# AI

## For Security Emergency Management

Reaction speed is key!

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

# The Formula

'Security success depends on the level of situational awareness of the people on the ground (all are decision-makers) and their reaction speed' (Juan Kirsten 2018)

In using the SPI formula, technology must identify a person in distress and alert relative people or activate counter measures. When every minute counts then the associated technology should be auto responsive.

## SPI: Situation, Position and Implications (Juan Kirsten 2015)

## Situation

All security practitioners manage incidents on a daily basis that could easily turn into an emergency. They are the ones that manage life impacting or deadly outcomes and therefore are in a constant state of pre-incident preparedness and reliant on technology besides their skill sets.

There are multiple global threats in theatre resulting in a deeper global economic meltdown with millions of unemployed and desperate. This in-turn will generate increased crime on all fronts besides riots and demonstrations. Consequently, there will be more incidents that can shift into emergency management besides the crime increasing the number of investigations. The security industry will rely more on using technology.

## Position

Using technology and workforce to identify the threat and react speedily. Reaction speed is vital.

## Implications

Life impacting or deadly incidents

## Highlighting

Before we go into describing methodologies, it is important to stress basic considerations for using AI for emergency management because we need to address important aspects such as the evacuation and crime impacting emergency management.

# Crime creating emergencies

Security practitioners take this very seriously for many reasons. There are times when perpetrators take advantage of the situation and could attempt to hack or trigger the emergency system. This is especially important if the doors are programmed or triggered to open automatically for any reason.

The system must be secured with high encryption security software (AES or Triple Des) besides the control centre must be secured with effective access control using all means, for example using all means restricting access to unauthorized people.

# Evacuation Control

AI can assist to ensure when an object is placed in distinct areas that would impact the exit flow throughout the site besides outside the site where the exits must  free of obstacles regardless of size. Object monitoring inside or geo-fencing outside needs to be enforced by way of immediately alerting the security ground force to ensure removal of such. This protocol must be adhered to, because an object could be large and may require many people or lots of time to remove such.

# Monitoring and Reporting

*Reporting and monitoring is vital.* The data extracted from these 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 besides vetting and compliance. *View AI merging technology and manpower for security criminology-risk investigation.*

The above is a shortened version of the AI for security criminology-risk investigation to know what it is, how it works and how to get the most out of it.

# Hotspots to prepare for various emergencies

*A global issue could impact all countries and the people on the ground besides job functions.*

- All sites and logistic chain that hold any product related to the basic needs of man is high risk example, food, alcohol, medicines, etc.
- The above also relates to sources of energy be it petrol or natural gas.
- Sites handling cash, jewellery and weapons.

To give an example, a basic need of man would be oxygen because oxygen is obviously required during a pandemic and also during anarchy or a war. Any compromising of this life-giving ingredient could lead to aggressive and violent crime besides organized crime getting involved in the logistic chain.

The crime related to economic meltdowns could also be impacting on a larger scale because of panic buying, along with mob assault on various sites. The type of crime that could manifest from criminals or desperate people during a state of economic hardship could lead devastating outcomes.

# What constitutes an emergency

A person having a stroke, heart attack, seizure, or any other physical illness makes sense when thinking emergency.

Let us consider the answer to the question that if someone is being kidnapped, raped, or violently abused – is it a security emergency? Most certainly, just as if the person or group is attempting to penetrate a site would constitute an emergency.

When any of these incidents or crimes take place on a site then the reputational damage could be devastating to the stakeholders.

Security staff would then use the technology or equipment besides the workforce to protect the site besides contact the authorities and could be the eyes on the ground giving intelligence on the situation.

Security Practitioners are advised to keep their eye on their local criminal stats or other issues of concern in in their location or field of interest. Being kept informed should prepare the security practitioners for a high probability that could lead to emergency status.

# PSIM & VMS

Physical Security Incident/Investigation Management systems and Video Management Systems can be used as the control panel. This a central controlled system that integrates technologies besides the reporting from the ground by staff. Once an incident occurs then it could lead to emergency management subsequently there must be an effective method of communication between ground floor staff and the controllers.

Obviously, predictive security research could reduce the number of incidents that could lead to emergencies.

One must consider a multitude of considerations related to designing, purchasing and using the PSIM and VMS technology system. It is the security criminology-risk investigator that must know the criminology, crime culture, and criminal behaviour to comprehend where, how and why technology will work.

The IT world simply make the technology. The integrators or installers and must install according to instruction criteria. When selecting an integrator or installer then it is suggested to validate their knowledge. They may refer to past clients or projects that they have undertaken. This does not mean that they have experience as there was a security practitioner that provided them guidance. For example, the practitioner could require a strong perimeter security system. However, the security practitioners in another location may be more educated and state that they require not only a strong perimeter but things that are just as important such as a system that also could inhibit drones flying into the perimeter. That sounds as if it easily makes sense, but it may not have been mentioned in the project management sheet that was provided. In other words, if the system integrator or installer asks what type of crime, they need to litigate then it displays that they could be more knowledgeable. They may also suggest specific technology for other crimes or concerns besides reasons that the buyer never considered, such as profit protection.

