What We Need to Know ...and when

by Igor Khripunov

Educating the public about nuclear terrorist risks can help raise levels of security

Nuclear power infrastructures could be the target of terrorist acts of theft, sabotage, unauthorized access or other malicious acts given their radiological and chemical content and potential for building weapons. Attacks on its major components, including fuel production, reactors, waste handling, and reprocessing facilities, would lead to serious consequences—even if there is little or no damage to a nuclear power plant itself and other related structures. Public fear of nuclear radiation, in combination with a possibly massive resultant blackout and other aggravating factors, could create significant distress and panic. In other words, successful terrorist attempts to attack nuclear power infrastructure can easily bring about systemic disaster.

Systemic risks impact society on a large scale and their effects may spread much further from the original hazardous source. Those risks widely affect systems that society depends on, such as health, transport, environment, telecommunications. Their consequences may be technical, social, environmental, psychological and economic and involve different stakeholders.

In this context, however, one important stakeholder has been under-appreciated, under-utilized and somewhat misunderstood: the general public. The nuclear power infrastructure must learn how to efficiently communicate to the public and develop better options for public risk communication that relate to deliberate attacks or accidents. The public is also a challenging stockholder because citizens are deeply split regarding the acceptability and value of nuclear power generation and tend to express their feelings emotionally. However, there is growing recognition that because of skyrocketing oil prices and evidence of the greenhouse effect, nuclear power may be approaching renaissance. Hence, the public must no longer be looked upon only as potential victims or panicked masses but rather as an important contributing factor for better nuclear security throughout all stages of a possible incident.

Common risk perception

Common risk perception is built on objective and transparent risk communication. This means an interactive process of exchange of information and opinion among individuals, groups and institutions and the transfer of risk information to the public, and from the public to decision-makers and infrastructure operators. In reality, a common level of acceptance of risk is based not only on technical expertise, but is strongly affected by cultural and individual aspects and values. To achieve this goal through risk communication regarding nuclear power infrastructure, the process must be based on a dialogue among major stakeholders — risk experts, policy makers, infrastructure operators, and the public involved.

For some, if not most professionals and experts, risk is the likelihood of an event multiplied by its estimated consequences, ranging from mild to catastrophic (risk=probability x consequences). There are at least three types of probabilities regarding nuclear facilities: deliberate attack, interruption failure, and neutralization failure.

The magnitude of a risk to individuals varies depending on their background and objectives. This leads to different opinions and interpretations of the risk and vulnerabilities. The public often tends to base its views of risk on personal experience and impacts. Hence, the probability that something bad will happen to people, combined with the aspects of the situation that upset them, leads to their perception of risk, which is based more on emotion than on analysis of the contributing probabilities. Thus, preventative actions are sometimes hard to prioritize by outsiders and even harder to explain to the public. There is also a question of understanding the language used, especially when the terminology differs and confuses the discussion between different fields of risk assessment.

Factors that may influence public attitudes include the perceived magnitude of the consequences, ignorance about the

nature of the hazard, distrust of the institutions attempting to manage the hazard, and the level of media attention devoted to an event. Also important for understanding public perceptions are the proximity of area residences and schools to a specific segment of the nuclear energy infrastructure; the local population density; and the activities of local interest groups. Even within a given population, risk perceptions are not uniform and may vary depending on experience, gender, social status, and world view.

Stages in risk communication

Risk communication is vital in the process of achieving a common risk perception. It can be defined as a two-way process of information exchange that includes multiple types of information with multiple purposes. As an important benefit, risk communication has the potential to build public trust and resilience in times of crisis.

There are different perspectives to approaching and understanding the meaning of risk communication based on a perceived notion of the public. On one hand, there is a perception of a passive public complacently waiting for the transmission of vital information from authoritative sources while, on the other, there is an image of a proactive public striving to understand the reality and contribute to shared management of risks. The second perspective provides the most optimal scenario of social mobilization consisting of an interactive process of information exchange and opinion among individuals, groups, and institutions.

A mode of risk communication is not seen as successful if its objective is the acceptance of the views or arguments of experts by non-experts. It may, however, be regarded as successful to the extent that it raises the level of understanding of relevant issues or actions for all stakeholders, including the public and ensures that they are adequately informed within the limits of available knowledge and, if necessary, can play a meaningful role in risk management.

Accordingly, in order to achieve desired objectives consistent with a given segment of the nuclear power infrastructure, any communication with the public ideally must proceed through three stages:

① **Public information sharing:** a one-way process in which information flows from government and/or operators to the public for educational purposes;

② **Public outreach:** a proactive campaign undertaken by government and/or operators to respond to emerging public concerns; and

③ **Public involvement:** an ongoing relationship in which communities become partners with government and/or operators for certain agreed-upon purposes.

The last stage is naturally more mature when the public is aware of the stakes involved and has the requisite knowledge to take on specific roles at pre-incident and post-incident stages.

Public involvement

Security is now a concern that affects public perceptions about nuclear and radiological risks and terrorist threats. To communicate effectively about security-related issues, government and operators must understand and respect the public's very real worries about safety and security. The public understands and is largely concerned that terrorists may be intent on breaching the safety features built into nuclear installations by denigrating security systems. The public typically questions whether security systems are adequate and develops an active interest in making the security regime robust enough to keep safety features reliably operational.

