A LIMIT TO SAFETY

Risk, 'normal accidents', and nuclear weapons

By Dr John Borrie
ILPI-UNIDIR Vienna Conference Series

Paper N° 3 of 6
#HINW14vienna

- Although improvements in managing nuclear weapons might reduce risk, factors like competing organizational agendas, biases, human frailty and the incomprehensibility of systems failures to their designers and operators mean that risk cannot be eliminated.
- One difficulty in assessing risk of detonation of nuclear weapons is due to lack of transparency on the part of possessors about their safety records. This serves to detract from claims that nuclear deterrence is safe or sustainable.
- At the same time, evidence from catastrophic accidents involving hazardous technologies of various kinds indicates that significant risk is endemic in complex and tightly coupled systems, as nuclear weapon control systems must be if nuclear deterrence is to function.

Introduction

Assessing the risk of detonation of nuclear weapons is an important if challenging aspect of understanding the humanitarian impacts of these arms (see Box 1). Risk in basic terms is the possibility of some bad event happening, something commonly quantified as the probability of an event multiplied by its consequences.[1] Proponents of nuclear deterrence have argued that the risk of nuclear weapon detonations in populated areas is very low because the probability is almost non-existent. In this view, the catastrophic humanitarian consequences arising from the use of nuclear weapons in populated areas are actually key to the nuclear deterrence concept: possessors' awareness of these consequences ensures that they take all necessary steps to ensure nuclear weapons are never exploded.[2] The absence of nuclear weapon detonations in populated areas since 1945 is sometimes put forward as proof of the validity of their position.[3]

Viewing nuclear weapons in this way raises issues. One questionable assumption is that the past is necessarily a reliable guide to comparatively rare but catastrophic future events (see Box 2). Another is whether, in the long run, it is feasible to exert sufficient control over nuclear weapons to prevent nuclear detonations from occurring, whether deliberately or inadvertently caused. Evidence from catastrophic accidents in-

Dr John Borrie is a senior researcher and policy advisor at UNIDIR.
The author thanks Dr. Seth Baum and Dr. Pavel Podvig for their comments.

BOX 1

QUANTIFYING THE PROBABILITY OF NUCLEAR WEAPON DETONATIONS IN POPULATED AREAS

The risk of nuclear weapons being detonated in populated areas (for whatever reason, not only nuclear war) is very difficult to quantify because the probability is uncertain. Estimates since the cold war ended have varied widely in their nature, but all depend on sets of assumptions that are subjective and therefore contestable.[4] However, scholars of catastrophic risk have observed that even considering order-of-magnitude estimates of probability can be informative.[5] Most people, for instance, would not board a commercial aircraft if the chances of it crashing were in the range of one chance in 1,000, or even one chance in 10,000—even if the precise probability were not known. Thus, an important question is: what is 'acceptable' probability for use of nuclear weapons, given that the consequences of use could end human civilization? And, if this range is unacceptable, what steps should the international community take (and what costs should it be willing to bear) to reduce that probability significantly?[6]

volving hazardous technologies ranging from human space flight, deep-water drilling, maritime shipping, chemical plants and nuclear power reactors indicates that certain risks are endemic to such systems. In that regard, this short paper introduces the reader to what is termed 'normal accident theory' and the limits of safety in managing complex, 'tightly coupled' nuclear weapon alert and launch control systems. A third questionable assumption—one explored later in this paper—is that the past is devoid of near-use of nuclear weapons.

Organizational and individual biases

The organizational systems involved in the development, production, storage, maintenance, deployment, safety and security of nuclear weapons are enormously complex. This is in addition to the complexity of systems involved in the detection of and response to incoming nuclear attack. Moreover, for nuclear deterrence to function, these systems must interact in order for nuclear weapons to be available to the operator to use at all. Yet it has been observed that the requirements for ironclad safeguards to prevent the inadvertent detonation of nuclear weapons while ensuring a convincing performance of the wartime mission pose daunting challenges. Writing of cold war-era American and Soviet nuclear command and control systems (but noting that it applies to any nuclear rivalry), Blair found that these 'requirements clashed, especially in crisis circumstances. Measures that would facilitate the speedy, deliberate use of nuclear weapons competed with measures that would minimize the risk of their aberrant use, and vice versa.'[7]

In 1993, Sagan described two schools of thought in the scholarly literature on complex organizations:

BOX 2

THE THANKSGIVING TURKEY AND THE PROBLEM OF INDUCTION

Nassim Nicholas Taleb, in his book The Black Swan, related a variant of the philosopher Bertrand Russell's illustration of the problem of induction—'certainly the mother of all problems in life':

'Consider a turkey that is fed every day. Every single feeding will firm up the bird's belief that it is the general rule of life to be fed every day by friendly members of the human race "looking out for its best interests," as a politician would say. On the afternoon of the Wednesday before Thanksgiving [an annual holiday in the United States that almost invariably involves a Turkey roast], something unexpected will happen to the turkey. It will involve a revision of belief.'[26]

A real-world example is the outbreak of the First World War, which was a surprise in the sense that since the Napoleonic conflicts ended a century before, Europe experienced a period of peace that would lead any observer to believe in the disappearance of severely destructive wars. August 1914 brought with it a stark revision of belief.

