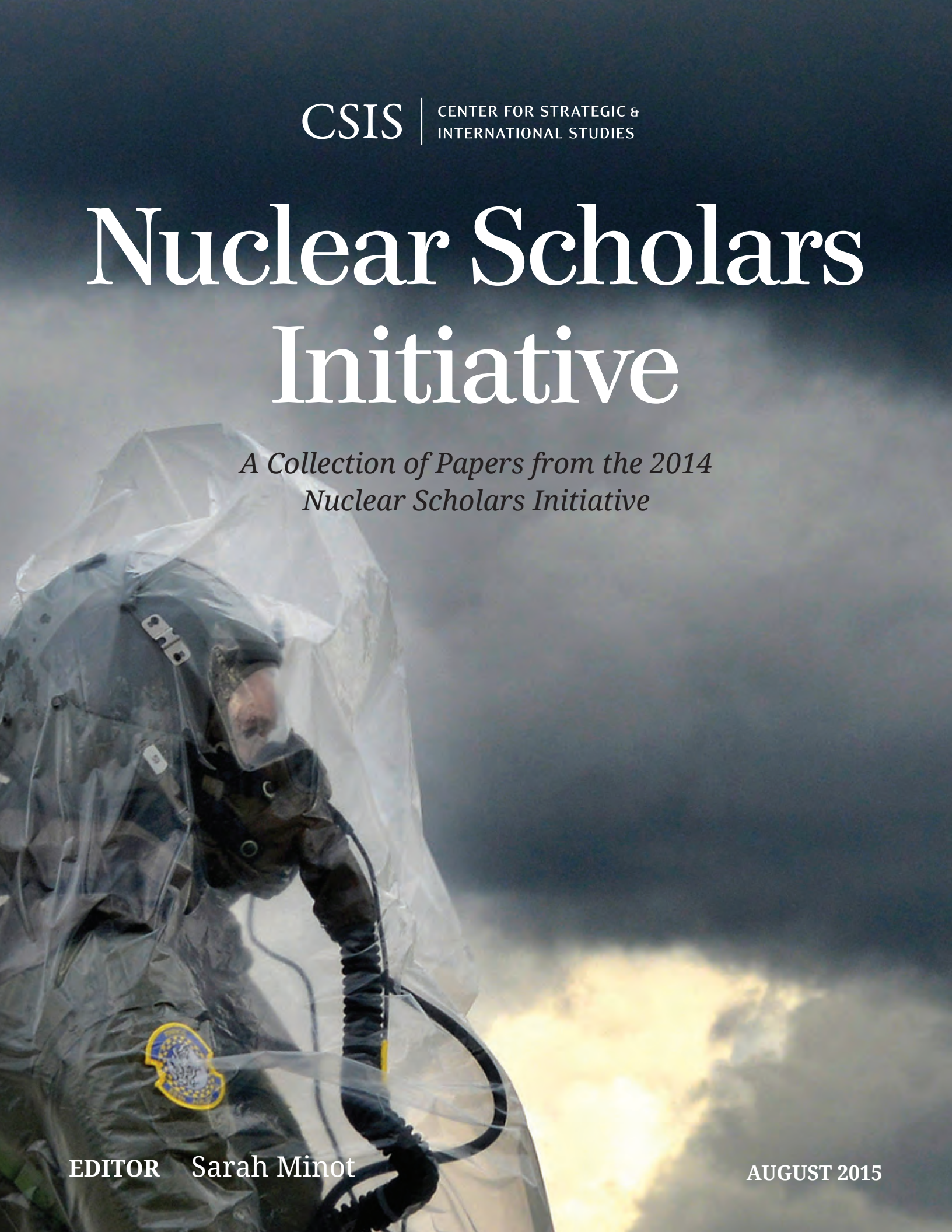
CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

Nuclear Scholars Initiative

A Collection of Papers from the 2014 Nuclear Scholars Initiative



EDITOR Sarah Minot

AUGUST 2015

Nuclear Scholars Initiative

A Collection of Papers from the 2014 Nuclear Scholars Initiative

EDITOR

Sarah Minot

AUTHORS

Seongjin James Ahn
Jerry Sergei Davydov
Matthew Fargo
Charles Goetz
Brian Gordon
Jooeun Kim
Alexander Lanoszka
Bonny Lin
Jonathan Moore
Carolyn Mullen
Blake Narendra
Abel Olguin
Elise Rowan
Lauren Rutledge
Travis Stalcup
Scott Stewart
Ariane Tabatabai
Julia Thompson
Jason Weaver
Nic Wondra

August 2015

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

ROWMAN & LITTLEFIELD

Lanham • Boulder • New York • London

About CSIS

For over 50 years, the Center for Strategic and International Studies (CSIS) has worked to develop solutions to the world's greatest policy challenges. Today, CSIS scholars are providing strategic insights and bipartisan policy solutions to help decisionmakers chart a course toward a better world.

CSIS is a nonprofit organization headquartered in Washington, D.C. The Center's 220 full-time staff and large network of affiliated scholars conduct research and analysis and develop policy initiatives that look into the future and anticipate change.

Founded at the height of the Cold War by David M. Abshire and Admiral Arleigh Burke, CSIS was dedicated to finding ways to sustain American prominence and prosperity as a force for good in the world. Since 1962, CSIS has become one of the world's preeminent international institutions focused on defense and security; regional stability; and transnational challenges ranging from energy and climate to global health and economic integration.

