LEADING THE FRONT LINE

With the threat of a major terrorist attack still pressing, Lina Kolesnikova argues that too many emergency responders are still poorly organised and led, and calls for a "top down" approach to managing major incident response

Managing security crises, which involve life and death situations, is the toughest task for an emergency responder. In recent years we have witnessed an increasing number of catastrophic terrorist acts, which lead to more complex incidents with larger numbers of victims and an increasing dramatic component.

In the 21st Century, organisations are moving towards greater participation by all their members. But no matter how much input agency members have in the decision-making process, someone still has to actually make the difficult decisions. People in charge of major incident response operations take decisions which are crucial for victims, their relatives, responders and society. Competent leaders are therefore essential, particularly in a hierarchical system such as law enforcement.

The unique nature of each terrorist attack dictates the need to operate in a state of uncertainty, where there will always be some new elements. This requires commanders to "learn learning" – to quickly structure and assess the information available, promptly identify novelty elements and adapt to them. Successful commanders should be well informed on a variety of relevant topics, be able to spot the problem and to find a solution. Passive information processing should be replaced with active information accommodation. We should admit that, in modern terrorist attacks, nothing is certain except uncertainty and frequent change.

Response to terrorist attacks requires resources beyond the capacity of the police, so law enforcement agencies are likely to require the assistance of multiple other agencies, including the fire services, medical and paramedical agencies, emergency management organisations, the intelligence community and even the military.

For many of these organisations, involvement in the response to a terrorist attack presents many challenges. These include performing their professional duties in atypical contexts, placing themselves in personal danger, accommodating unique cultural attitudes and practices, working in isolation or facing political conflict and instability. Inter-agency rivalries between lead and supporting agencies, and even personal clashes between their commanders, are also among the challenges of inter-agency response.

The issue of compatibility and interoperability is also a very important aspect. Whatever plans and intentions are put in place, if agencies and their representatives are not capable of acting together in joint teams the operation is unlikely to be an overall success.

Currently, agencies are typically designed to meet their own objectives, and smooth integration and interoperability between agencies are typically under-developed. Forcing co-operation of such incompatible components almost inevitably results in inefficiencies, overlapping and competing responsibilities, with duplicated efforts in some areas and gaps in others. As a result, this approach to response organisation induces errors and, ultimately, leads to failures in operations.

Many governments are currently attempting a "bottom-to-top" approach to decision making. This is an approach based on identifying the existing or presumed capabilities of individual agencies. These disparate pieces are brought together to deliver an orchestrated effort. The still-disparate pieces might then be placed in the context of new, wider organisation, which leverages the individual capabilities of agencies and fills the gaps in its overarching capability set. In practice, this approach hardly works due to the persisting lack of built-in interoperability, as well as competing priorities and practices.

A "top-to-bottom" approach could produce somewhat better results. With this approach, the aim is to develop a strategy and define requirements first. This approach assumes that the global picture needs to be built. By adding a co-ordinating (driving) player, adherence by all parties to the same policy is achieved, while maintaining the benefits of proprietary competencies. Through this natural compatibility and under the supervision of an "owner" organisation, co-operation becomes "business as usual". Awareness of the competencies of different parts of the whole system comes naturally, as does the ability of different agencies to achieve joined-up, smooth operations.

In the very early stages of an incident no one usually knows the scale of the disaster. Typically, only ambiguous information is available at the outset, so one of the local agencies takes the first steps and then starts escalating. No one knows who is in the lead or whether its own agency priorities need to be subordinated to directions from a command post, or even whether the self-proclaimed lead should be obeyed.

Depending on the selected level of operation, the leadership will be defined and assigned differently, different agencies will play somewhat different roles and, in all likelihood, events will follow different escalation paths within the agencies. Different response plans might also be activated. Effectively, selection and subsequent changes of the operation level from local to regional to national and back should be obvious, transparent and comprehensible for all agencies in real-time.

Situational awareness, including awareness of possibly changes to response organisation, is critical. Responders should be able to access a known system, register a new incident or link to previously registered incidents, and find information on who is in the lead right now, where to go, etc.

Another challenge is related to the ever-growing size of the response organisation to major attacks. Law enforcement officers exercise quite a bit of individual discretion when operating on calls or initiating activities, and they generally work alone or in small groups of two or three. Terrorism, like special events such as G20 meetings, changes the equation, bringing hundreds of officers together in a single function. This fundamental shift must be addressed through the establishment of team work, including vertical (up and down within an agency) and horizontal intra- and inter-agency communication and co-operation. Co-ordinated work must be made "business as usual".

Another serious problem is that most incident commanders have little or no real experience of crisis situations such as terrorist attacks. Law enforcement leaders tend to have a command-and-control mentality; this is effective for policing, but when leading a response organisation it could fail because it relies exclusively on internal intelligence, experience and perceptions. In addition, the way in which agencies function differs from one to the next – even in the way orders are introduced, executed and reported. One can hardly expect similar behaviour from military organisations and civilian-staffed agencies.

