, not only could they be viral contingents, but also, they could be classed as *a high-risk insider threat with possible nefarious intentions. When someone is compromising their health, then there could be a no-good reason for being on the job.*

Furthermore, the AI incident or investigation software could track and trace the relationships that they may have or come into contact with by u*sing the appropriate and relevant technologies* (e.g., RFID on devices or tracking person using object monitoring, access control cards, video analytics with video footage searching).

## Crime related to threats

All the following examples specific technology and equipment, however this are more outlined in other works of the author.

Pandemic and Economic meltdowns related to war: We put both together because increased 'bad or desperate behaviour' will also increase the numbers of injured people that will need oxygen, medications, or any other form of medical assistance.

There is distinct crime related such as **corruption besides theft**. There is theft of PPE, medicines, oxygen gas cylinders and also being refuelled by staff or visitors especially at various sites, i.e., nursing homes, dentists, clinics and obviously hospitals. **There is such crime in all fields** of interest so best is to the reader to research/investigate their field of interest

There are more issues related below in other scenarios that will demand unique technology applications or AI solutions integrated with reporting and *fast actioning defence systems are required stop mobs in panic mode (state of emergency)*

# Impact on economic meltdown on Crime from War

## Current situation

The world economy having two threats being energy security and food security that elevate the cost for living will impact with millions being made jobless.

Millions of people will be unemployed and desperate for money to service their basic needs. This is when the insider threat from people escalates when one would think never that some people would never compromise their moral code but do because of their desperation.

The motivations for crime have evolved since the outcomes of Maslow' needs (1943) such as food, water, etc., besides wants (love attention acceptance) to *include today's needs* which could be asthma pumps for themselves or their children, actually all types of meds required for longevity of life or state of mind, drugs and drink for those with addictions, besides others mentioned within other related works by the author (biological threat security).

## Appropriate Technology

The technology discussing above the biological threat *may use some of the apps for specific reasons,* but the massive economic meltdown could demand that the apps are used for other purposes.

Consider for high-risk sites that organized and gang crime could maintain the same modus operandi in your location or there could also be an emergency of smash and grab that is happening elsewhere in the world that could playout in your location*. Then the s*oftware detecting people wearing motorcycle helmets could be denied access. The software could also lock the doors and message security.

*We must add that t*here could be specific sites or sites in certain locations where *gun-shot detection* would serve well to manage panic by either shutting doors or opening up the exits for emergency evacuation.

## AI used for 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

- notify appropriate people to respond thus not wasting money on irrelevant people that also cost money in transportation besides for their time.
- some 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 handling aggressive and violent behaviour and stopping it.

## AI protecting company secrets

People could resort to theft of company secrets

The above technologies for access control could be considered for good reason. Furthermore, use appropriate technologies to ensure such is cyber protected even information that one would not consider valuable such as the costing sheets and customer list. Also, keep in mind that the hardware (all devices and memory cards) containing the information is at elevated risk.

*Solutions:*

- Login activity of users
- Data download activity
- Keyboard stroke detection
- And obviously appropriate methods of protection for restricted area besides the security screening of staff within the zone.

# Other scenarios

When investigators complete their investigations then the final decision-makers are able to view the big-picture to look for patterns. This means that all may know that there is a pattern of crime but then what must then be done? This is where once again we can seek solutions where a complete AI system or part of the system being ELINT,TECHINT, DATAINT, COMINT besides OSINT (open-source intelligence) or SIGINT(Signals intelligence).

*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 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 such 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.

## Retail stores have experienced mob-theft.

Definition: *Mob thievery*

This is when people enter together, thieve openly and all walk out together. This is usually, high value goods where a crowd formation sensing application 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.

# Using AI applications for specifics

## Safe Containment of children and adults

The apps for anti-tailgating must be considered also to *avoid kidnapping.*

Using facial recognition software: children and people with registered escorts on the database may only enter and exit (facial recognition relationship detection). The matching of people with people by using facial recognition or additional technology can also be included such as anti-tailgating or entry control technology using RFID technology that could be embedded in a bracelet of sorts.

## Witness Protection High Security Containment

For law courts, perhaps hospitals if a witness is injured, witness protection accommodation or quarantine centers (for specific reason. The above safe containment rules apply besides, the 'facial recognition relationship detection, person down and the anti-tailgating' could make for a high-level form of security. However, RFID technology besides ankle-bracelets (GPS) could enhance the security even more so for various reasons.

## People slipping and falling

This may need to be even considered further when age is factored into the scenario such as a retirement village *or in a prison* when person is pushing another to slip and fall. Hopefully these scenarios will open ideas for many scenarios.

## Diseases and Conditions could determine apps required

Indecent exposure or epileptic fits, wandering patients, wheelchair toppling, people walking disorderly, perhaps drunks or disorientated patients, or any abnormal condition. This simply just gives an idea where the reader must research for either the technology, equipment or physical reactions for mental disorders that dictate room for concern.

## Community Assistance

It could be a good thing for databases of all sites that could identify missing children or people at any age and patients that may have mental disorders or wanted criminals. Specific sites could identify criminal behavior such as indecent exposure or monitor registered sex offenders.

## Anti-Tailgating Note: people <u>entering</u> as well as **<u>exiting.</u>**

*Having stressed intensively* this technology it must be mentioned to give the reader ideas of criminology-risk perspectives for example,

- 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 (anti tailgating with facial recognition of allowed and disallowed people)*
- Mental institutions, rehabilitation centers, nursing homes, retirement villages and schools to ensure *safe containment*. (Position outside going in and inside going out)
- *Restricted areas* 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 with facial recognition and direction of walking detection.

