Global Transformational Events and Nuclear Security: The Threat from Sub-State Entities

M. A. Root, LANL, K. E. Apt, Capstan Global LLC, T. Hernandez, SNL, C. McMath, LANL, and B. Hornbein, LANL

LA-UR-21-27758

Abstract

The objective of the joint transformational events study conducted by Los Alamos and Sandia National Laboratories is to analyze the threat, including insider threat, posed by domestic and international sub-state entities intent on theft or sabotage of states' nuclear material, facilities, or operations—concurrent with significant geopolitical change or a triggering global transformational event, i.e., a "black swan." Black swan events are usually high consequence, but low probability, which makes them difficult to mitigate. This study analyzes global transformational events ontologically by identifying event properties and understanding how these properties are interrelated through definition of a set of categories and concepts that represent the overall subject area. The study provides insight into how the event might affect the nuclear security threat environment and what mitigation or prevention strategies could be advanced by relevant stakeholders.

Introduction

The potential for "black swan" events[a] to impact global security has rarely been as evident as during the ongoing COVID-19 pandemic. The COVID-19 pandemic led to impacts that are far-reaching, including financial hardship, shipping and manufacturing disruptions, and a pause in nearly all non-essential domestic and international travel, to name a few. It is not hard to imagine how these profound impacts could reverberate in the nuclear security arena– in particular, through the International Nuclear Security (INS) program core elements of physical protection, regulatory framework, and transportation security. The LANL-SNL transformational events study aims to analyze the threat, including insider threat, posed by domestic and international sub-state entities intent on theft or sabotage of states' nuclear material, facilities, or operations—concurrent with significant geopolitical change or a triggering global transformational event, i.e., a "black swan."

This paper describes the methodology used to establish potential black swan events for consideration, to rank these events according to their potential to enable a sub-state entity to take actions that could affect the nuclear security of a country, and to determine potential mitigation and prevention options. Because the results of the study will be distribution controlled, specific nuclear security risk factors and threat modes are not associated here with actual events. The ontological approach to this project provides a concise and accessible reference for relevant stakeholders.

Methodology

The general approach taken by the project was to bring together Subject Matter Experts (SMEs) in nuclear security, nuclear safeguards, and other relevant fields to brainstorm issues, as this

project is ambitious in both scope and depth. Particular consideration was given to determining techniques to stimulate open and inclusive conversation between SMEs and to ensure a diversity of opinion was represented. Ground rules were established to ensure that no one person would control the conversation, and that dialogue could continue regardless of disagreements. Due to pandemic restrictions, all meetings and brainstorming sessions were held virtually via WebEx. Two 2-hour roundtables were held on January 26, 2021, and two more on April 12, 2021. Additionally, two 1-hour sessions were held to discuss the event prioritization process, which was limited to only a small subset of the roundtable participants. The first set of roundtables was meant to determine and winnow the list of concerning transformational events. The second set of roundtables focused on determining potential prevention and mitigation techniques for exploitation of transformational events by sub-state entities.

Event Selection and Ranking

A list of potential "black swan" transformational events was generated by the project leadership team in advance of the first SME roundtable to stimulate participant thought. These included events such as global pandemics, global economic crises, cyber warfare, climate change, asteroid impact, collapse of country governments, hostilities toward or an ending of the Nonproliferation Treaty, and many others. The first set of roundtables focused on determining potential transformational events that the project leadership had not originally considered and determining whether the events posited posed a significant threat to nuclear security.

To determine whether events posed a nuclear security threat, participants made an initial assessment of the likelihood and consequence of the events. Likelihood and consequence were considered initially in small groups using a simple Cartesian plot with four quadrants, with likelihood on the y-axis and consequence on the x-axis. An event that was considered high-likelihood and high-consequence would be placed in the upper right quadrant, while a low-likelihood, low-consequence event would fall in the lower left. Aside from an obviously important event like domestic civil conflict, this exercise was unfortunately inconclusive – there were too many factors involved, and SMEs became bogged down in the details of speculative events and their ramifications. This led the leadership team to consider a new approach to ranking events.

Instead of the quadrant system, we decided to ask the SMEs to examine the ontological factors associated with transformational events. Several ontological factors were identified that could be associated with the transformational events, including timescale, predictability, likelihood, initiation, perpetrator (if any), progression, and political influences. A true transformational event can be described as a *complex adaptive system* [1] and, as such, is associated with gross concatenation and unpredictability. In order to bound the problem, the study identified shifts in global, national, regional, social, political, and personal domains that could be caused by the events. These shifts were then considered in the context of possible changes to the nuclear-security threat environment.