However, emerging threats of terrorism increasingly elevate security including physical protection to a more independent and unique status beyond a simple safety-security synergy. In other words, the overlap between safety and security is somewhat shrinking, revealing conflicting elements that need to be reconciled. First, terrorist attacks have the potential to increase significantly the impact of an accident, making routine safety procedures inadequate. Second, as adaptive adversaries, terrorists not only have the ability to change tactics as an attack unfolds but also are capable of concurrent and/or subsequent multiple attempts against infrastructures. Third, terrorist attacks are criminal acts and, as such, include the additional complications of securing a crime scene and conducting an investigation during the response phase.

For effective risk communication, safety and security must be explained and presented to the public as two sides of the same coin which is trouble-free operation of the nuclear power infrastructure under any conceivable circumstances. Hence, by getting the public on-board and recognizing it as an important stakeholder, a meaningful risk communication strategy can achieve four interrelated missions:

1. Reach a common risk assessment enabling the public to be educated and prepared. Gaining public support requires a realistic portrayal of risk that is accurate and draws a fine line between hyping the threat to spur people to action and trivializing it to provide them false reassurances. Preparedness provides a way for the public to translate risk awareness into action and can consist of a range of activities, including developing and practicing contingency plans, such as communication, evacuation, or sheltering. Preparedness also serves as a bridge between risk education which occurs in advance of an event and taking protective actions during a crisis.

Much, if not all of the information available to the general public about the risk of terrorism, preparedness programs, assessments or response capabilities, and so on will also be available to potential terrorists, who may use it to decide whether to undertake an attack and which segments of the infrastructure are most vulnerable. It must be understood that the ultimate target for terrorists is public confidence in itself and the government rather than infrastructure specific units per se. Risk communication, in this respect, represents a careful balancing act for government and industry. Both must understand the benefits of keeping the public adequately informed, the deterred potential of certain kinds of public communication for terrorists and the need for confidentiality regarding sensitive information. These competing aspects must be weighed when deciding what types of information should be made available and in what detail.

2. Encourage a well-informed and well-motivated public to contribute to a healthy nuclear security culture, not only at the nuclear plant or other associated unit level but also nationally. Security culture at the facility level can be defined as a linked set of characteristics that together ensure that the workforce pays sufficient attention to nuclear security. Shared beliefs, assumptions, principles which guide decisions and actions, and patterns of behavior hospitable to security represent the ordered and hierarchical set of characteristics that make up nuclear security culture. It is important to understand that most members of the nuclear plant workforce are part of the community adjacent to the site. They have families there and socialize with local citizens on a regular basis. Hence a strong commitment to nuclear security on the part of the local community heightens the public visibility of security-related issues, indirectly improving the motivation of the staff that operates that site.

3. Build up public vigilance, persuading citizens to cooperate more closely with law enforcement. This vigilance will manifest itself in reports of unauthorized efforts to gain access to sensitive infrastructure sites or breach the site's boundaries. An engaged public will even report suspicious people or activities near the site. A small portion of local citizens could be trained to perform such functions on a voluntary basis, particularly in sparsely populated and difficult-to-monitor areas.

Such initiatives must, however, draw lessons and avoid the pitfalls of what is described as "vigilantism." Also, these programs need to be leery of creating a cadre of members of the public who rush to the scene of a terrorist incident and attempt counterterrorist actions because they believe, wrongly, that they are qualified in terrorist response operations. However, there is a niche for a security conscious public to fill. Training of local citizens, when and if it is deemed necessary, must be a well thought-out, stably funded, and widely publicized campaign.

4. Reduce the immediate and long-term physical and psychological impact of a terrorist incident by fencing off panic, boosting morale, maintaining credibility, and providing guidance. This emphasis is especially important while counter-terrorist actions are underway or other terrorist acts are likely. These post-incident arrangements consist of steps that individuals and communities can take to save lives and reduce losses when an event occurs. The ultimate test is their effectiveness in a real crisis when traditional societal institutions tend to unravel as was evidenced in the wake of hurricane Katrina which hit the US last year. Such actions include forms of sheltering, evacuation, and quarantine as well as using individual protective equipment and a variety of medical counter measures.

How much information and when?

A major question is: how far in advance is it necessary to intensify the risk communication campaign and educate citizens about the actions they should take in response to various types of terrorist incidents? While a large swathe of the public will likely not pay much attention to these efforts or retain the information and materials provided in anticipation of future incidents, some people will—perhaps because they are convinced that terrorist incidents will occur and perhaps because they feel empowered by information. Given the potential of this activist group to influence the behavioral and psychological response of others—at home, in the office, or at school—it is worth investing at least some time and resources in educating the public.

Ultimately, it all comes down to creating a more resilient and prepared population in the face of terrorist adversaries. Resilience is usually defined as the ability to handle disruptive challenges, characterized as emergencies that can lead to or result in crisis.

Technical solutions and competence can contribute to resilience but ultimately real resilience is about attitude, motivation and will. Engendering such attitude requires a cultural change and more focus on the mindset of people. Resilient citizens will be more than bystanders in the effort to deal with terrorist acts—be it nuclear power infrastructure or any other target—and will be less prone to fear and anxiety before an during crisis situations. Resilience-building and other public-related campaigns, however, cost time and money, and they have to be sustained over the long term. Careful forethought should go into the planning and execution of such campaigns in order to reap maximum benefits.

Igor Khripunov is Associate Director of the Center for International Trade and Security at the University of Georgia, USA. E-mail: igokhrip@uga.edu