Former U.S. senator Sam Nunn has chaired the CSIS Board of Trustees since 1999. Former deputy secretary of defense John J. Hamre became the Center's president and chief executive officer in 2000.

CSIS does not take specific policy positions; accordingly, all views expressed herein should be understood to be solely those of the author(s).

About the CSIS Project on Nuclear Issues

Many of the most pressing national and international security challenges are tied to nuclear weapons. The need to reduce the prevalence of nuclear weapons globally and prevent their use by states and nonstate actors runs parallel with the need to maintain certain nuclear capabilities and the intellectual assets that support them. Both tracks present long-term challenges that, to be managed, will require sustained effort by talented and dedicated professionals. The Project on Nuclear Issues (PONI) seeks to help improve the effectiveness of U.S. nuclear strategy and policy through professional development and networking activities that target the next generation of leaders in the field.

PONI maintains an enterprise-wide membership base; hosts four major conferences and several smaller events each year; maintains an online blog; holds live debates on critical nuclear weapons issues; runs a six-month academic program for young experts; organizes bilateral exchanges involving young experts from the United States and abroad; and distributes regular news and event announcements to members. More information can be found at www.csis.org/isp/poni.

ISBN: 978-1-4422-4108-4 (pb); 978-1-4422-4109-1 (eBook)

Center for Strategic & International Studies
1616 Rhode Island Avenue, NW
Washington, DC 20036
202-887-0200 | www.csis.org

Rowman & Littlefield
4501 Forbes Boulevard
Lanham, MD 20706
301-459-3366 | www.rowman.com

A Perfect Record: Assessing Risk and the Human Factor in Avoiding Nuclear Catastrophe

Elise Rowan[1]

Despite a number of close calls and accidents involving nuclear weapons and warheads throughout the nuclear age, there has never been an accidental detonation of a nuclear warhead or an unauthorized, accidental, or miscalculated launch of a nuclear weapon. Robust safety and security technologies, policies, and procedures have been developed and refined over time to prevent such a catastrophic event, but the risk can never be fully eliminated. Risk assessment techniques are used to certify that U.S. nuclear weapon systems meet a set of qualitative and quantitative criteria, supporting their continued deployment. There are a number of challenges to assessing the risk of an event that has never before happened, including a limited pool of data to draw from, the difficulty of considering all possible failure scenarios, and the fact that risk assessments are subjective. The complicated "human factor"—the role of human error, performance, and judgment—may not be adequately considered in U.S. nuclear weapon risk assessments. The information available on U.S. risk assessments is limited, reflecting the sensitive nature of nuclear weapon-related information and provides limited assurance available to the public that the risk of a catastrophic nuclear weapons incident is low.

Introduction

In the 70 years since the beginning of the nuclear age, a nuclear warhead has never accidentally detonated or been launched without authorization, by accident, or as a result of miscalculation, despite a number of close calls.

1. Elise Rowan is communications officer at the Nuclear Threat Initiative in Washington, DC. Prior to her current role, she held positions with the Senate Foreign Relations Committee, the U.S. Department of State's Office of Weapons of Mass Destruction Terrorism, the Ploughshares Fund, and the Stimson Center's Managing Across Boundaries Program. She holds an MA in security policy studies with concentrations in transnational security policy and strategic communication from the Elliott School of International Affairs at the George Washington University and a BS in international business management and French from Butler University.

Catastrophic nuclear weapon incidents are considered to be low-probability, high-consequence events. Despite an impressive safety record and the implementation and refinement of safety and security protocols over time, the risk of an incident can never be completely eliminated. Indeed, there is a first time for every event.[2] Can this extraordinary record hold, or is it just a matter of time before human or system error gives way to catastrophe? And how sure can we be that we understand the risk effectively enough to mitigate it?

A former U.S. Air Force chief of staff once said, "The possibility of a launch of an ICBM [intercontinental ballistic missile] without the president's authorization is as close to zero as anything I can imagine."[3] On the other hand, former secretary of defense Robert McNamara and one of his successors, William J. Perry, have both highlighted the role of luck in the history of nuclear nonuse since 1945.[4]

This chapter provides a definition of risk and focuses on strategies used to assess the risk of catastrophic incidents involving nuclear weapons in the United States, including probabilistic risk assessment (PRA). Special attention is paid to the human factor—the role of human error, performance, and judgment—in the nuclear weapons enterprise. Finally, the broad outlines of U.S. risk assessment practices are described, with a particular focus on how the United States incorporates the human factor in its nuclear weapon risk assessments. Recent personnel issues and safety and security lapses within the U.S. Air Force's ICBM and bomber forces illustrate why the human factor should not be overlooked.

Information about nuclear weapon safety assessments, procedures, and practices is extremely sensitive, and most information about these details in the United States is classified. A number of sources have suggested that the practices followed to assess civil nuclear risk mirror those on the weapons side, making civilian nuclear risk assessments—for which there is more publicly available information—a useful proxy.[5] Valuable insights are also drawn from expertise and experience in other high-risk fields that use similar risk assessment techniques.

Catastrophic Nuclear Weapon Incidents: A Proposed Definition

This analysis focuses on the range of potential scenarios leading to nuclear yield not ordered by the requisite authority or ordered on the basis of inaccurate or misinterpreted

2. Scott D. Sagan, *The Limits of Safety: Organizations, Accidents, and Nuclear Weapons* (Princeton, NJ: Princeton University Press, 1993), 12.

