29 November 2019

A co-ordinated responsE to nuclear security events – Challenges and opportunities

# Summary

Nuclear Security Events (NSEs) represent serious risks to the public and responding services alike and are extremely complex situations to resolve. It is essential therefore that States have a clear framework to deal with all aspects of those risks and that supporting plans facilitate the effective joint-working of multiple-agencies. The IAEA will publish formal guidance on this issue shortly. This paper is intended to share experiences gained so far during the development of that guidance in designing, delivering and sustaining capabilities required to provide an effective multi-agency response to NSE’s.

# challenges

Several workshops at national, regional and international level have been delivered to Member States (MS) during the development of the National Framework guidance. Without exception, those MS which have received the workshops have commented positively on the added value provided by having a well-structured and clearly defined national framework for dealing with NSEs. A number of challenges have been identified by MS during the workshops and some options for facing up to those challenges considered.

* **Joint planning**: responding services are very capable of developing plans to deploy their own response capabilities to the scene of an NSE. However, there is often a reluctance to participate in joint agency planning sessions as this implies a loss of control.

The workshops were able to convince delegates of the vital importance of joint planning and the development of multi-agency concepts of operation which are necessary to deliver a joint plan.

The Workshops were designed around the development of a terrorist/malicious attack over a period of time and mini-scenarios or vignettes were presented to the delegates so that they could test the existing levels of expertise and capability. To be most effective, those scenarios should be based on a risk assessment which indicates the levels of probability and impact. If the scenarios had not been realistic there could have been a lack of engagement by delegates during the workshops.

In many cases, the scenarios revealed a proliferation of plans but often without a clear hierarchy or understanding of how plans need to fit together to be fully effective. Similarly, single agency concepts of operation were the norm. From my own experience of developing CBRN plans in the UK the emergency services are always very focused on their own role and may often not be fully aware of the role of others. This is particularly the case in situations which are not regular occurrences or where plans have not been tested during an exercise.

* **Ownership of the planning process and the response:** unless the organisational hierarchy is clearly identified and formally agreed by all stakeholders, it is likely that levels of commitment from stakeholders will be sub-optimal or, even worse, the command and control arrangements lose clarity and become confused.

A frequent situation encountered during the workshops was uncertainty over who was in charge and over the appropriate level at which decisions should be made. In the worst cases, relatively straightforward decisions were being relayed to very senior (even Prime Ministerial) level leading to severe delays to the operational response. In real incidents these delays could easily result in loss of life which could otherwise have been avoided.

It has to be recognized that agreements between ministries on hierarchies and lines of responsibility are not always straightforward to achieve – sometimes there are overlapping responsibilities. A consensus has to be generated so that meaningful discussions on planning and responding can take place. The alternative would be lengthy debates at the time of the incident bringing about the same situation described above.

* **Capability development:** a particular challenge has been an undue focus on the procurement of detection equipment without an associated deployment strategy, a clear understanding of the limitations of the equipment, or indeed, trained and equipped personnel who can interpret the output of the equipment and take appropriate action without delay.

This paper is not suggesting that equipment is not important. The point to be made is that without a detection strategy and the necessary supporting capabilities there is a real risk that precious investment is wasted or even that long term damage to human health or the environment is caused. In order to assist with a holistic approach to capability development and to avoid overlooking some key requirement, the workshops invited delegates to consider the following capability elements:

Policies – including the legal frameworks

Plans and Procedures – concepts of operations

Organisational Structures – agreements on roles and limits of authority

Logistics – transportation of resources

Infrastructure – locations for the storage of resources

Equipment – purpose and limitations

Personnel – numbers and availability

Information – scientific support and knowledge management

Training – enabling the personnel to comply with the ConOps and to appropriately use equipment

Even if those elements are used as a basic checklist it can avoid some very expensive mistakes.

* **Sustainability:** it is inevitable that threat levels will vary over time and it is, of course, hugely expensive to develop a capability which can respond to a high threat environment. However, MS can be tempted to make economies in sustaining the level of the response as soon as the threat level appears to diminish. If this is done without agreeing a sensible baseline capability which can be easily maintained and quickly upgraded, and without a knowledge management strategy which prevents expertise from being drained away and not replaced, MS can easily find themselves unprepared to meet emerging threats. This often leads to constant re-learning of the same lessons by organisations, with a vicious circle of capital investment followed by premature scrapping of equipment and a further round of expenditure when the response falters during the next incident. It is one of the saddest realities to recognise that investment is often dependent on a disaster having happened.

# Opportunities

Some potential solutions have been identified during the workshops which expand on the formal guidance. There are some non-complex opportunities for improving the quality of the response to NSEs

* Joint planning and exercising develops relationships which will be of critical importance during an NSE. The level of trust generated between individuals during joint activities cannot be over-stated. True interoperability comes when the responding agencies understand not only their role but also the roles of the other agencies working alongside them.

A graded approach to the management of operational risks, when adopted by the responding agencies, facilitates a shared understanding of the problem, a joint evaluation of the hazards and a shared approach to their management.

* National Framework guidance (NSS-37G) rationalizes the key activities and outcomes necessary for a response to be effective. These can then become part of a joint concept of operations linked to a set of strategic priorities. In that way there is a clear “line of sight” from strategic command through to the front-line response operation.
* The benefits of the collaboration on planning for, and dealing with, NSEs can flow into the planning process for the response to other types of security event, not only those involving the potential or actual release of radiation.
* Lessons from joint training and exercising -‘red-teaming’ for example where delegates are invited to design attacks against their own defences - can be fed back to protective security planners and assist in identifying the vulnerabilities which led to material becoming out of regulatory control in the first place.

# Conclusion

The value of a National Framework for response to NSEs is clear – addressing the complexities of planning and responding to NSEs jointly with partner agencies brings benefits which reach beyond nuclear security.

John Edward Jones

Independent Consultant

UK