As an example, the 2020-21 pandemic greatly reduced possibility for international travel, which in turn reduced the options for international terrorists traveling to a country and, correspondingly, probably decreased the threat by such parties to nuclear facilities and materials.

At the same time, the pandemic created financial and psychological stress on a personal level, which might have contributed to a greater incentive for untoward actions by nuclear insiders.

Of several ontological factors that could be used to evaluate events, three were selected: *exploitability*, *likelihood*, and *progression*. The *exploitability* of a transformational event is a measure of how easily a sub-state actor or insider with malicious intent could take advantage of that event (by way of changes to the nuclear security threat environment) for the purpose of disrupting the nuclear security regime through sabotage, theft of nuclear material, and/or diversion in transit. The *likelihood* for a particular event was defined as the chance that the event will come about by any means, i.e., naturally, state-sponsored, non-state actor initiated, etc. Likelihood refers to how possible or feasible an event is—even as its predictability might be completely unknown or vary widely. The *progression* factor was viewed as an indication of how the event could spread regionally and globally, either physically (as with a tsunami) and/or through other mechanisms (as with a financial market crash). Progression is a measure of how uncontrolled an event is and how widespread it becomes. This measure is more closely related to aspects of a complex adaptive system, as national and international responses (i.e., system interactions) can greatly reduce—or exacerbate—adverse effects, depending on coordination. The SMEs ranked the relative importance, in the context of this study, of the three evaluation criteria of exploitability, likelihood, and progression. Not surprisingly, exploitability was viewed as the most important, yet all three come into play when considering mitigating strategies.

Without attempting to quantify the transformational events *per se*, the study polled SMEs to compare the relative importance (in nuclear security space) of events against each other. Recognizing that it was too complex to rank all 16 events together simultaneously, the down-selected events were grouped according to the four major categories (discussed below in the results section) and then compared within each category. All transformational events were compared using a standard Analytical Hierarchy Prioritization (AHP) process [2] where SMEs completed dyadic (pairwise) matrices of events according to the three criteria *exploitability*, *likelihood*, and *progression*. For example, a "global pandemic" was compared to the event of "large-scale, critical infrastructure failure." For event pairs like this, SMEs posited which would be more exploitable, more likely, and more likely to progress to other dimensions beyond the original event.

Prevention and Mitigation Techniques

Techniques to prevent and mitigate sub-state actor impacts to nuclear security were the focus of the second set of roundtables. In this session we emphasized that SMEs should *not* consider how to prevent the actual events from happening, as that is outside the scope of our study. Rather, we wanted SMEs to focus on how to prevent sub-state actors from taking advantage of the events to threaten nuclear security, and how to mitigate the consequences should prevention techniques fail.

In an effort to simplify the brainstorming process, we used a technique commonly used in many industries, including aerospace and intelligence, to analyze risk. The technique is commonly called the "Bowtie Analysis Method." [3] The Bowtie Analysis Method is a visual method to visualize the risk of a given hazard in an easy-to-read format. The "Bowtie" name comes from the analysis providing both *proactive* (i.e. prevention) and *reactive* (i.e. mitigation) responses to

the hazard. SMEs were given a template for the Bowtie Analysis containing the components shown in the graphic in Fig. 1, below.

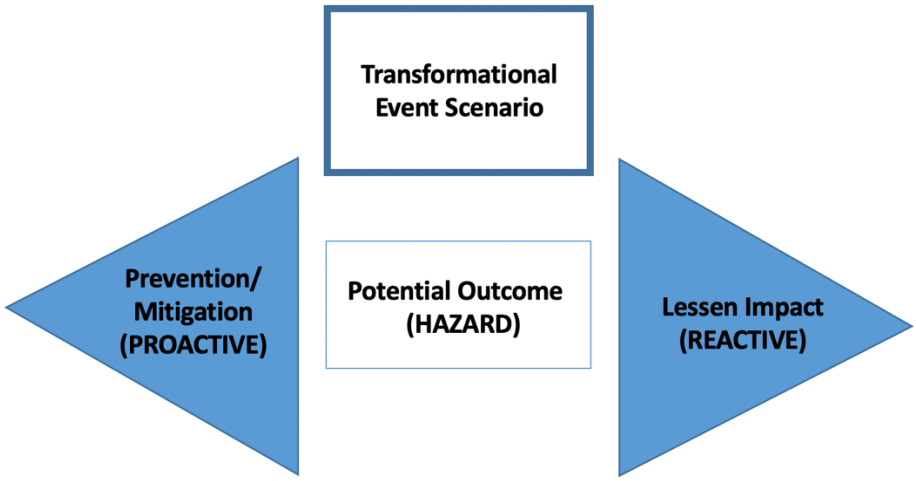

Fig. 1. Bowtie Analysis schematic

In each session, SMEs were given 1 to 2 transformational events to analyze. They were asked to brainstorm potential adverse outcomes of the event that could lead to nuclear security threats from sub-state actors. For each outcome, they were asked to determine proactive and reactive techniques to manage the situation.

