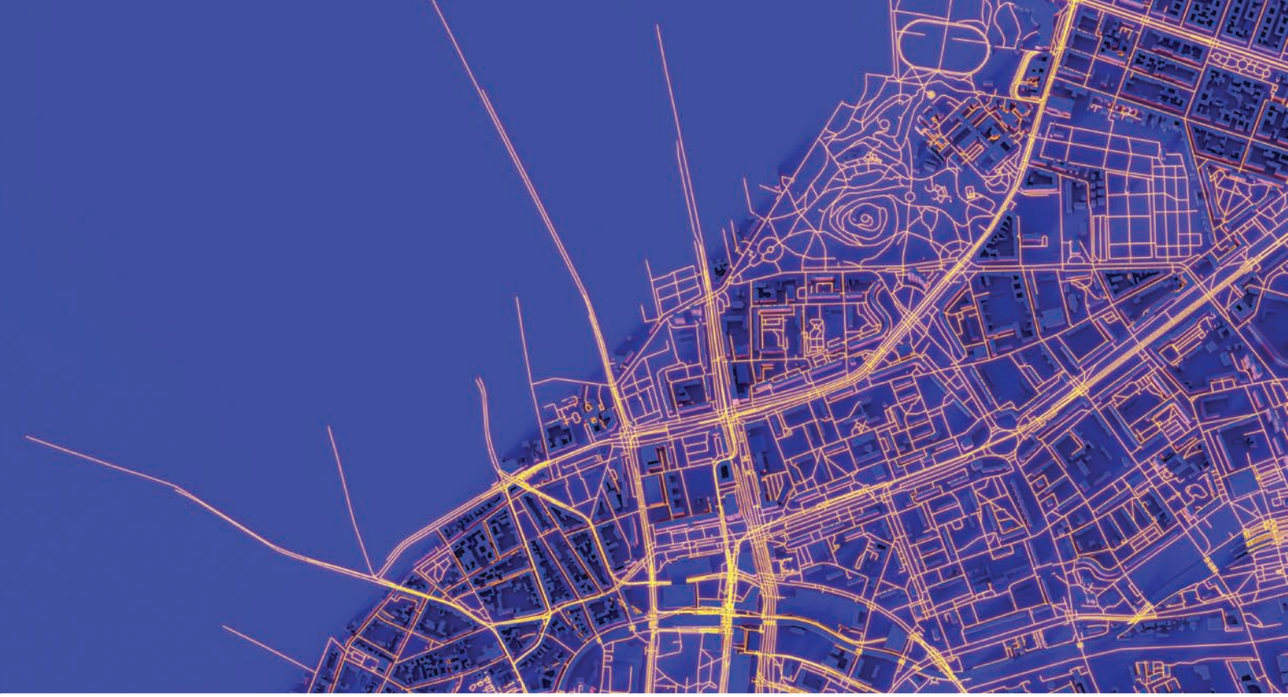
Technology:
The bridge between civil and military planning



Tostphoto | Adobe Stock

Adam Berry of CRJ Key Network Partner Initsys describes how military processes for crisis management can be applied to a civilian environment, with the assistance of technology

Following processes printed on paper is a thing of the past. Automated scripting eliminates mistakes and allows operators to focus on what is important. The processes behind managing a crisis have become critical in military and civilian environments and, in this article, I will look at how both automated scripting and making the best use of available technologies can vastly improve and speed up crisis management, as well as helping to eliminate errors and the element of doubt.

In the military, failure to prepare is simply not an option. Plans must be put in place for every eventuality, including what to do if these plans fail. As such, Armed Forces across the globe have developed processes for dealing with a crisis, and these can be applied to help businesses deal with a major incident, or to tackle something as seemingly trivial as a burst pipe in a village.

The recent wars in Iraq and Afghanistan, and the type of warfare experienced by the militaries of the many nations involved, have revealed a need to develop crisis strategies to deal with events of varying severity.

Recently, I wrote an article in the *Crisis Response Journal* about how Merlin deals with the very modern threat of terrorism. Technology can be applied to some of the crisis strategies developed by the military to deal with incidents of varying severity on the front lines or bases, and the same principles could be applied in the civilian world. Former service personnel of various nations have written documents on how they dealt with crisis management in a military environment. We can study these documents to identify common trends on how significant incidents would be dealt with and how Merlin can be used to help manage those incidents.