3. Ibid., 248.

4. *The Fog of War*, directed by Errol Morris (Culver City, CA: Columbia TriStar Home Entertainment, 2004), DVD; William J. Perry, interview by Ben Goddard, January 26, 2008.

5. Christopher Stubbs, "The Interplay between Civilian and Military Nuclear Risk Assessment, and Sobering Lessons from Fukushima and the Space Shuttle," in *The Nuclear Enterprise: High-Consequence Accidents: How to Enhance Safety and Minimize Risks in Nuclear Weapons and Reactors*, ed. George P. Shultz and Sidney D. Drell (Stanford: Hoover Institution Press, 2012); Stacey Hendrickson and Stacey Durham, Sandia National Laboratories, telephone interview by Elise Rowan, July 30, 2014.

information. This includes an accidental detonation of a nuclear warhead, an unauthorized launch, an accidental launch, or an authorized launch based on miscalculation (e.g., a false warning of an attack). This list of potential incidents is based largely on accounts of "near misses" that did not result in nuclear yield but could have under slightly different circumstances. These categories cut across a range of possible safety- and security-based failure scenarios. The section below describes the range of potential incidents considered and brief historical anecdotes or notional examples of each.

ACCIDENTAL DETONATION

An accidental detonation is the detonation of a warhead due to warhead component malfunction. The warhead may be mated with a delivery vehicle or separate, and it occurs without the input signals required to arm, fuse, and fire a nuclear warhead.[6] This can be classified as a failure of one or more safety features, perhaps due to exposure to "extreme environmental insult," including fire, crush, or shock or to conditions that imitate deployment.[7] In the United States, the range of the potential environments to which a nuclear weapon might be exposed is detailed for each weapon system in a classified stockpile-to-target sequence (STS) document.

Almost all historical examples of close calls in this category occurred in the early decades of the nuclear age, when concerns in the United States about the weapons' effectiveness under deployment trumped safety. In 1961, a B-52 bomber flying airborne alert broke apart in midair and dropped two hydrogen bombs over Goldsboro, North Carolina. One of the bombs sustained nominal damage. On the other bomb, one safety switch broke during the crash and two became incapacitated when the aircraft broke apart. There were four switches total. A single safety switch prevented the bomb from detonating.[8] In the late 1960s, after a series of additional plane crashes involving nuclear weapons, the United States abandoned "Continuous Airborne Alert," a doctrine that kept U.S. nuclear weapons ready to launch from the air for 29 years.[9]

UNAUTHORIZED LAUNCH

An unauthorized launch refers to "deliberate launching or releasing of a nuclear missile or bomb (except jettisoning) before execution of an emergency war order."[10] An unauthorized launch might occur at the hands of an insider from the nuclear weapons establishment who does not have the proper authority to execute an order to launch a nuclear weapon, or

6. R. E. Kidder, *Report to U.S. Congress: Assessment of the Safety of U.S. Nuclear Weapons and Related Nuclear Test Requirements* (Livermore, CA: Lawrence Livermore National Laboratory, 1991), D-2, http://www.fas.org/resource/08062004142243.pdf.

7. David W. Plummer and William H. Greenwood, "The History of Nuclear Weapon Safety Devices" (paper submitted at Joint Propulsion Conference, American Institute of Aeronautics and Astronautics, 1998), 1.

8. Ed Pilkington, "US nearly detonated atomic bomb over north carolina—secret document," *Guardian*, September 20, 2013, http://www.theguardian.com/world/2013/sep/20/usaf-atomic-bomb-north-carolina-1961.

9. "SAC Airborne Alert," *National Museum of the United States Air Force*, http://web.archive.org/web/20090114035353/http://www.nationalmuseum.af.mil/factsheets/factsheet.asp?id=1851.

10. *Department of Defense Nuclear Weapon System Safety Manual*, U.S. Department of Defense, Number 3150.02, January 31, 2014, http://www.dtic.mil/whs/directives/corres/pdf/315002m.pdf.

it could be the result of an external actor. An unauthorized launch is initiated by intent and may stem from malfeasance.

There are no known examples of close calls in this category, though there have been cases involving the so-called insider threat in the area of nuclear materials security. *A Worst Practices Guide to Insider Threats* by Matthew Bunn and Scott Sagan, illustrates a number of dangerous assumptions that can be applied to a nuclear weapons context, including the beliefs that background checks are foolproof and organizational culture and employee disgruntlement will not negatively impact the mission.[11]

ACCIDENTAL LAUNCH

Also called an "inadvertent launch," an accidental launch is probably the most unlikely of the potential incidents considered and would most likely happen by way of nature, human error, or system or component failure.

The 1980 incident at Damascus, Arkansas, profiled in detail in *Command and Control* by Eric Schlosser, illustrates a variation of this incident type. Though not technically a launch, the accident happened when a technician dropped a wrench that punctured a liquid-fueled Titan II missile. The missile was ejected from its silo, and the warhead landed on a nearby roadside.[12] Fortunately, the weapon did not detonate.