## Person Down, could be crawling or having a seizure

- A person call be attacked or simply could fall and unable to get up for many reasons such as, being injured, a stroke, heart attack, or an epileptic fit or seizure of some kind.
- Perpetrator/s crawling on mission (perimeter security) or on-site under the laser beams or radar.

**Note:** This technology should be installed in all buildings and streets or in any site where the health condition of a person could be compromised.

# AI assisting Specific Crime Detection

It is not the weapon that is the threat – it is a person/people. Identifying human behaviour will service well for many reasons. Sure, to find a person of concern weapon identification would assist tremendously however there may be more incidents related to aggressive and violent behaviour that causes just as much grief.

For greater insight into the reasons why people could resort to such crime in these times of multiple threats then comprehend that their basic needs related to themselves, and their family would compromise their moral code.

There are serious issues where nepotism and corruption will rear their ugly heads from ground level staff taking bribes. A solution could be by using Facial recognition together with Object monitoring that could pick up a security guard handing over something when they should not be.

*Depending on the nature of the beast* for *a particular AI project* one may need to know about finding the silent victim or being bullied to identify the insider threat and to determine if they are working in concert with transnational and local organized crime besides gang crime either voluntarily or under duress.

This knowledge then dictates that manpower and *incident, or investigation management software* 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 method.

This booklet outlined 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.

One may have a distinct field of interest but still one has to critical thinking situational awareness because all professionals must comprehend their unique situation.

Practitioners in this field keep their eye on the ball by watching the news for crime in session in their location or field of interest besides specialist groups. Against this backdrop, it is apparent that the security and investigation community must be fully aware of the criminology-risk to know what to look for and to consider various remedies to limit the level of collateral damage using technology and layering the workforce by skillsets.

Obviously, oversight would investigate or use the same for governance and compliance management to determine specific criteria has been kept.

# Transferrable methodologies

Different job functions can use the same incident or crime investigation software reporting system for a variety of reasons:

- There is crime in all professions and job functions
- Crime or incidents could have occurred in one location or field of interest and mimicked elsewhere.
- The person responsible for oversight and compliance for any department besides security, investigation, incident management, risk management, emergency and disaster planning besides health and safety *that could use the same software for their own objectives.*

*Other Departments (**note** that security measures must be considered when allowing other departments partial access or not to have any access to the security system or the information obtained by security.)*

Financial Department

- The accountant could use the security guard-force management systems to determine the working hours in relation to sick leave, clock and in/out besides using the system to invoice the system clients.

- The accountant could work out the financial implications relating to loss of profits resulting from specific crime. Keep in mind that there is a difference between loss prevention and profit protection. For example, incidents could occur where money cannot be recuperated because there is no insurance for damages related by incidents that cause reputational damage.

- The financial department also use the software for their field of forensic investigation and may need to identify crime and to gather evidential proof. They do have oversight and governance management by the Auditors which may give peace of mind to security however it may be wise to restrict their access. (This is debatable).

- For in-house security services, the accounting officer could have access to a specific part of the security management software only to use extract information from access control software to determine the salary payments of all company staff and not only the security teams.

Human Resources HR.

The same security access considerations for the amount or type of information shared with HR. For argument's sake, let us say a person was hired by nepotism and they became a person of concern then HR should only be made aware when charges have been instituted.

- This pandemic may have brought to HR situational awareness with assertive actions to be taken. Staff must not be in the space of people that are shouting, verbal assault or any form of aggressive behaviour.

- The HR department could use the incident information to consider what skillsets need to be employed or what type of person besides their qualifications that should be employed, deployed in other departments.

- The 'Security HR' needs to strategically and deliberately layer staff by character traits and skillsets or to consider upgrading or acquiring distinct training resulting from the incidents that occur.

- *Incident reporting of Staff*: When staff are off on holiday leave or sick leave then security should be notified so that any visitation to the site during that period by those staff in particular could be for nefarious reasons. This is to avoid any form of theft if the person of concern may be fearful that they would not survive their illness and may need to obtain funds by reselling assets, for example, company secrets.

- From the sick leave reporting or deaths incurred the HR may need to consider employing temporary staff or cross-skilling existing staff in order to retain resilience. They could provide the financial implications to the accounting department.

- If HR notices staff that are in distress because of insider threat or by visitors, then HR should be notified so that the person can be monitored along with another or others within the site using the technology. At all costs reputational damage must be avoided.

Marketing Department

- The traffic flow would be of tremendous interest to place advertising material effectively besides for layout design.
- The behaviour of the shoppers could give good insight for many reasons which the marketing professional should know.

Safety Officer

- Could identify compliance criteria that is relative to field of interest.

# Guidance Project Sheet

- Describe the full and complete nature of the beast 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).
- What is the crime related to the above or other issues or concern?
- 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?
- Describe layering the manpower by skillsets for the scenario in the field of interest.
- What is required in the incident or investigation software to identify flags of concern?
- What knowledge and skillsets should an analyst 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 many reasons besides the crime related to the location or fields of interest besides other considerations for example, environmental conditions.

# Eating this AI elephant

To understand the size of AI and how it works in your field of interest could be like eating an elephant. One could eat an elephant by using technology and manpower by way of placing the elephant into a huge fridge (tech) and then eat bit sizes (manpower) for an extended period of time – depending on the number of people eating.

Quicker than you think!

By using the tools as prescribed in HIM and paying attention to the knowledge provided then the user will 'get–it' quickly!

Also, by using the HIM Tool and following the method prescribed herein could get to know how to read people, the situation, where to look and what is required to limit the collateral damage.

**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. All relevant material and skill development can be located on HIM Human Investigation Management.