Making information security central to global nuclear security policy

Foreign and Commonwealth Office

Preventing terrorist groups from developing the capability to create and use weapons containing nuclear material is vital to global security. Prevention is not just about securing the physical nuclear material – information about its storage and transportation as well as research information that could assist with the successful assembly of a bomb also needs to be protected.

The UK government wanted to make information security an integral part of global nuclear security policy. To successfully embed the policy, FCO officials worked with academia, industry, international bodies, other countries and colleagues across Whitehall.

From Communiqué reference to practical action
The UK Government led on turning a brief mention it had secured in the 2010 Nuclear Security Summit communiqué into a real increase in action to support nuclear information security. They wanted it to become ‘business as usual’, rather than an optional add-on. This required not just persuading state actors and international organisations like the IAEA, but others who have access to or generate potentially sensitive information, particularly academia and industry.

Finding allies
The team used their existing networks and made contact with relevant umbrella bodies to help them identify the key players who could help them.

They recognised that success would only come if others were persuaded of the importance of the issue and took on finding solutions for themselves rather than having them dictated from Whitehall.

For example, the Team developed a close partnership with Kings College London who developed a module on Information Security for inclusion in professional training delivered internationally. A network of academics has also taken on producing a code of conduct for those carrying out research in potentially sensitive areas of nuclear technology. Produced and owned by the academic community, this document will have far more credibility and traction with its target audience.

In a similar way, the World Institute for Nuclear Security (an industry umbrella body) was brought on board. They agreed on the importance of the issue and developed training and guidance, as well as contributing to industry summits on the topic.

Nuclear information security on the international stage
By the Nuclear Security Summit in March 2012, the Team’s work engaging other states, academia, industry and others enabled them to bring proposals signed up to by 31 countries, the most supported of the Summit.

Outcome
The aim of the team to embed nuclear information into the mainstream is becoming a reality, thanks to their collaborative approach.

Following the March 2012 summit, individual countries are now drafting their own legislation to bring in the policies and codes of practice suggested. The final code for academics is being work-shopped at an academic discussion meeting this autumn.

Overarching guidance from international bodies now includes information security and industry is addressing information security in their own conferences and training.
Here in the UK, cross Whitehall working has created a common language and purpose. Colleagues in the Department for Energy and Climate Change, the Office for Nuclear Regulation, Atomic Weapons Establishment and the Defence Science and Technology Laboratory are now taking forward the work in their own areas.

Lessons

For others trying this approach, the team suggest you:

- Accept that the solutions may well be outside government. Identify who you can work with and how you can jointly develop your aims. This may seem time consuming, but saves work in the long term as the end results are more likely to succeed and less reliant on continuing Whitehall intervention
- Encourage allies to talk to their own communities (e.g. academia, industry). The message is far more likely to be heard if it comes from within.
- Understand why there is resistance to enable you to overcome it. The team found misconceptions of what they wanted to achieve was leading to push backs. They and their partners worked with these groups to explain and clearly make the case for the work.
- Be careful what you call it. ‘Information Security’ was often misinterpreted to mean ‘Cyber Security’. The Team felt this resulted in time wasted explaining the purpose of the work.

Find out more

- Government policy on nuclear security
- Multinational Statement on Nuclear Information Security
- Security guidance from the International Atomic Energy Agency