Security Investigators & Threat Researchers use Digital Investigation Tools

The tech is only as good as the user's critical thinking ability and level of situational awareness.

IT'S HIM HUMAN INVESTIGATION MANAGEMENT

Introduction

This document refers to current threats that require technologies and human intelligence to predict or find the crime and stop it- protecting sites and saving lives.

On social media people ‘telegraph’ their intentions, emotions, abuse, and their loyalties to the world. In other words they display their religious beliefs, moral code or political affiliations.

The reason why the word ‘telegraph’ is used above is because not only are words used but also people click the like, dislike or on an emoji. They display how they feel about something that is on the picture or video clip which could be, someone burning a flag, raising the flag, abusing or hugging others, painting graffiti on a building or statue, just to mention but a few.

The technologies can assist greatly for example, when the digital investigation tools match people with people or people with objects. By specific technology, one could scan images of someone or something which could be masked people or people carrying specific flags. This practice then could be used to find social groups that are supported by various people that in turn could lead to further investigations.

The above scenarios display that various or a variety of technologies or resources should be used at the same time which is required to mitigate the challenges of today.

One of the x factors is the biggest nightmare which is not knowing what is truly happening on the ground and such can be discovered through digital investigation because the internet is mankind’s greatest ‘living’ information resource.

At the end of the day, the scenario painted above is our reality. We are living with social media, the evolving technologies and in a state of unrest and disorder. The Researchers or Security Investigators need to adopt the mentality of surgeons for professional development. Those studying surgery that are not adding robotic surgery onto their curriculum will be made eventually redundant. Use the educated workforce and technologies to find the crime and stop it - protect sites and save lives!

Considering

A. Whatever happens in the world could impact different countries, the job functions and the populations. This means to some that there are certain issues related to migration that impacts polarized neighborhoods to which some may consider something as a crime and others do not.
B. We consider two bundles of technologies. One for location and the other for field of interest. We could use one bundle for a certain function, perhaps a mixture of both or just the other on its own for a specific purpose. Sounds complicated but you should be able to distinguish them easily after reading about them herein.

Cleary know your Job Function

Security is in a constant state of investigation regardless of title. Security personnel manage the flow and behaviour of people besides finding crime and stopping it, as well as, protecting sites and saving lives.

This example demonstrates that knowing the job function gives the security sector direction and in particular the researcher/investigator specific missions to focus on related to the location or field of interest. The practitioners should consider two objectives namely,

- What is happening in the ***location***: countering common [holistic] crime (Rape and Murder, Hijackingi Abuse, Kidnapping, Woman and Child Exploitation, Corruption, to mention but a few)

- What is happening in the ***Field of Interest***: investigating and countering distinct crime besides risk concerns to a particular sector

  There is distinct crime in each sector be it a hotel, polarized neighborhoods, border control, critical infrastructure or even businesses for example, vehicle repair workshops.The focus could be on identifying known crimes or discovering new crimes using specific knowledge and skills that need to be mitigated or to reduce the collateral damage.

Using Digital Investigation Tools

According to the Google AI description ‘’Digital investigation, often referred to as digital forensics, is the process of identifying, analyzing, and reporting based on digital evidence that could be found on electronic devices and systems’’.

The Author of this document suggests ‘’Use different tools for digital investigation for specific purposes or the same tool for different reasons’’.

In the book ‘Security and Criminology Investigation’, the Octopus describes a methodology of integrating or fusing different technologies to comprehend the narrative (big - picture).

The security criminology-risk investigation personnel would focus on their own sites and/or clients for drawing intelligence through the security system PSIM (Physical Security Information Management) or VHS (Video Management Surveillance) that connects various technologies together. Let us not forget that they would also rely on HUMINT (Human Intelligence) besides the technologies.

When connecting physical security technologies with digital investigation besides cyber investigation with a reporting system then the all-in-one system makes for an incredible intelligence driven proactive tool.

HUMINT - DATAINT - COMINT - SIGINT - TECINT - OSINT - PSIM -VHS -REPINT (reporting intelligence)- UAVINT besides others that could be required or newly discovered.

Above is simply an outline that the main decision-maker could need specific information to employ an investigator that is skilled with all above mentioned relevant tools or summon silo experts from one or all different fields for distinct purposes to secure or investigate the asset.

Subsequently, we may need to view the perimeter security records along with the cctv and access control technologies besides verifying the personnel. For example, HR may need to ensure that workers must have background checks when considered for employment and perhaps a lifestyle audit from time to time could be necessary. This means that the HR could employ a silo expert or hire a OSINT professional besides a specialist in background checking the potential candidates so as to mitigate the insider threat.