MISCALCULATED LAUNCH

A miscalculated launch may be ordered rationally and follow procedure perfectly but is ultimately deemed a mistake. In this case, an order to launch could be based on misinformation, misinterpretation, or misjudgment, perhaps due to rushed decisionmaking as a result of the limited time available for the president (in the case of the United States) to respond to indications of a nuclear first strike.

Had events unfolded differently, a 1979 incident in which a training tape was mistaken for a massive incoming Soviet attack and a 1980 close call in which a computer chip malfunctioned and showed incoming Soviet missiles would have fallen into this category.[13]

A miscalculated launch could also take place as a result of a confluence of events in a tense political environment. Events during the Cuban Missile Crisis illustrate the potential for miscalculation. Throughout the 13-day crisis, when tensions between the United States and the Soviet Union were at an all-time high, a number of provocative events took place that could have led either side to believe its adversary was escalating or even launching a nuclear war. A planned test of an ICBM at Vandenberg Air Force Base took place as

11. Matthew Bunn and Scott D. Sagan, *A Worst Practices Guide to Insider Threats: Lessons from Past Mistakes* (Cambridge, MA: American Academy of Arts and Sciences, 2014).

12. Eric Schlosser, *Command and Control* (New York: Penguin Press, 2013).

13. For more on these incidents and other close calls, see Patricia Lewis et al., *Too Close for Comfort: Cases of Near Nuclear Use and Options for Policy* (London: Royal Institute of International Affairs, 2014), http://www.chathamhouse.org/publications/papers/view/199200; and Schlosser, *Command and Control.*

scheduled. A series of false warnings from radars detected indications of Soviet nuclear weapons launched from Cuba, and a U.S. U-2 spy plane mistakenly crossed from Alaska into Soviet airspace, resulting in a 300-mile chase by Soviet fighter planes. Coincidentally, the Alaskan U-2 incident occurred the same day another U.S. U-2 was shot down over Cuba, a move not ordered by centralized leadership in Moscow or Havana.[14] These incidents illustrate the array of actors, aside from the central leadership in Washington, who have responsibility over nuclear weapons in some capacity in the United States.

Defining and Measuring Risk

Before we can conceptualize the risk of a catastrophic nuclear weapon incident, it is essential to first understand what is meant by "risk." According to scholars Stanley Kaplan and B. John Garrick, risk is the probability of a scenario occurring combined with the consequences of that scenario. It involves both uncertainty and the possibility of damage or loss.[15] Three fundamental questions are used to assess risk:[16]

1. What can happen? (i.e., What can go wrong?)
2. How likely is it that it will happen?
3. If it does happen, what are the consequences?

To assess these questions and measure risk in complex systems where the data pool of events is small or even zero, such as with nuclear weapons, PRA is useful. PRA breaks down a complex system into subsystems and components for which there are data (or data can be extrapolated from models when data does not exist) to estimate the occurrence of a range of potential failures that could lead to an accident. PRA combines those scenarios to form an overall judgment about the integrity of a system.[17] Data from subsystems may come from component tests or judgments about the likelihood of an operator following a procedure according to protocol. Fault trees break down components, tasks, or procedures into a diagram, using data to assign a statistical probability to each possible outcome. A fault tree begins with an overall outcome—either a successful operation or failure—and elements that contribute to that outcome are shown underneath to demonstrate how a particular outcome might happen.[18] Event trees are also used in PRA to profile the potential consequences of an initiating event, and possible outcomes and consequences are recorded based on a variety of potential intervening actions listed within the pyramid.

---

14. Sagan, *Limits of Safety*, 78–80, 122–134, 135–140.
15. Stanley Kaplan and B. John Garrick, "On the Quantitative Definition of Risk," *Risk Analysis* 1 (1981): 12–13.
16. Ibid.
17. Vicki M. Bier, "Challenges to the Acceptability of Probabilistic Risk Assessment," *Risk Analysis* 19 (1999): 704.
18. James Reason and Michael Maddox, "Chapter 14: Human Error," in *Human Factors Guide for Aviation Maintenance*, ed. Michael Maddox (Washington, DC: Federal Aviation Administration, 1998).

Conventional or Gaussian statistical methods cannot meaningfully model the risk of catastrophic events for which there is little to no data. Conventional statistics employ the standard bell curve to represent event frequency, but for rare events the focus is on the extreme ends or "tails" of the curve. Thus, PRA is represented by a family of curves representing components of the system and, ultimately, by a cumulative probability curve that shows confidence measures for the risk assessment.

CHALLENGES TO RISK ASSESSMENTS

There are a number of challenges relevant to assessing nuclear weapon risks that shed light on the fallibility and potential shortcomings of these assessments.

Completing the Scenario List

Risk assessors must identify all the potential hazards, risky components, and ways in which a system could fail and lead to an accident, a process that is subjective and not absolute. As Christopher Stubbs writes, "What about situations that we weren't clever enough to incorporate into our probabilistic risk models?"[19] Omitting a crucial scenario from a model can impact the assessment's accuracy.