# Using AI reduces false alarms

Technology can identify something and make decisions to ignore or alert an action be it emergency protocols. Filtering out false alarms saves time, effort and money especially when the workforce is deployed.

Another benefit is when the AI identifies an issue then time is saved by notifying the appropriate people to respond which in turn saves lives. Every minute counts.

## Situational Awareness using technology

True AI is machine learning and machine doing. There is technology that filters false alarms by way of recognizing visual, audio or motion detection and alters the alarm sequencing. In this way, the technology can distinguish for example,

- between a car back-firing and a gun shot
- a person carrying a trumpet and a bazooka
- recognising a group of people with their hands raising and clapping or a group of people putting their hands up and standing still.

# Technology and equipment fit for purpose

*Learn from the pandemic:* The protocols set by the security industry dictate that the technology and equipment must comply with the health regulators (e.g., thermal imaging, fever cams and electronic thermometers by the FDA or any such body in the location of interest). This includes the installation and usage of such. So, when IT offers this equipment, technology or apps be sure it complies with the protocols set by the ministries of health.

*Brand Performance:* There are laboratories or investigative journalist that check the brand performance and compliance for technology besides their claims in their sales literature. Any contravention could lead to reputational damage. (Check IPVM.com)

The IoT of things connected for access control, perimeter security, industrial temperature detection, fire or smoke detection other devices must be verified and fit for purpose according to their own criteria for governance.

# Technological Applications can trigger emergency

The biggest nightmare for any professional is not knowing there is a situation in theatre that should be managed as a state or emergency. Technology can notify the necessary stakeholders to activate emergency status. There could be sites that could experience the wrath of a *'Population in Panic'* or *'Terrorism'* which dictates that the same technology would be required.

Holistically speaking we should focus on human behaviour identification in aggressive mode or in distress, which could be human down, being attacked or kidnapped, to give the reader the idea when considering a 'must have list as all of these issues demand emergency response.

*Human-down* is when a person falls the ground and motionless, crawling or having a seizure. The technology should also be *focusing on the front-line staff* at any site where they could be located internally or on the perimeter that could be involved in any scenario relating to aggressive or violent experiences. One must consider that also human traffic flow could contain people at any time that could faint, have an epileptic fit, heart attack, or stroke besides other physical ailments that are life threatening. Therefore, this technology should be installed on all streets and within all sites.

Keep in mind that the technology must be able to *distinguish* between the various positions, movement and timing of a person on the ground to reduce the false alarms. For example, there could be a cleaner on the ground or a person in crisis to reduce the false alarm.

*Facial Recognition Relationship Detection (matching people with people)* is used for high security by the faces being registered on the database of approved or disallowed.

- Anti-kidnapping. By matching people with people. Adults or children escorted by unknown people or known people that have been disallowed.

- Counter human trafficking by uploading pictures of missing children or adults being escorted by unknown people.

- Avoid escapes from prisons or any containment sites when people are escorted (e.g., witness protection, the mentally unwell, etc)

*Facial recognition and RFiD Tagging along with anti-tailgating for anti-kidnapping:* Maternity Security of New-born children with mother to child RFiD tagging.

*Anti-Tailgating* whereas people break the social distancing regulations. *This is also of service to,*

- accommodation for the elderly or places of safety for the mentally unwell where the anti-tailgating must be *deployed for incoming and outgoing to litigate escapes.*

- rehabilitation wards or centres for alcohol or drug addicts.

- restricted areas that could contain medicines, oxygen supply or assisted breathing equipment besides any other asset that contains such high value assets that desperate people would need and security control rooms.

- Research laboratories, quarantine sites or hospital wards

- Reinforcing, one must always keep in mind **that all sites need** to litigate stalking, rapes, kidnapping, and murders.

- This is also used to reduce corruption or theft whereas goods could leave the premises by an employee or people provided access to the site especially during panic-buying during an economic meltdown or lockdown for any reason including unrest.

- *Crowd formation detection* where a limited number of people must be in a space and when such is outnumbered must summon an action by technology shutting doors or manpower deployed.
- Control a population in panic-buying mode

- *People flow monitoring w*ithin a mall or building. 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.

- 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 (Object Monitoring).

This above could mean that *people counting technology* could be used or we could go further depending on the field of interest or location. Additional indicators may need to be added for visual, audio or motion detection. For example, if the people 'in-sight' are running or carrying something.

*There could be countries may experience acts of terrorism or crime*

- Security technology and equipment could assist with an active vehicle assailant by stopping the vehicle and limiting the collateral damage.

  - Gun shot or seismic detection software could activate the opening of access or exit points besides locking the site down.

  - Weapon detection could be included

  - Also, defensive actions using non-lethal means by way of, automating defensive and protection equipment such as, door closures, deploying security smoke, pepper vapour spray or arming electrified fencing.

  It is suggested to read all the other work of the author for good reason such as on how to the most out of using AI and relative applications to litigate different crime.