The commander should always be responsible for the operation from A to Z. Due to the enormous amount of work and stress, this can only work well if the commander exercises delegation and management by exception, at least in less critical domains. To make this work, they should, at least to a certain degree, be accustom to it, and have some familiarity with and trust in colleagues from other agencies. To achieve this, it is reasonable to encourage horizontal links between leaders at certain levels of different agencies, or within the same agency but in different jurisdictions. They should, in short, get to know each other.

Often, there is contradiction between political ambiguous goals and expressly defined objectives. This usually leaves the commander with uncertain priorities, as well giving them the impression that, whatever decision they make, someone will find a reason to blame them for any mistakes. It is, however, possible to counter this challenge by shielding the commander from immediate and short-term political influences, and protecting him in the longer term. This would greatly helped if reporting and commanding lines for the operation commander were clearly defined.

Policy and legal requirements are the other aspect. It is necessary to support command post and operational teams with a fully resolved and clear framework of operation. The command centre must not have to spend time reconciling the policy and legal issues (for example regarding the large-scale use of military force within the ▶

©Getty Images

country during peace time), but needs rather to concentrate on planning, preparation and implementation of the response operation.

The system should always take into account the novelty aspect of the processes, as each attack will be different from any other. And, in addition to the prepared information sets, there need to be subject matter experts available on-demand. In this latter case, certain service levels need to be defined in the crisis management framework.

Another challenge is communication, which has proved itself to be a serious and widespread challenge. In all cases, it is important to train possible commanders to quickly assess incoming information. There should also be an information system supporting information gathering, and the sorting, processing, scoring, correlating, routing and dispatching of information and orders (multi-channel and multi-process). This system should support the automated follow up and translation of plans into specific, detailed and focussed directives (blocks of processes, assignments and reporting standards, etc). Queuing information following one simple process always helps to decrease information overflow.

While it is important to pay a lot of attention to the known challenges, there is also a need to look beyond them and try to foresee what the future might bring us. One of the potential challenges for the future could be the need to respond to terrorist attacks using WMD, when it may be necessary to take very tough decisions on the priorities of assistance to affected people, or worse, the isolation and even abandonment of people and territories. Who could make such decisions? Who should take the full responsibility in such circumstances? Who will be accountable for outcomes?

It is practically impossible to foresee and to train for all possible terrorist attack scenarios. But the crisis management framework defined by law should specify triggers and criteria indicating when such tough decisions are required. They should also lay out the decision-making chain, as well as minimum requirements for compulsory actions and mandatory information dispatching, including public information, while also maintaining sufficient audit trails. Maximum response times must also be set out. This would provide a sort of service-level definition for the people and agencies involved in such decision making.

©Getty Images

Leaders needed: emergency responders must be well organised and well informed

In the age of information systems, one can reasonably expect an increase in the number of attacks using information warfare. Such attack could very well have very negative and tangible outcomes, such as a major incident, even though the attacks themselves could be very brief. Such an attack might bring about a requirement for decisions and actions spanning far beyond the responsibilities of the immediate response organisations, and even beyond the capabilities of involved governmental agencies. For example, a cyber attack might occur in which there is a need for the expedient use of private sector or simply external resources who, because of the nature of the operation, would need to access critical information and resources. By whom, how and when can such things be decided? And how fast might such involvement become operational?

A good way to address this challenge seems to be the implementation of an information system for crisis management, with flexible process management, layered access control and powerful information gathering, sorting, scoring, routing and dispatching (and, naturally, sufficient activity monitoring and legally recognisable audit trails). Without such a system, involving new organisations in the operation will take far too long, thus missing window in which their involvement might produce the most positive effect.

In the modern world, attacks involving cross-border aspects might grow significantly, especially in the so well-connected Europe. There might be a need for actions spanning far beyond national geographical boundaries. Again, by whom, how and when these decisions be made? And how fast can action be taken?

Aside from the essential governmental co-operation frameworks and international treaties, it is highly recommended that personal links are encouraged between possible commanders and relevant contacts in neighbouring countries. Such links might help establish a certain degree of trust and co-operative spirit. Even if the only result is that the right advice can be obtained at the right moment, this relationship could significantly speed up a response, possibly preserving lives and avoiding huge financial losses.

There is a great deal that we can all do to ensure successful leadership of a response to a terrorist attack. The key is to learn how to identify, to adapt to and to deal with novelty quickly. This adaptive approach should be supported by powerful and adaptive information gathering and processing, scoring, correlating, routing and dispatching, and managed customisable processes.

Lina Kolesnikova is a Russian-born, Brussels-based associate of CS&A Risk and Crisis Management Consultancy. She provides consultancy to a number of organisations within both the private and public sectors.