Narrow Base of Experience

PRA deals with events for which there is often no past experience, making it necessary to extrapolate using Bayesian statistical models. Experts disagree on the accuracy and reliability of these extrapolations, and some experts question the credibility they lend to risk assessments.[20] The National Academies of Science recognized the difficulty in quantifying the probability of possible attack scenarios at nuclear weapon and nuclear material storage facilities and advised against relying on PRA to improve security at U.S. National Nuclear Security Administration sites.[21]

Identifying and Estimating Correlations

In developing a list of possible failure scenarios or components that might fail, it is essential that each scenario or component is truly independent. With nuclear weapons, as with any complex system, it is difficult to identify, estimate, and incorporate correlations into risk assessments, especially if the correlations are subtle or if they may only be apparent as a result of a severe external insult to the system.[22] If events are independent, the probability of them occurring together amounts to the product of the marginal probabilities of each, but if they are dependent, simply multiplying their respective probabilities together

19. Stubbs, "Interplay between Civilian and Military Nuclear Risk Assessment," 101.
20. Ibid., 100.
21. National Research Council, *Understanding and Managing Risk in Security Systems for the DOE Nuclear Weapons Complex* (Washington, DC: National Academies Press, 2011).
22. Stubbs, "Interplay between Civilian and Military Nuclear Risk Assessment," 98–99.

may underestimate the risk and undermine the risk assessment.[23] Similarly, unplanned or unforeseen interactions between redundant safety components applied to ensure reliability may initiate a common-mode error, causing all the components to fail.[24]

The Subjective Nature of Risk Assessments

Risk assessments are inherently subjective because they require individuals to classify a scenario as risky and then fold assumptions about the consequences into a model. "Red-teaming," or engaging a team of experts to challenge assumptions, is a helpful antidote but not a panacea.

Risk assessments are also often conducted by parochial actors who have a vested interest in demonstrating that the system they manage has low risk.[25] In the nuclear weapons realm, this is a particularly potent question given that the national laboratories, the Department of Energy (DOE), and the Department of Defense (DOD)—the organizations that built, maintain, and deploy U.S. nuclear weapons—assess the safety and security of the U.S. nuclear weapons stockpile annually.

The Human Factor

The challenge of incorporating the varied and sometimes unpredictable role of humans in nuclear risk assessments deserves more attention. As Scott Sagan writes, "Why have imperfect humans, working in imperfect organizations and operating imperfect machines, been so successful?"[26] It is tempting to equate the so-called human factor with human error, but in reality, the human factor is much more complicated. It encompasses human error, performance, and judgment, which can impact nuclear weapon system safety and security positively or negatively. Subjectivity, as noted above, is one manifestation of the human factor and is present in nuclear weapon design, maintenance, deployment, and risk assessment.

Human judgment adds a fascinating layer. Scrutiny of past close calls has focused largely on human error and technical failures and less on the judgment of individuals who, in all cases of near nuclear use so far, have resisted launching nuclear weapons, sometimes against protocol.[27] For instance, in the dozens of examples in the literature of false warnings—caused by faulty computer chips, training tapes mistaken for actual events, and failures in communication—caution and critical thinking led to what was later determined to be the "appropriate" outcome.

---

23. Elisabeth Paté-Cornell, "On 'Black Swans' and 'Perfect Storms': Risk Analysis and Management When Statistics Are Not Enough," *Risk Analysis* 32 (2012): 1825, 2014, doi: 10.1111/j.1539-6924.2011.01787.x.
24. Scott Sagan, "The Problem of Redundancy Problem: Why More Nuclear Security Forces May Produce Less Nuclear Security," *Risk Analysis* 24 (2004): 937, doi: 10.1111/j.0272-4332.2004.00495.x.
25. Bier, "Challenges to the Acceptance of Probabilistic Risk Analysis," 705.
26. Sagan, *Limits of Safety*, 4.
27. Lewis et al., *Too Close for Comfort*, 2.

The human factor touches many different fields of study, including organizational behavior, ergonomics, and behavioral psychology. These are areas of extensive scholarship, and this section will merely attempt to highlight relevant concepts for nuclear weapon accidents and nuclear risk assessments.

HUMAN ERROR

Human error is "an identifiable human action that in retrospect is seen as being the cause of an unwanted outcome."[28] The concept seems straightforward, but there is some debate about what should be considered human error. Frederick Hansen argues that the inclusion of "slips, lapses, violations, and blunders" when referring to human error overstates the concept, though broadening the term highlights the true dynamics of human involvement in accidents.[29]

Other scholars rightly include these types of actions in the definition of human error. Slips are errors of execution on routine tasks that have been practiced many times and can include omitting a step on a checklist—known as an "error of omission"—or a clumsy action that disrupts the procedure—an "error of commission." Errors of omission are generally easier to catalog because they are based on steps of a well-defined operating procedure. Conversely, errors of commission are more difficult to model in a risk assessment because of the enormous variety of actions a person could take.[30]

A higher-level type of error is a mistake. These can be "rule-based mistakes," where an operator misapplies a correctly chosen course of action (a rule) to solve a problem or follows a rule or procedure that is wrong for the circumstances. Alternatively, an operator may make a "knowledge-based mistake" when solving a novel problem for which there is no prepackaged procedure. This requires quick, independent thinking on the spot and is highly error prone.[31]

Violations and errors are the two types of human acts that cause failure. Errors are unintentional, whereas violations are usually deliberate. Violations are "deviations from safe operating procedures, recommended practices, rules or standards," and although they are generally intentional, the bad consequences that stem from them are not.[32] The most relevant type of violation for nuclear weapons management is a "necessary" or "situational violation," where an operator may feel the need to commit a violation in order to complete the mission. For example, there are numerous examples of launch officers violating protocol in response to a warning of a nuclear first strike because they deem the warning to be false.

