Pool Re was set up in 1993 by the insurance industry in co-operation with the UK government following the IRA's UK mainland bombing campaign to act as a mutual reinsurer to provide cover for losses resulting from acts of terrorism, regardless of the scale of the claims. The scheme's chief underwriting officer, Steve Coates, talks to Insurance Day about the evolution and use of terrorism risk models over the past decade.

How would you describe the state of terrorism risk modelling and to what extent does Pool Re make use of such models?

In comparison with modelling for natural catastrophe perils, terrorism modelling is still in its infancy. Improving deterministic techniques mean estimations of severity are becoming more credible but these are hampered by the variations in possible attack vectors for the terrorist.

The inherent difficulties in modelling frequency for terrorism remain a significant barrier as does a lack of historical data. Pool Re works with Guy Carpenter, our reinsurance broker, to model the scheme exposures and it uses RMS deterministic models, augmented by its own 3D building layers, to inform the event based scenarios we present to reinsurers. We also do our own modelling in-house to provide a contrast to the vendor model view.

We are working with a number of government agencies to inform our view of credible attack types and blast modelling. Modelling is viewed as key by any terrorism capacity provider and any return to a more normal market for this peril will require credible modelling.
Has there been a clear evolution in the sophistication of these models over, say, the past 10 years? In which ways are they helpful and what are their main limitations?

I think the evolution has been rather slow but understandably so. Modelling was non-existent pre-September 11, 2001 but thereafter, with the advent of the Terrorism Risk Insurance Act and given the sheer size of the US market, a number of vendor models came to the market. Since then it has been difficult for significant change to the model as there has been an absence of terrorism property losses.

Much development has focused on the US and one of the key elements to the Pool Re modernisation was to help foster an improvement to the models in UK. Hopefully by buying cover and thus exposing the global reinsurance industry once again to UK terrorism, we have enabled this process as there are now a lot more people asking for UK terrorism modelling.

The main limitation of terrorism models is the lack of data and thus their credibility. Also, there is a gap between the people who know most about the risk (government) and the insurance industry. That is something we hope to bridge.

Do the recent reforms of Pool Re, particularly the fact Pool Re now obtain its reinsurance cover from the private market for the first time in its history, mean it is now much more likely to make use of terrorism risk modelling as a way of providing a more transparent benchmark for its partners in the private sector?

Yes, the Pool Re modernisation means we are moving to more risk-reflective rates and for that we need better modelling. We are also buying retrocession and thus, we need modelling capability as do our reinsurance partners. If the scheme is to remain relevant we must demonstrate thought leadership and translate that into our underwriting approach. Modelling is one of the key mechanisms for that.

To what extent is the level of exposure associated with a chemical, biological, nuclear or a radiological attack part of the typical terrorism model?

There is little demand for chemical, biological, nuclear or radiological (CBNR) modelling, as property insurers exclude such losses and only a few pools cover some or all of these perils. Vendor models only consider CBRN at a very high level. As we cover CBRN we have engaged with ex-government consultants to help us understand the likely event scenarios, key loss drivers and post-event scenarios. This will enable us to build our own loss model for these perils and we hope to conclude this in 2016.

Pool Re coverage excludes cyber attacks at present. However, such attacks are increasingly part of the terrorist arsenal.

Do terrorism risks models take into account cyber attacks and, if not, to what extent is there a debate in the industry they should do so?

Terrorism risk models do not include specific consideration of cyber. We are aware modelling agencies are looking at cyber models but their focus initially seems to be cyber crime, not terrorism.