In the first instance, let's evaluate the input of former British Army officer Lieutenant Colonel Mark Wenham and former US Army Colonel Jimmy Blackmon, who both consider planning and preparation as the first step. At this stage, it is necessary to analyse the nature of a crisis, what risk it presents, and to who. Although it is impossible to identify every single potential threat, especially in a military environment, there are many that can be planned for by identifying those that are more obvious, by conducting after action reviews (AARs) and by analysing lessons identified.

Crisis strategies

Blackmon, a former Task Force Commander in the 101st Airborne Division, provides an example of how the software can help in these sorts of scenarios (*Leadership In Crisis – 5 Steps of Crisis Management*, April 13, 2020). Blackmon oversaw a force of soldiers stationed at an outpost in Nuristan Province, Afghanistan, which was only accessible by air. All supplies, including ammunition, rations and medical equipment, had to be delivered by helicopter. Personnel were flown into and out of the outpost in the same way. For Blackmon and his team, this represented a significant risk. Under any large-scale attack, his taskforce would be completely cut off and dependent solely on its abilities to deal with the situation. In this scenario, plans for dealing with the care of casualties, the distribution of supplies and, if necessary, a procedure to call in a relief force or medical evacuation were needed.

Blackmon and his team had to determine what threats could present themselves and how to deal with them from the moment an incident started, to the moment it was filed as complete. Much of these processes were in a hard copy format held in files, with duplicate copies stored at secondary locations. Many businesses may have similar plans in the event of a crisis and, while the nature of that crisis might differ from those experienced by Blackmon and his team, the underlying principles remain the same. Some of the key points from phase one of Blackmon's strategy are outlined below.

Who is in your plan? It may sound obvious, but you need to determine who is involved in your plan, and at what stage. You cannot, at any point in the process of handling a major event, be lacking critical information such as who to contact next. This may include key personnel from the emergency services, security officers, primary liaison with your customers, anyone who may be affected as a result of the event and any of your own employees who may be at risk. Remember, the technology to store this data is readily available, and it can help to contact them automatically from the moment an event occurs.

What are their roles? Do you know the role each person will take in handling this event? With technology allowing different stakeholders to receive information relevant to their role, it is no longer a case of simply identifying someone and calling them with generic information about the event; the technology can take these individuals to temporary flash pages, with all the data they would need to carry out their roles. In a military world, this may include information sent to medical teams, but for businesses it could be the teams that will secure a building after a significant break-in, or those responsible for evaluating any losses.

What are your processes? In Tony Jaques' *Relational Model of Crisis Management*, the author argues that crisis management is not: "A linear process of sequential phases in which you manage one issue at a time." I agree with him. The technology allows for multiple processes to be handled autonomously and to change depending on the way an event might evolve. It is no longer acceptable that a process should consist of: "Do this, do that." It must ask questions and change the way it reacts depending on how those questions are answered. Consider your process, do you have every eventuality covered?

And third, discuss the threat, your plans to react and train your staff. It is essential that the threats identified and your processes for handling them are reviewed regularly. Changes in technology might allow you to handle the incident differently, or previous incidents might not have gone as well as you had hoped. Stay proactive in your approach to handling these events, ensuring that the processes are run through and that all stakeholders are fully trained in their roles.

It is no longer acceptable that a process should consist of: "Do this, do that." It must ask questions and change the way it reacts depending on the answers

Once a crisis has been analysed and decisions made about how it might best be handled, it is possible to look at how the technology can be alerted and how those processes can be put in motion. In Blackmon's example, technology presents several options in terms of how this can be achieved. First, we can consider how

the threat of an attack can be passed to what Blackmon refers to as the crisis action centre (CAC). In a military context, this might be task force headquarters or brigade HQ. Crisis input terminals can be fine-tuned by users to allow events to be raised by the click of a button, putting a process into motion. For example, a crisis input terminal could be located at each combat outpost (COP), allowing personnel in these positions to alert the CAC immediately in the event of an attack. Crisis input would allow personnel stationed in those positions to determine the attack's key details, such as the number of enemy combatants and information on any weaponry they are bringing to bear on the COP.

Having received information via crisis input sent by those on the ground, the direction from where the attack is occurring will be known, allowing a specific set of procedures to be put into action to counter the threat. It will also be possible for those within the CAC to send alerts to other COPs, both manually and automatically, warning them of the attack. In such a scenario, it will be possible for those manning observation posts or checkpoints away from the point of attack to confirm whether something is also taking place at their location. This information is vital to determining how best to deal with the situation.

