The Future of Global Security Operation Centres

“It’s time for a re-think on the future of global security operation centres”

E. info@icetana.com   P. +61 8 6365 0458

AUTHOR - ANTHONY JONES (ICETANA CHIEF INFORMATION OFFICER)
01. INTRODUCTION

The modern Global Security Operation Centre (GSOC) is a marvel of technology. Often, they are setup with dozens of flat panel screens displaying maps, operational information and video feeds from all corners of the assets they are designed to protect. Unfortunately, much of this technology is focused on the perception that if operators are presented with more and more video feeds then they will be more productive.

The reality however, is that the majority of the data now flowing into control centres is irrelevant and serves only to dramatically increase the operator fatigue experienced by operation centre staff as they struggle to identify events of interest amongst the myriad of video data.

In this paper, we will look at breaking the paradigm that more is better in terms of the amount of surveillance data presented to operators. We offer alternative modes of operation that can be applied to the contemporary operations centre to improve incident detection rates, engage operators and improve overall efficiency of the key components of security, safety and operations.
02. THE CHALLENGE
RISK ENVIRONMENT

We live in a chaotic world with an ever-changing risk environment. The key drivers of this are technological obsolescence, emerging new technologies, changes in man-made threats, cyber security, and climate change that have combined to create our current global dilemma in which it is simply not possible to predict or to pre-empt every risk that may eventuate. Many major incidents in history and/or asymmetric violent attacks have been attributed to a “failure of imagination” [Ref. The Final Report of the National Commission on Terrorist Attacks Upon the United States: Executive Summary - 2004-01-27], the concept that something seemingly predictable and undesirable was not planned for.

In many instances, the solution has lagged the problem. The typical reaction as a result of the impact of undesirable events is to place additional cameras at the scene of the crime. The belief is that this will assist security operations by gathering more data resulting in greater situational awareness and better support to decision-making processes in the future. The reality of this, however, is a decrease in overall situational awareness due to the aggregation of enormous quantities of irrelevant data effectively lowering the signal to noise ratio. Meaningful data is drowned out by the sheer volume of additional data that covers every day activity and as a result important events are routinely missed as operators continue to search for that “needle in the haystack” [Ref. Velastin, S.A, Boghossian, B.A., Vicencio-Silva, M.A.; A motion-based image processing system for detecting potentially dangerous situations in underground railway stations. In: Transportation Research Part C, pp. 96-113. ELSEVIER, (2006)]

This is not to say that the additional data being recorded is not useful. While CCTV cameras have proven a poor deterrent in most cases [Ref. Velastin, S.A, Boghossian, B.A., Vicencio-Silva, M.A.; A motion-based image processing system for detecting potentially dangerous situations in underground railway stations. In: Transportation Research Part C, pp. 96-113. ELSEVIER, (2006)], the additional camera feeds mean that more data is captured for post review and analysis. What this usually equates to, however, is retrieval of video to support court inquires for supporting video evidence in an attempt to prosecute offenders.

To further exacerbate the issue, modern operation centre staff are often encumbered with additional responsibilities such as responding to fire panels and control system alarms, ringing telephones, dealing with onsite contractors, visitor sign-in registration and/or other administrative and operational tasks [Ref. Keval, H. CCTV Control Room Collaboration and Communication: Does it Work? Paper. London: University College London, 2006.] It is no wonder that events are missed [Ref. Ainsworth, T., 2002, Buyer beware. Security. Oz 19, pp. 18-26].
“...Important events are routinely missed as operators continue to search for that “needle in the haystack”...
Artificial Intelligence (AI) is any technique or technology that mimics human intelligence in performing a task [Ref. Russell, Stuart J.; Norvig, Peter (2009). Artificial Intelligence: A Modern Approach (3rd ed.)]. In recent years, the development of AI computer systems has progressed in leaps and bounds. We are now in the age of robot vacuum cleaners, voice activated assistants, and even driverless cars. More and more we are seeing the application of AI technology enhance the way we communicate, work, play, and travel.

Advancements in faster and more powerful computing technologies such as Graphics Processing Units (GPU), Field Programmable Gate Arrays (FPGA) and Application Specific Integrated Circuits (ASIC) provide the computational horsepower to enable devices to process vast quantities of data, produce meaningful information from it and use the results to direct a course of action.

AI methods such as Machine Learning (ML) and Deep Learning (DL) in real time are now possible and we are seeing a massive proliferation of this technology throughout our everyday lives.

Rapid advances in technology mean that we are getting closer to the development of systems that are able to analyse and understand large quantities of data in real-time. We have already seen the application of AI technologies to the security domain in areas such as people counting, biometric analysis and object detection and classification algorithms.
These systems are becoming increasingly pervasive and we are becoming ever more reliant on this technology in order to secure our facilities and domains.

The technology still has many limitations, however. Whilst these systems have improved and proven to add value, they address only threats that are well known, understood and expected. The problem with these systems, however, is that often it is the context that dictates whether a particular situation is in fact a serious threat, or an innocuous event.