---

28. Erik Hollnagel, "Human Reliability Assessment in Context," *Nuclear Engineering and Technology* 37 (2005): 159, http://www.kns.org/jknsfile/v37/JK0370159.pdf.
29. Frederick D. Hansen, "Human Error: A Concept Analysis," *Journal of Air Transportation* 11 (2006): 75.
30. Bier, "Challenges to the Acceptance of Probabilistic Risk Analysis," 706.
31. Reason and Maddox, "Chapter 14: Human Error."
32. Ibid.

These human-driven failures can be either "active" or "latent." Active failures are the result of errors or violations and have immediate consequences, whereas latent failures are usually introduced when a weapon or component is designed or when a procedure is developed and may not become apparent until much later.

A 2007 incident in which U.S. Air Force personnel mistakenly loaded and flew six nuclear-armed cruise missiles across the country serves as a potent example of human error in the management of nuclear weapons. Crews at the point of origin in Minot, North Dakota, and the destination at Barksdale Air Force base in Louisiana broke protocol throughout the operation and left the weapons on a runway overnight—unguarded and unaccounted for—for 36 hours. What might have happened had the B-52 crashed or caught on fire? The airmen would not have known to invoke the emergency procedures required when transporting nuclear weapons—posing a potentially serious threat to those along the flight path.[33]

PERFORMANCE SHAPING FACTORS

Engineers incorporating human error into PRA have tended to use simple probability trees and basic assumptions about human error probabilities,[34] but there is a general consensus among those who study risk and human factors that assessments would be more meaningful if they accounted for organizational, environmental, and cultural performance shaping factors.[35]

Organizational Factors

Scott Sagan has done extensive work on the role of system or organizational factors in nuclear weapon accidents. In *The Limits of Safety*, Sagan applies two organizational theories to nuclear weapons management, using close calls from history to evaluate which theory is most relevant. He finds that the more pessimistic "normal accidents theory" fits most closely with U.S. nuclear weapon policies. According to the theory, accidents are inevitable if organizations managing hazardous technology have system components that can fail simultaneously and in unexpected ways ("high interactive complexity") and when these failures can escalate out of control rapidly ("tight coupling").[36] This is especially true when human operators must follow procedures in a strict sequence and on a short timescale, as with nuclear weapons. Essentially, Sagan argues that the U.S. systems we have built in the name of nuclear deterrence are laden with potential latent failures.[37]

---

33. Scott D. Sagan, "On the Brink," review of *Command and Control: Nuclear Weapons, the Damascus Accident, and the Illusion of Safety* by Eric Schlosser, *American Scholar* (autumn 2013), http://theamericanscholar.org/on-the-brink/#.U9bGJkDDaSo.
34. Bier, "Challenges to the Acceptance of Probabilistic Risk Analysis," 707.
35. See Reason and Maddox, "Chapter 14: Human Error"; Hollnagel, "Human Reliability Assessment in Context"; and Bier, "Challenges to the Acceptance of Probabilistic Risk Analysis," 707.
36. Sagan, *Limits of Safety*, 44.
37. Ibid., 276.

Sagan also highlights how organizational culture might enable failures. Members of the U.S. military—and nuclear launch officers in particular—experience extreme socialization, strict discipline, and isolation from broader society. This suggests that individuals within the nuclear command and control structure are part of a "total institution," where the overall mission conflicts with more self-serving organizational interests, such as self-preservation. This coexistence can "encourage excessive loyalty and secrecy, disdain for outside expertise, and in some cases even cover-ups of safety problems, in order to protect the reputation of the institution."[38]

How personnel are managed is also relevant to nuclear risk reduction. Whether workers are disgruntled, whether they feel there is a clearly defined path for career advancement, and whether lower-level operators feel frustrated by their lack of influence over policy are all organizational factors that may contribute to nuclear safety and security, as illustrated by recent scandals within the U.S. ICBM force.[39]

Environmental and Cultural Factors

Factors affecting the operator's local environment can also contribute to errors and violations. Examples of these factors include fatigue due to long shifts, stress, pressure to perform perfectly, adverse physical environmental conditions (e.g., hot and confined spaces), inadequacy of training, and availability of procedures or plans.

National culture may also impact performance in a crisis. For example, the Japanese cultural tendency to make decisions collectively may have been a barrier to timely action to mitigate the Fukushima nuclear disaster.[40] Although this example is on the civil nuclear side, its relevance and application to nuclear command and control is obvious.

ASSESSING THE HUMAN FACTOR IN RISK MODELS

The human factor is thought to have contributed to 70 to 90 percent of past accidents in other complex, high-risk systems (nuclear power and civil aviation, for example).[41] As Erik Hollnagel writes, "Since no system has ever built itself, since very few systems operate themselves, and since furthermore no systems maintain themselves, the search for a human in the path of events leading to a failure is bound to succeed."[42]

Anticipating how a human might commit an unsafe act is less straightforward. Human reliability assessment (HRA) is used to estimate the occurrence of human errors, and the earliest and most widely implemented HRA methods were modeled on PRA in order to easily incorporate the results into PRA fault trees. These early methods used estimated

