Contribution ID: **107** Type: **Poster**

Exercise Blue Beagle and Information Security

Tuesday, 8 July 2014 13:00 (1 hour)

On 7-9 January 2014, the UK Foreign and Commonwealth Office, the UK Home Office, the UK Ministry of Defence and the UK Atomic Weapons Establishment (AWE) hosted a Nuclear Forensics workshop and Table Top exercise (Blue Beagle) under the aegis of the Global Initiative to Combat Nuclear Terrorism (GICNT) Nuclear Forensics Working Group. Over 80 representatives from 25 GICNT partner nations and three of the GICNT observers (IAEA, Interpol and European Union) attended the event. The event aimed to demonstrate the importance of maintaining continuity of evidence throughout nuclear forensics investigations and aid partner nations in making decisions about the type of national or regional capabilities they might want to create.
Exercise Blue Beagle started with a short scene setting video showing an RDD attack in Accordia's capital city; Centreville. We see a terrorist fabricating an RDD, placing it at a busy shopping centre and then detonating it. In the aftermath police with protective suits and detection equipment are seen near the attack site, the surrounding area is heavily contaminated. There is concern about possible further detonations, the police are under pressure to find the perpetrators and fast!
Through a series of video enriched scenarios a UK panel of experts talked through how they would respond to the evolving incident. The exercise intended to provide extensive insight into the UK model, whilst also allowing the audience to provide international context. Each session was designed to focus on key areas; they deliberately did not cover exploitation of the post-detonation scene, but concentrated on the investigatory process as new leads emerged.
The scenario had multiple crime scenes: a café where suspects are overheard talking, a lorry where devices are fabricated, a car used to transport the devices and then finally at the scene of the next attack where officers successfully find and neutralise the device before it is detonated. The exercise considered the recovery of RN contaminated evidence from associated material, partially fabricated devices and neutralised devices. Throughout experts described how they maintain the continuity of evidence. They explored the decision making likely to be faced with: down selecting between covert or overt operations, RPE selection, operational safety and the importance of evidence prioritisation. We then saw the recovered evidence safely transported to a "state of the art"laboratory designed to exploit RN contaminated evidence. The complexity of analysing evidence in specially designed RN glove boxes and within a compliant safety regime was explored.
Finally, following a presentation from the UK Crown Prosecution Service, we explored how this complex evidence would be presented in court: the importance of decision making with respect to the offence, the subtle differences between witness of fact or expert witnesses, how to explain complex technical evidence in court, the need to retain evidence for appeals, implications of disposing of evidence because it is unsafe to store and decision making regarding the admissibility of evidence. To further promulgate the sharing of good practice, the material used for Exercise Blue Beagle and an exercise playbook have been packaged as an "exercise in a box"that was shared with GICNT members attending the conference. The exercise and the "exercise in a box"support the Dutch 2014 Nuclear Security Summit gift basket on nuclear forensics.
Information security: as nuclear materials and technologies spread, the global community needs to be ever more vigilant to prevent their acquisition by those that have no legitimate reason to use them. States are responsible for their own nuclear security architecture, and for putting in place a nuclear security regime appropriate to their national context.

Fundamental to any nuclear security regime is the need to effectively protect nuclear material and physical assets from non-state actors. Over recent years, however, the international community has increasingly recognised the need for States to also ensure the effective security of sensitive nuclear information, knowledge and know-how.

The United Kingdom Foreign and Commonwealth Office has created a guide on Information Security that provides an overview of issues, and identifies sources of further guidance and advice. This guide supports activities in support of the UK Nuclear Security Summit gift basket on nuclear information security. It has been shared with GICNT partner states through the Global Initiative portal.

Country and/or Institution

UK

Primary author: Mr SMITH, I. (United Kingdom)

Presenter: Mr SMITH, I. (United Kingdom)

Session Classification: Poster Session I