How can the same methods of triggering an event be used in a civilian environment? Take away the battlefield and consider how the threat of terrorism could be handled in the same way at a concert venue or sports arena.

In his article, *Leadership and Teamwork in Crisis Management: A Military Perspective*, British Army Officer Mark Wenham speaks of the need to define roles and responsibilities clearly, based on an individual's competence in a particular position. This information can be added to the processes so that specific jobs or roles can be passed on to the individuals to which they have been assigned.

Again, the terminals found in the COPs and medical or other facilities can alert personnel stationed in those areas that they are needed elsewhere or to prepare for the potential influx of casualties. These processes need not be any different in a civilian environment. The technology can be used to alert first aiders or additional security officers and help in the allocation of resources depending on how the event evolves.

Through the process flow, it is possible to define these tasks to reduce or eliminate the element of doubt about what steps should be taken next. It also provides the flexibility that will be required in these circumstances to allow the processes to evolve, depending on how the situation changes. For example, suppose the COP begins to incur casualties and it becomes necessary for wounded personnel to be medically evacuated. In that case, through Merlin, the medical emergency response team could be activated. If a protocol allows for it, the process of requesting medical aid or air evacuation can be entirely automated via calls to an external command post or messages sent to terminals at each location. This automation allows for personnel in the CAC to continue to deal with the procedures that require human interaction.

Using the information received from a terminal at the beginning of the attack, the technology can also provide the CAC with direct links to any CCTV situated in the area where the attack has taken place, allowing it to monitor the situation as it evolves. This CCTV will be recorded, and all footage saved to the database to be used later as part of the post-event analysis or within AARs. These reports are vital, and Blackmon defines the AAR as phase five of his process.

In a civilian world it is unlikely that it would be called an AAR, but the same method should be applied, as broken down by Blackmon:

- What did we say we were going to do?
- What actually happened?
- Why did it happen?
- What did we learn? and
- What will we do to prevent it from happening again, or do we have a new best practice?

In many instances, scenarios like the one detailed above would be dealt with using more standard forms of communication, such as radios and procedures in paper format. It is also necessary to consider that the primary CAC may not be able to deal with the incident locally, owing to the nature of the attack. Therefore, it is necessary for other CACs, perhaps at a higher HQ, to receive the same signals from the COP so that the same procedures can be put into motion regardless of where that CAC happens to be located. In a civilian environment, this may be classified as *force majeure*, which can be defined as interrupting the expected course of events and preventing participants from fulfilling obligations.

> Take away the battlefield and consider how the threat of terrorism could be handled similarly in a civilian environment, such as at a concert venue or sports arena

It is also possible to apply some of the technology to a military environment that may not necessarily be in a warzone. For example, if we look at military bases such as airfields or army barracks situated in the UK, we can see how the technology may improve and speed up the process at which some crises are handled, which are quite similar to incidents that may occur on a civilian premises.

Royal Air Force Officer Jon Short believes that there is enormous potential in using software such as Merlin to handle situations in which Duty Guards or Military Police stationed at checkpoints or gatehouses can call in more personnel quickly and efficiently in the event of an incident.

Again, we can look to a crisis input application and terminals stationed at these checkpoints to alert many personnel without the need to contact each one separately, as is the current method.

Flight Lieutenant Short cites the example of the moment news reached military campuses in the UK of the passing of HRH Prince Philip. In this instance, several senior officers needed to be alerted to the news, each of which had to be contacted individually by phone. Using one of two features within Merlin, this could have been achieved automatically, either via a call from a text-to-speech application, or by sending a notification to a custom-built mobile or tablet application.

In both instances it is possible to determine whether that message or notification has been received. It can also, if necessary, seek a response from the individual to determine the next course of action.

Recordings

The same can be applied to instances where there is a physical threat from a terrorist or malicious actor. Again, crisis input can be used for personnel stationed at strategic locations to alert a control room immediately at the onset of a significant crisis.