DO NOTE that it is legal to extract published data off public sites however it is illegal to hack sites to extract information on people.

At the end of the day, when it comes down to community/neighborhood or on-site investigations then the silo experts that are related could be an in-house security investigator or outsourced expert and must have experience related to security investigation because they need to find specific crime that they are knowledgeable with or have the critical thinking ability of finding crime that they have never seen before by using what they do know.

Use Authentic Digital Evidence

If for any reason the digital forensic evidence was recorded by some CCTV manufacturers which have been banned from government websites then consider that any evidence from those brands should not hold up in a court of law. Do check with laboratories such as IPVM. Consequently, the same rule should be considered for any form of technology that is used to secure evidence.

Furthermore, when CCTV tech is banned from governmental sites because of FIST *for the Private Sector* then the argument is sound and the forensic evidence is tossed out in court because the evidence could be extracted, then doctored or manipulated deeming it unreliable.

Securing the integrity of the evidence is crucial. It is suggested that besides keeping a backup, it would be wise to make two extra backups onto any medium and safeguarded in different physical locations.

It goes without saying that the evidence must have the latest or better yet encryption endorsed by recognized encryption standards.

Analysing and Reporting

AI could assist greatly in identifying patterns or pick up on an irregularity which should be reported on. The reporting could be transmitted to the main DATAINT capture or the reporting by some technologies could be by messaging appropriate personnel especially during an incident or for emergency management.

We must keep in mind the x factor in analytics. The narrative is built on a situational awareness framework. When something is not taken into account then the analytics are out of sync. We need all the truthful and reliable information to not only build but also to comprehend the narrative.

The instruments are only as good as the critical thinking ability and level of situational awareness. At the end of the day, an intelligent person knows that they need knowledge and skills to comprehend intelligence.

Security using Digital Investigation Technologies for this moment in time

As stated above, ‘’what happens in one part of the world impacts all of us’’. During such turbulent times all investigators need to fully comprehend the narrative and comprehend the impact on their location or the field of interest. Subsequently, some threat research resource agencies are fit for purpose. It is strongly advised to fact check from time to time.

Besides relying on outsourced threat research resources detection services, we must nevertheless rely on HUMINT (Human Intelligence) on the ground. This could be from our own staff that need to provide all the truthful information to the team or it can be from the ' ‘intelligence analysts’’ that use specific threat detection software or intelligence service providers.

The Digital Investigator’s Head Quarters or Home Base.

The security investigator's workplace should be the first place to start to uncover issues of concern that could be happening under their own nose in your work place (control room) because it is the head of intelligence’s premises. For some, the control room could be the first evidence capturing or evidence storage point.

The most important thing is using different or should one say appropriate technologies for digital investigation. Subsequently, ‘applicability’ is the relevant thought-process for digital investigations *especially during unrest or war-times taking into account policing agencies or government institutes. There are some technologies that are banned from government sites for good reason. Understand that personnel could visit any other sites that contain the banned technologies. Therefore, be aware of FIST (Foreign Instrument Surveillance Technologies)*

Digital Investigation and Digital Evidence Security

It goes without saying that the devices used for investigation must be considered such as mobile phones, laptops besides CCTV which was addressed earlier.

Again, we should be aware of FIST (foreign instrument surveillance technology) as they contain algorithms that could contaminate and action the opening of doors, windows or shut down the power supply besides having cameras (eyes) and voice (ears). Evidence could go missing or be manipulated. Consequently, keep yourself in the loop regarding security of the entire eco system besides training the team.

Current Threats should invoke digital investigation to counter many issues.

Pro-Revolutionary and Pro-Nationalist rallies should be digitally monitored from the beginning to the end. In other words, the monitoring should begin at the first meeting point. Certain demonstrations could be hijacked by a gang of sorts under the guise of some mission for the sole purpose is to loot, maim or kill others. When such is identified then appropriate measures could be activated.

Researching and investigating all technologies to achieve certain objectives such as using the technologies to identify crime besides mitigating various threats for example, counter corruption, counter terror for this moment in time and others related to security or for that matter other fields of interest because there is crime in all sectors.

The booklets referred to in this work 'Security Criminology-Risk Investigation using technologies and the workforce, 'Using AI and Technologies for Security Criminology-Risk Investigation, Critical Thinking the X Factor in Criminology, Security and Risk (Vol3), Security and Criminology Investigation Management(Vol4), Critical Thinking in Investigation(Vol5), to which all are endorsed by various organizations. Authored by Juan Kirsten for HIM Human Investigation Management.