Results

Event Selection and Ranking

The preliminary results from the first roundtable meetings generated nearly thirty possible transformational events for consideration, many overlapping or with similarities. From these, four general categories were identified, with a total of sixteen down-selected events. The four categories were 1) natural disasters (e.g. tsunamis and climate change); 2) endogenous societal disasters (e.g. pandemics and economic collapse); 3) war and conflict (e.g. terrorist attacks and regional battles); and 4) geopolitical upheavals (e.g. collapse of government or internal civil conflict). These events were considered in geographies where there are significant nuclear fuel-cycle capabilities, generally those where there is US-origin nuclear material or Office of International Nuclear Security collaborations.

Many of the events considered were speculative and seemingly improbable, but nevertheless within the realm of possibility. Pairwise AHP results from the analysis yielded a preliminary breakdown of events reflective of their importance in the three criteria, as shown in Fig. 2, below. Although the events are not identified here, some are clearly highly exploitable but relatively unlikely. A global economic meltdown (one of those on the right in Fig. 2) could create far-reaching financial, personal, and societal disruptions, which taken together could be readily exploited by terrorists intent on nuclear disruption. But only one such event occurred in the 20th century, well before the advent of nuclear power. And the financial "Great Recession" of this century did not rise to a level threatening nuclear systems.

Other events, a tsunami for instance, are far more probable (indicated by the column's relatively large green segment) but are correspondingly harder to exploit for clandestine nuclear security purposes. Because the AHP provides only an approximate ranking of transformational events, these data of Fig. 2 are best considered in general groupings, rather than as absolute comparisons.

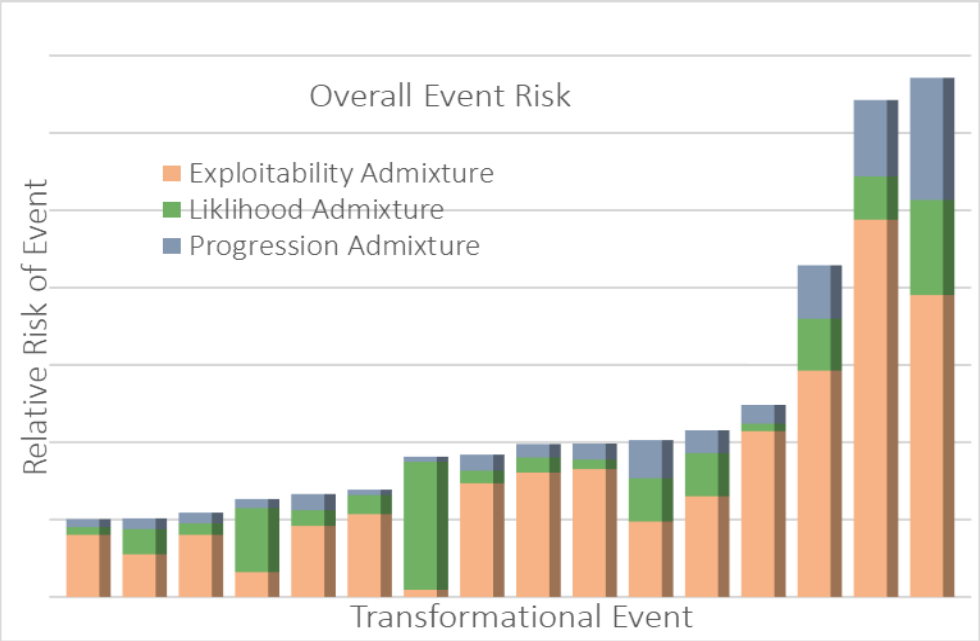

Fig. 2. AHP results show overall event risk of nuclear security threats from sub-state entities. Actual event identities are distribution controlled and are not presented in this graphic.

On average, likelihood and exploitability play the largest roles in determining the overall event risk. Therefore, another possible way to prioritize event response is to consider only the exploitability and likelihood of the events. In fact, the AHP process involving the SMEs pointed to a relative ranking of the evaluation criteria exploitability, likelihood, and progression as approximately 5 to 3 to 1. Events that fall in the red, upper right region in Fig. 3, below, would be considered the most concerning, while those falling in the green, lower left region of the figure would be considered much less so.