38. Ibid., 252–254.
39. Robert Burns, "Nuclear Weapons Investigation," *Associated Press*, http://www.ap.org/index/ap-in-the-news/us-nuclear-weapons.
40. Richard Harris, "What Went Wrong in Fukushima: The Human Factor," *National Public Radio*, July 5, 2011, http://www.npr.org/2011/07/05/137611026/what-went-wrong-in-fukushima-the-human-factor.
41. Hollnagel, "Human Reliability Assessment in Context," 160.
42. Ibid.

probabilities of whether an operator will succeed or fail at a certain task and assumed that human failure can be decomposed like a system or component. [43]

The first-generation HRA method of predicting human error probabilities (still used in the global civilian nuclear enterprise) has been replaced in newer second-generation models of HRA in favor of examining variability in human performance as a more useful measure of the human contribution. These second-generation methods also recognize that context may be an error-forcing condition and thus account for performance shaping factors.[44]

Illustrating a first-generation HRA approach, Niles T. Welch walks through the tasks required by a navy operator for a particular procedure. In referring to the first step, he writes, "If the power button is pushed when connections are not completely seated, the operator may be injured and/or the equipment damaged. However, since the operator is well trained, the likelihood of an error at this step is highly remote (human error probability $= 1 \times 10^{-6}$)."[45]

Welch does not provide any supporting evidence as to why that specific human error probability is assigned to that task or any other task within the procedure, raising questions about the reliability of the overall analysis.

Second-generation models are still being developed, and many have yet to be empirically validated, but the recognition they give to the variability of human performance and the role of context are promising.[46]

Assessing the Risk of a Catastrophic Nuclear Weapon Incident in the United States

The United States employs a variety of risk assessment techniques to evaluate the risk of a catastrophic nuclear weapon incident and the range of potential safety and security failures that could lead to such an event. The full spectrum of methods and assumptions employed to evaluate risks is not available to the public, but this analysis attempts to describe U.S. practices broadly. Without complete information, it is impossible to make a judgment about the adequacy of U.S. risk assessment efforts, but questions are raised for further investigation.

43. Ibid.
44. Julie Bell and Justin Holroyd, *Review of human reliability assessment methods*, prepared by Health and Safety Laboratory for the Health and Safety Executive, RR679 (Derbyshire, UK: Crown, 2009), 8, http://www.hse.gov.uk/research/rrpdf/rr679.pdf.
45. Niles T. Welch, "Human Error Risk Assessment," *Professional Safety* 43 (1998): 19.
46. Bell and Holroyd, *Review of human reliability assessment methods*, 8.

MEETING QUANTITATIVE STANDARDS

Every year, the United States assesses the safety, security, and reliability of its nuclear weapons arsenal. Through modeling, component testing, surveillance, and risk assessment, members of the U.S. nuclear weapons establishment certify that the weapons in the arsenal meet a set of safety criteria throughout the range of environments to which a nuclear weapon might be exposed. The secretaries of energy and defense communicate that judgment in a letter to the president.[47]

Regarding the potential for accidents, the U.S. nuclear weapons establishment assesses the stockpile's safety against the 1968 "Walske Criteria," which states that the probability of a premature nuclear warhead detonation (due to component malfunctions and without any input signals) should not exceed 1 in 10^9 per warhead lifetime for "normal environments" and 1 in 10^6 when exposed to an "abnormal environment" or accident.[48] The Walske probabilities do not account for the likelihood of an accident—an airplane fire, for example—but for the probability of getting nuclear yield assuming the accident or malfunction has already happened.[49]

An STS document for each weapon type considers the range of possible physical environments to which a nuclear weapon may be exposed throughout its lifecycle—from stockpiling to deployment—and categorizes these environments as "normal" (expected) or "abnormal" (unexpected or likely to cause the weapon to lose full operational capability). According to the 2014 DOD *Nuclear Weapon System Safety Program Manual*, "Credible combinations of abnormal environments pose an additional risk to nuclear weapon systems and may not have been tested extensively for their combined effects."[50]

STS documents focus only on physical environments (fire, explosion, vibration, and temperature) and not necessarily on the human factors that could contribute to those environments or to the management of the weapon from stockpiling to deployment.[51] Human error probabilities during manufacture, assembly, testing, monitoring, quality control, and surveillance by the labs are folded into the quantitative nuclear weapon risk assessments that certify that the U.S. nuclear weapons arsenal meets the Walske Criteria,[52] but the integration of human error probabilities may not be completed for deployment scenarios.

This annual assessment process focuses on the warhead itself and involves testing safety features and components within the warhead meant to safeguard against an

47. For a thorough description of the annual assessment process, see Gene Aloise, *Nuclear Weapons: Annual Assessment of the Safety, Performance, and Reliability of the Nation's Stockpile*, GAO-07-243R+(Washington, DC: U.S Government Accountability Office, 2007).

48. U.S. Department of Defense, *Nuclear Weapon System Safety Program Manual*, 3150.02 (Washington, DC: Department of Defense, 2014) 15.

49. Jason Weaver, e-mail message to author, July 10, 2014.

50. U.S. Department of Defense, *Nuclear Weapon System Safety Program Manual*, 39.

51. John Harvey, telephone interview by Elise Rowan, June 12, 2014.

52. Jason Weaver, e-mail message to author, July 10, 2014, and Hendrickson and Durham, interview by Elise Rowan.

accidental or unauthorized detonation. If the surety of these individual components is confirmed, the cumulative probability of their success meets the quantitative safety requirements. This determination is reached using PRA and, increasingly, a technique called Quantification of Margins of Uncertainty (QMU). Today, QMU quantifies confidence that a nuclear weapon will operate as intended; this approach is evolving to assess safety as well.[53]

Outside experts and advisory groups, such as the JASONs and the Defense Science Board, review surety assessments, and their feedback is sometimes incorporated to strengthen safety over specific portions of the STS.[54] External oversight—from production to deployment—is a crucial tool for accountability and for ensuring the surety of the stockpile.