While computers are very good at processing, analysing and characterising large quantities of data, they are still unable to provide the context that a human operator brings. To date no technology surpasses the ability for humans to apply their understanding and context to events. AI technologies still currently fall short of the powers of intuition and ability to reason. With current technologies and for the foreseeable future, the most powerful capabilities are made possible when AI technology is used in conjunction with human context and understanding to inform the decision-making process.

In this way, AI technology can be used to filter out the noise from important information in large data sources, link together related data and provide only the relevant details to a human decision-maker in a timely fashion.
The use of AI technologies in a security operations centre is a logical next step in GSOC evolution. AI technologies will enable the massive amount of information such as video feeds coming into the control room to be analysed by a machine converting this vast amount of data into meaningful information.

An example of how AI assistance can be applied to the GSOC is with the incoming surveillance feeds. As described in the first chapter, a typical operations centre may have thousands of camera feeds being piped into the facility. These feeds can be categorised into two groups. Firstly, the majority of the feeds are displaying everyday usual activity such as people going about their daily business, normal road traffic and empty spaces. These feeds are of essentially no value to the operations centre.

The second category of feeds is the more interesting group, and may represent a minuscule fraction of the entire surveillance operation. In this category of feeds, things are happening that need to be seen and assessed by the operations centre personnel. This group includes activities that are out of the norm, for example, trespass, loitering and suspicious behaviour, equipment malfunction, etc.

AI assisted video monitoring can be applied to this particular scenario to allow surveillance system operators to focus on the latter group of feeds thereby putting their focus where it is required. This increases situational awareness of unusual activities throughout the facility and serves to dramatically improve incident detection rates. Furthermore, the flow on effect is that important events are detected sooner, incident response times are dramatically lowered and events are able to be dealt with before escalating into major incidents.
In addition, once unusual events have been identified via AI systems the GSOC gains the ability to change operational processes and resources to prevent these events from occurring. The efficiency not only of the GSOC, but the entire security operation is significantly increased as resources can be applied in a more targeted and timely manner. The GSOC’s mode of operation shifts from one of reactive surveillance to proactive operations.

A secondary side effect of the fusion of man and machine lies in the efficiency of GSOC personnel themselves. The quantity of feeds that they view is dramatically reduced, and the focus of these feeds is unusual or interesting behaviour. This serves to improve operator engagement and elevates their skillset to that of risk manager, rather than CCTV operator. Modern security operations centres are manned by highly skilled personnel that focus on risk management rather than the day to day tasks of recording, archiving and retrieving video footage.

AI technologies can cut through the noise of the control room, eliminating the need for cluttered screens showing irrelevant video feeds and replacing them with shortlisted views showing only potential threats to the organisation. Operators will be able to focus on this information presented, make an assessment in real-time of threat using their own context and reasoning and note pre-cursor events and / or enact necessary measures to eliminate or mitigate the risk.
05. THE FUTURE

The progression of development from basic Artificial Intelligence to Machine Learning to Deep Learning techniques will have big ramifications for future global security operations centres.

ML gave computer systems the ability to learn and categorise security data. Deep learning techniques applied in real-time will give computer systems the ability to truly understand what is happening throughout the assets that we seek to secure. Once we have achieved this level, it is likely that computers will be able to automate the response to an event, ensuring that incidents are responded to in the most appropriate and timely manner possible.

For example, automated systems may take in fire alarm, video and audio data, analyse and cross reference and instigate a turn out from a firefighting team, a security response team, and police without operator intervention.

This does not signal the end of the security operations centre personnel, however. Ultimately the responsibility for response to a threat must lie with a human. Human context, reasoning and judgement plays a critical factor in securing our assets and protecting life, property and reputation.

Rather than being made redundant, security operations centre personnel will also need to adapt to the changing technology risk and threat landscape by upskilling their risk management, threat analysis and incident management skills.
06. CONCLUSION

We are already seeing the kinds of transformations described in this paper throughout security operations centres across the globe. This is in response to the ever-changing threat, and a desire to detect and respond to threats that we could not possibly predict.

The enabler for this transformation is the implementation of advanced AI assisted technologies. In particular, the implementation of AI assisted video monitoring has been proven to enable the transformation from a reactive surveillance operation to a proactive surveillance operation.

This paradigm shift in global security operation centre operation is essential to improve situational awareness, efficiency and the ability to adapt to the modern threat landscape.

As the threat landscape evolves, the future global security operation centre will also be forced to evolve. This can only be achieved by implementing more advanced AI assisted technologies to equip the control rooms greatest asset, its personnel, with the tools needed to tackle the contemporary risk environment ever present in this day and age.
REFERENCES

REQUEST A CONSULTATION

APAC
T: +61 8 6365 0458
info@icetana.com

AMERICAS
T: +1 (949) 798 5787
info@icetana.com

MEA
T: +971 56 691 1659
info@icetana.com

UK/EU
T: +1 (949) 798 5787
info@icetana.com

www.iCetana.com