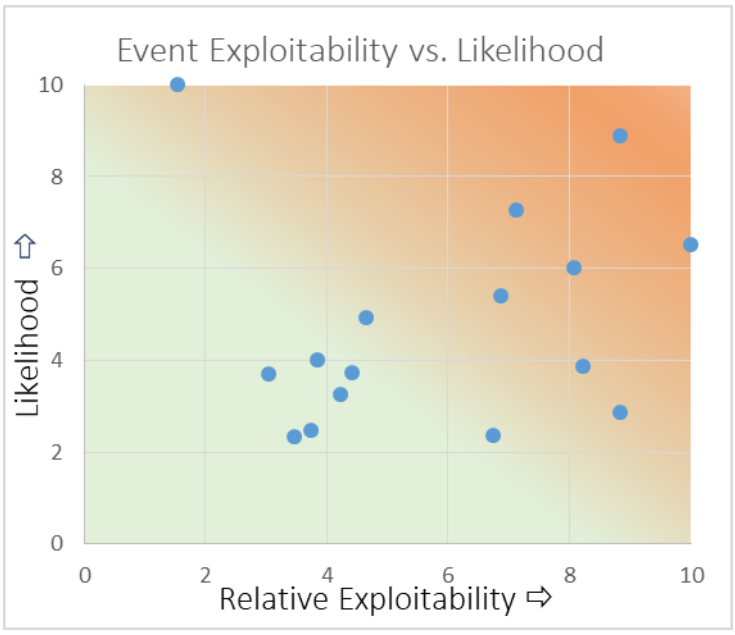

Fig. 3. The event exploitability vs. likelihood plot provides an additional way to visualize and prioritize event mitigation and response.

Event Prevention and Mitigation Techniques

Brainstorming of event prevention and mitigation techniques yielded hundreds of potential outcomes, and proactive/reactive responses. Additionally, many event responses were cross-correlated across events. For example, many of the same techniques can be used to manage the potential impacts from an asteroid impact and a tsunami, as the outcomes of each can be quite similar. This cross-correlation was true even across event categories, and this cross-correlation will be used going forward as a way to organize the presentation of potential responses to interested agencies.

The adverse outcomes that were brainstormed fell into three primary categories: 1) direct threats and stressors to nuclear security (largely facilities and transport), 2) indirect threats and stressors to nuclear security (i.e., opportunities provided by the event), and 3) secondary effects to nuclear security (i.e., longer-term changes caused by the event). Considering the first grouping of adverse outcomes, SMEs identified those of most concern, which include:

- Direct internal or external sabotage of nuclear facility and security systems
- Unauthorized access and loss of nuclear material and facility control
- Radiation dispersal with associated area and access denial
- Disruption of utility grids and communication systems
- Evacuation, displacement, or absence of personnel
- Military or paramilitary combat nullifying government control
- Loss of sensitive nuclear information

While any one of these outcomes are cause for alarm, other factors of the transformational event like its timescale, initiation, perpetration, and spread would determine the severity and level of response needed. These outcomes ultimately would be matched against a country's security

posture in order to determine what mitigating strategies would be most effective—and needed. Where deficiencies exist, knowledge sharing and technical assistance can then be provided to improve national capability and capacity addressing this expanded spectrum of threats to nuclear security.

Additionally, possible changes to the nuclear security threat environment caused by events fell into three primary categories: 1) individual and personal changes, 2) national-level changes, and 3) international and multinational changes. The SME roundtable discussions identified numerous threat-environment changes in all three groupings. On the national level, for instance, some of the more important changes include:

- Scarcity of goods and services and major supply-chain disruptions
- Business failures, reduced commerce, and massive shifts in jobs and businesses
- Distrust of government and loss of public confidence
- Diminished national response capabilities
- Reduction or curtailment of international cooperation
- Restrictions on travel and greater border security
- Increased extremist political and cult activities

The SME roundtable discussions formulated numerous mitigating approaches to the subject transformational event groupings. Examples of these were national and government-level approaches, such as:

- Increased preparedness for disaster response entities
- Emergency communications and "dumb" backup systems
- Interagency communications and action plans
- Redundant engineering safety systems
- Public relations and outreach campaigns

In addition to national level approaches, preventative and mitigation techniques were also categorized at the facility-level and at the multinational and international level. These categorizations will ultimately be used to advise relevant stakeholders on where to focus time and resources in preparing for and managing potential "black swan" events.