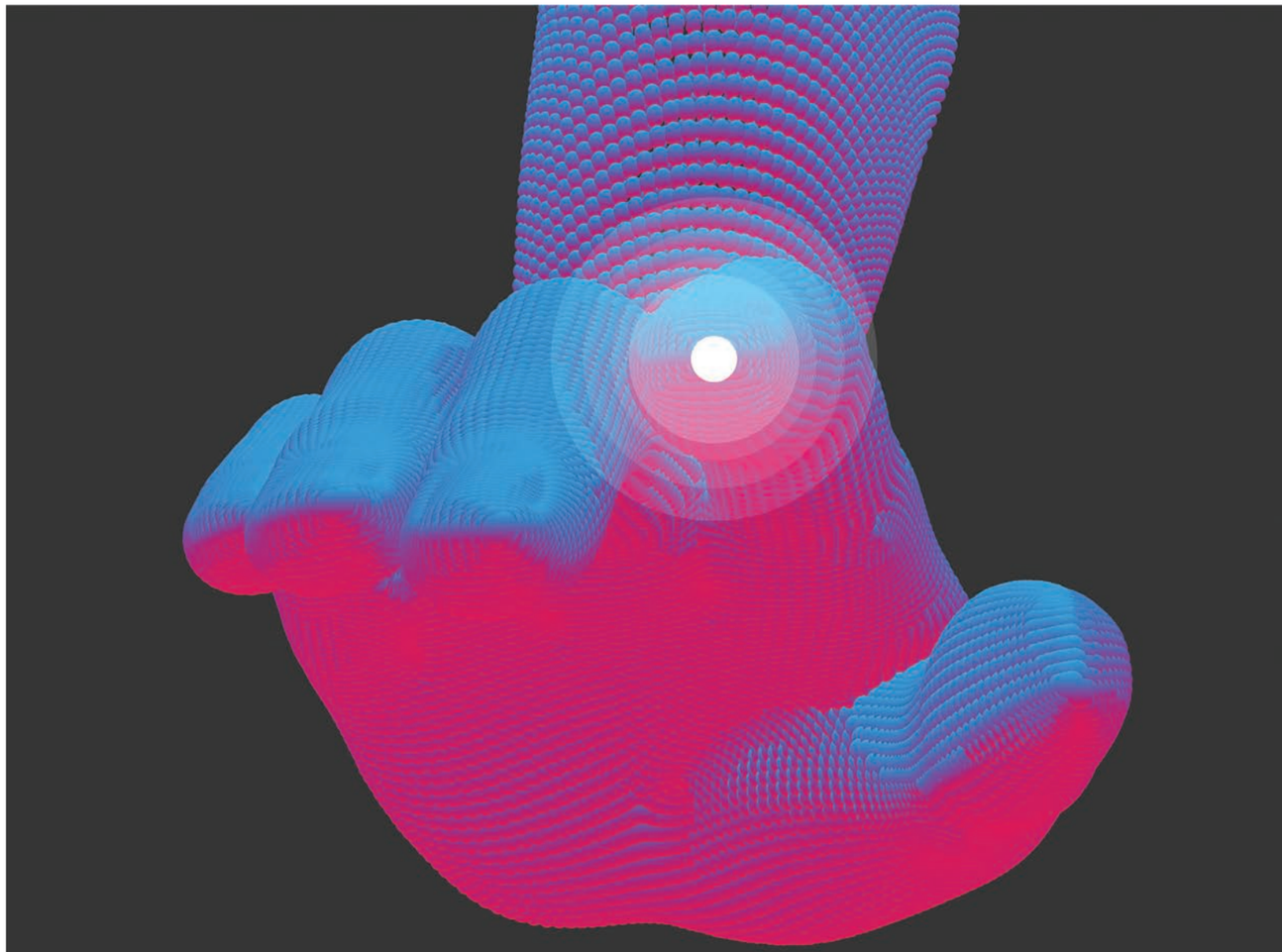
As described above, many of these steps can be automated, including the mobilisation of additional forces or the closure or evacuation of various areas of a campus. In all examples of crisis management within the military, one of the key stages is the AAR or post-event analysis. In-depth reporting features means that every step taken when the event was live is recorded to the database, from the moment it is reported to when it is closed. This includes the actions of personnel who are key to the event, such as those who raised the alert, those who dealt with it and those who were contacted. Audio recordings of any communication made through the system and complete footage from any associated CCTV are recorded in the database.

This information is all exportable as graphs or presentable reports that can be used in post-event reviews to determine how well the situation was dealt with and what lessons could be learned.

These reports also allow commanders or team leaders to assess their staff's performance and fine-tune any future training to ensure that any similar event in the future is dealt with more efficiently. C·RJ

Author

ADAM BERRY *is the Managing Director of Initsys Ltd and has been with the company since 2008. Initsys is a* CRJ *Key Network Partner, visit www.initsys.net for more information*



Studiom1 | 123rf