INMM Workshop On The Quantification Of The Likelihood Of Attack

Authors

Joe Rivers[1], Azaree Lintereur[2], Matthew Durbin[2].
[1]Rivers Security Services, LLC, GERMANTOWN, MD, USA, [2]Penn State University, University Park, PA, USA.

Abstract

This workshop was intended to address the age-old question of whether it is possible to quantify the likelihood of an attack on a nuclear facility to enable credible risk comparisons with safety. The INMM Nuclear Security and Physical Protection Technical Division has been working with the Joint Committee on Nuclear Risk Management (JCNRM) to develop guidance on risk-informing security, using safety risk information. It has become clear that there is a need for a quantification of security initiating events to enable some form of comparison between safety and security risk. This would enable more appropriate expenditure of resources to protect a facility. After significant discussion with the JCNRM, it appeared that such a quantification might be possible. The workshop brought experts from multiple disciplines together to assess whether it might be possible and to identify possible approaches for this quantification. Originally, it was intended to be held in-person at Penn State, but was postponed due to the pandemic. The Penn State Student Chapter made it possible to hold the workshop virtually. There was discussion on many aspects of the issue. This paper summarizes the discussion and identifies a path forward.

Background

This workshop was intended to address the age-old question of quantifying the likelihood of an attack on a nuclear facility to enable credible risk comparisons with safety. The INMM Nuclear Security and Physical Protection Technical Division had been working with the Joint Committee on Nuclear Risk Management (JCNRM) to develop guidance on risk-informing security, using safety risk information. This resulted in the formation of the JCNRM Physical/Cyber Risk Informed Security Working Group. It became clear that there was a need for a quantification of security initiating events to enable some form of comparison between safety and security risk. This would support more appropriate expenditure of resources to protect a facility and allow government agencies to better allocate resources between safety and security. After significant discussion with the JCNRM working group, it appeared that such a quantification might be possible. This workshop brought together experts from multiple disciplines to assess whether it might be possible and to identify possible approaches for this quantification.

Although originally planned as an in-person workshop, with the onset of the COVID-19 pandemic, the workshop was conducted virtually from November 9 – 11. The Pennsylvania State University INMM Student chapter hosted the workshop ion a virtual platform. This allowed approximately 150 participants from 5 continents. The workshop consisted of several panel discussions where panelists made presentations and then responded to questions from the workshop participants.

The workshop brought together a diverse set of experts on the topic, from government, industry, academia, and non-governmental organizations. The workshop provided for a discussion of the history and background related to the topic, possible solutions, cautionary notes, and benefits if it could be accomplished.

The Workshop

The workshop was opened up with a discussion of the long-standing perception that it was not possible to quantify the likelihood of attack. Historically, the arguments have been that nobody knows, there would be too much uncertainty, and it isn't a random event. As a result, the security community relies on conditional risk, which tends to give the impression of being too conservative, as this approach give the perception that the security community believes that an attack will happen with a probability of one.

The first panel provided a discussion of the historical perspective for looking at risk in the security community. Risk has been used in security programs for decades. The first vulnerability assessment approaches for nuclear facilities were developed almost 50 years earlier. The session provided a discussion of the history of assessing risk in the nuclear security environment, a discussion of the cataloging of terrorist attacks worldwide by the University of Maryland's Study of Terrorism and Responses to Terrorism (START) Program. This was followed by a presentation on a semiquantitative approach that might be an alternative to quantifying the likelihood. Additional presentations were provided on security risk approaches that have been developed for and used by US government agencies in nuclear and non-nuclear arenas.

The second panel discussion was on the topic of safety risk metrics. The INMM has conducted a number of workshops on the topic of risk-informing security. The one constant conclusion has been the need for the security and safety communities to leverage each other's insights and assessments. Risk approaches in the safety community are used routinely and are well-developed. The session provided workshop participants with a better understanding of safety risk metrics that might have some value in security, or where benefits might result if a comparable security risk metric could be identified.

The third panel provided discussions of a variety of security risk modeling approaches by panelists from national laboratories and academia. The speakers were asked to provide their thoughts on how these modeling approaches might be enhanced using the concepts of safety risk analysis approaches.

The fourth panel provided a discussion of the policy and operational advantages that would result from a quantification of the likelihood of attack. One of the biggest challenges for both government and commercial entities that must address nuclear security is how much security is enough. Relying on conditional risk makes this determination very difficult to make. There are a lot of non-quantitative factors that impact this decision, such as political and public perception, but having a better understanding of the risk would improve decision-making. One of the biggest decisions in budget process for government agencies and commercial nuclear facilities is how to best allocate resources between safety and security.

Given historical concerns over quantifying this likelihood, the fifth panel provided insights regarding how caution should be exercised if a quantification is developed. There has been little effort over the years to attempt to quantify the likelihood of attack. There is a general belief in the community that it cannot be done. The primary reasons include the lack of randomness, the low likelihood of any such attack, the adaptive adversary, and the credibility of using historical data. In addition, some believe that the uncertainty may be too large for any quantification have much value. This session provided a discussion of these concerns to allow the panels in the next sessions to better identify solutions that might address some of the concerns.

The final sessions focused on identifying potential approaches for the development of a quantification of the likelihood of attack. They addressed the cautions that have been identified, and how these cautions might be addressed in policy and operational environments.

General Consensus

The general consensus was that it was possible to quantify the likelihood. Some participants questioned the usefulness of any quantification, given the high level of uncertainty associated with any estimate. Others expressed concerns on how the results of a quantification might be misused.

Given the somewhat optimistic outcome of the workshop, it is appropriate to move forward with the identification of potential approaches to the quantification. In particular, a series of workshops should be convened with a smaller number of experts participating in each. The workshops would provide an iterative approach to developing possible quantification approaches.

The first workshop would convene a group of experts from academia, national laboratories, and industry to consider possible alternatives and develop up to two or three possible approaches, identifying pros and cons. This would be followed by a workshop with a diverse group of experts to provide feedback on the proposed approaches. Concurrently, panel discussions would be conducted at appropriate technical conferences to obtain feedback from a broader group of experts.

The next step would be to convene a working group to develop one of the identified approaches. Once this has been developed, the working group would share the approach with experts in the field to obtain feedback so that the approach could be fine-tuned.

Finally, a working group of safety and security risk professionals would be convened to determine how safety and security risk might be compared and contrasted if the likelihood of attack is incorporated into a measure of security risk.