MEETING QUALITATIVE STANDARDS

The Departments of Defense and Energy, including the national laboratories, also adhere to qualitative safety and security standards to prevent accidental or unauthorized launch. These standards call for "positive measures" to protect against catastrophic nuclear weapon incidents.[55] Positive measures include a design feature, procedure, or device (described above and evaluated using PRA and QMU) to protect against human and system failure. They are applied in a layered approach to reduce the likelihood that an accident could happen due to failure of a single component.[56] Taken together, these measures provide "defense-in-depth" and have been informed by decades of lessons learned through the management of nuclear weapons. Though they are not the focus of this chapter, it is essential to note that these technologies, policies, and procedures are the U.S. nuclear enterprise's response to risk of an accidental detonation and unauthorized, accidental, or miscalculated launch.[57]

The annual *Nuclear Weapons Surety Report* details any safety, security, and use control incidents over the past year—including applicable human performance components—and provides information about efforts to improve nuclear surety, such as force-on-force exercises to strengthen nuclear security.

Other assessments used to measure the risk of an accidental detonation or an unauthorized or accidental launch are called Unauthorized Launch Analyses (ULAs) and Inadvertent Launch Analyses (ILAs). Unlike the annual assessment undertaken by the nuclear weapons enterprise, these methods consider the warhead and the warhead's delivery vehicle as well as command and control and support elements. According to DOD, they can be qualitative

53. National Research Council, *Evaluation of Quantification of Margins and Uncertainties Methodology for Assessing and Certifying the Reliability of the Nuclear Stockpile* (Washington, DC: National Academies Press, 2008), http://www.nap.edu/download.php?record_id=12531#.

54. John Harvey, e-mail message to author, July 18, 2014.

55. Kidder, "Report to Congress," D-2.

56. Ibid.

57. For a discussion of specific nuclear weapon safety devices and measures, see Jason Weaver, "One in a Million, Given the Accident: Assuring Nuclear Weapon Safety," *Nuclear Scholars Initiative: A Collection of Papers from the 2014 Nuclear Scholars Initiative* (Washington, DC: CSIS, 2014).

or quantitative and are used to "analyze technical malfunctions, natural events, human errors, and malicious acts that could result in the inadvertent or unauthorized use of a nuclear weapon."[58] A ULA is meant to shed light on elements of a nuclear weapon system's design that could be vulnerable to malfeasance. It considers the range of human actions that could circumvent nuclear weapon safety measures. An ILA looks at what could go wrong with the weapon system to lead to an accidental launch. Human error, component failure, and combinations of the two are evaluated using fault trees and PRA. These techniques are used when there is enough weapon system design data and are updated periodically when the weapon system undergoes changes or when DOD or DOE requests an updated assessment.[59]

DOD recognizes the role of the human factor "in the degradation of nuclear weapon surety standards through noncompliance with established safety policy or guidance" and states that the Nuclear Weapon System Surety Group, an interagency body with jurisdiction over nuclear weapon surety in the United States, will consider the results of quantitative and qualitative ULAs and ILAs.[60] Yet there is no publicly available description for how these results are used and against what standards.

Conclusion

The United States may be the most advanced state with respect to nuclear surety, given its seven decades of experience with nuclear weapons, extensive test record, and expansive nuclear enterprise. Other countries' safety systems, in particular—and the methods used to assess their vulnerabilities—may not be as rigorous and may pose significant risks. Yet, U.S. safety and security systems are fallible, making the risk of a catastrophic incident with nuclear weapons credible, however unlikely such an incident may be. The intrinsic shortcomings of risk assessments, coupled with the complexity of nuclear weapon systems, may mean that we are underestimating the risk and overestimating the system's surety.

The management and deployment of nuclear weapons is inherently risky, and the role of humans may not be adequately factored into risk assessments. To address this, the United States—and all countries with nuclear weapons—should focus efforts to better understand human factors with respect to nuclear weapons and work to vet and integrate second-generation HRA methods into risk assessments. Incorporating the true nature of human performance, including the impact of performance shaping factors, will improve understanding of nuclear safety and security. The U.S. Air Force's recent troubles present an opportunity for the nuclear enterprise to shift focus toward human and organizational factors.

Additionally, more information should be available to the public about how nuclear weapon risks are assessed and how the United States determines what level of risk is

58. U.S. Department of Defense, *Nuclear Weapon System Safety Program Manual*, 39.
59. Ibid., 40–41.
60. Ibid., 39.

acceptable. Specific information that could jeopardize nuclear weapon safety and command and control should remain secret, but some insight into the process of assessing risk and assurances that risks are being mitigated effectively would boost public confidence. A modified, unclassified version of one of the existing annual reports, or a new report altogether that provides a comprehensive overview of the risks and how they are assessed and addressed, could be a valuable tool for public oversight. The consequences of an incident with nuclear weapons would be horrific, making this a matter of extreme relevance to publics around the world.