Transformational events can be further analyzed in the context of systematic risk. Here, multiple factors are considered that give rise to a systemic untoward outcome, such as theft of nuclear material or insider sabotage.

The diagram in Fig. 4 represents how a transformational event, in this case global pandemic, could lead ultimately to a "systems failure" of sabotage by a facility insider. Several direct and indirect factors and conditions, all arising from or augmented by the primary pandemic event, interact in a complex way to result in the possibility of nuclear sabotage. Acknowledging and addressing these factors as an interactive, complex system will be important in devising effective mitigating strategies.

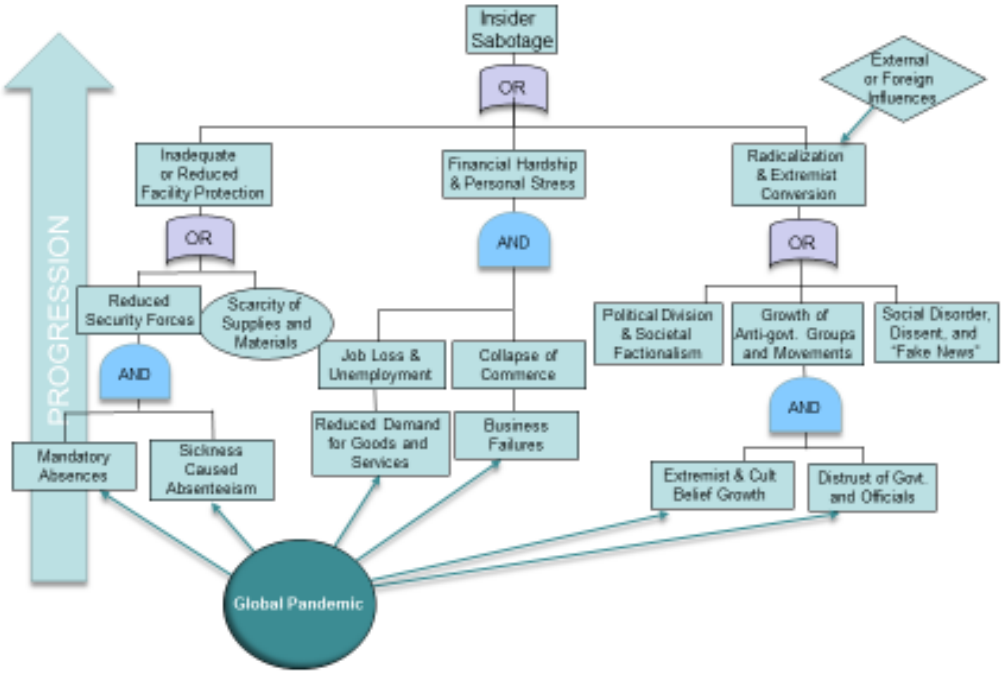

Fig.4. Notional systemic-level risk analysis of global pandemic effects on insider threat to nuclear security

Conclusions

"Black swan" events are by their very nature impossible to predict precisely. However, the potential threats to nuclear security brought about by black swan events can be managed and mitigated. This report presents the methodologies and high-level results from a set of virtual brainstorming sessions meant to determine potential events that could cause threats to nuclear security from sub-state actors, to categorize and prioritize the events, and to determine avenues of prevention and mitigation techniques for these events. The techniques used to brainstorm events and responses of this sort are instrumental to the final results from the study.

This study has successfully determined thirty potential transformational events that could cause impact to nuclear security due to sub-state actors, down-selected and ranked the events by risk-level, and determined potential mitigation and prevention strategies for each event. The ontological approach to this project provides a concise and accessible reference for relevant stakeholders.

References

1. Carmichael, Ted and Mirsad Hadzikadic, "The Fundamentals of Complex Adaptive Systems.", DOI: 10.1007/978-3-030-20309-2 (2019)
2. Saaty, T. L., Rev. R. Acad. Cien. Serie A. Mat., "The Analytic Hierarchy/Network Process", Vol. 102 (2), 2008, pp 251-318. https://rac.es/ficheros/doc/00576.pdf

3. *The Bowtie Method*. (2018). Retrieved from Patient Safety BowTies: http://www.patientsafetybowties.com/knowledge-base/6-the-bowtie-method#Top%20event

Footnotes

[a] The term "black swan" refers to an unforeseen event, as when Western civilization believed that all swans were white and that a black variety didn't exist—until they were observed in Australia in the 17th century.

Acknowledgements

We would like to thank the DOE; National Nuclear Security Administration, NA-211/Emerging Threats and Technologies Working Group (ETTWG) for funding this work.