Taleb observed that the turkey problem is generalizable to any situation in which 'the same hand that feeds you can be the one that wrings your neck.'[27] The problem of induction also applies to the claim that because nuclear deterrence has not resulted in the detonation of nuclear weapons in populated areas since 1945 there is little likelihood of it happening in future. Past experience is not of unconditional benefit here.

TABLE 1

COMPETING PERSPECTIVES ON SAFETY WITH HAZARDOUS TECHNOLOGIES

HIGH RELIABILITY THEORY	NORMAL ACCIDENTS THEORY
Accidents can be prevented through good organizational design and management.	Accidents are inevitable in complex and tightly coupled systems.
Safety is the priority organizational objective.	Safety is one of a number of competing objectives.
Redundancy enhances safety: duplication and overlap can make 'a reliable system out of unreliable parts.'	Redundancy often causes accidents: it increases interactive complexity and opaqueness and encourages risk-taking.
Decentralized decision-making is needed to permit prompt and flexible field-level responses to surprises.	Organization contradiction: decentralization is needed for complexity, but centralization is needed for tightly coupled systems.
A 'culture of reliability' will enhance safety by encouraging uniform and appropriate responses by field-level operators.	A military model of intense discipline, socialization, and isolation is incompatible with democratic values.
Continuous operations, training, and simulations can create and maintain high reliability operations.	Organizations cannot train for unimagined, highly dangerous, or politically unpalatable operations.
Trial and error learning from accidents can be effective, and can be supplemented by anticipation and simulations.	Denial of responsibility, faulty reporting, and reconstruction of history cripples learning efforts.

Reproduced from Sagan, *The Limits of Safety*, Princeton University Press, 1993, p. 46.

> 'The first is the optimistic view [...] "high reliability theory", whose proponents argue that extremely safe operations are possible, even with extremely hazardous technologies, if appropriate organizational design and management techniques are followed. The second school, [...] "normal accidents theory", presents a much more pessimistic prediction: serious accidents with complex high technology systems are inevitable.'[8]

The high reliability view is grounded on the plausible belief that properly designed and managed organizations can compensate for human frailties, and can be more rational and effective than individuals (see Table 1).[9]

> ...organizations are not necessarily particularly rational or effective in delivering safe outcomes

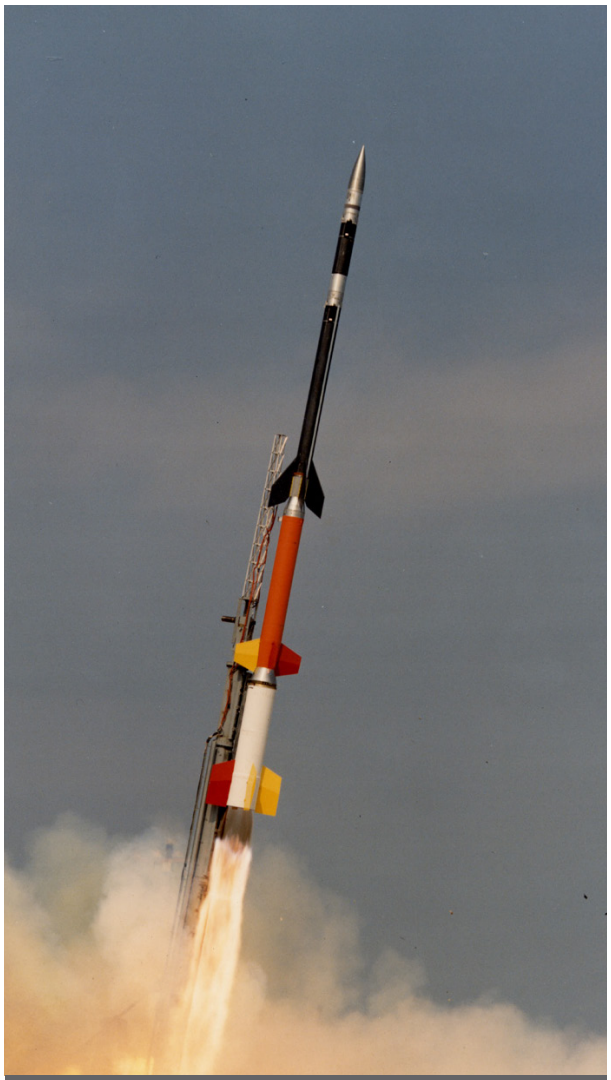
A problem with the high reliability view is that there is ample evidence to show that organizations are not necessarily particularly rational or effective in delivering safe outcomes in the face of complex, tightly coupled systems (explained in the next section). For instance, a recent study by Chatham House catalogued many historical instances in which organizational or technical systems failed or offered ambiguous signals, so that individual judgment at odds with those systems was all that stood in the way of nuclear weapons use (see Table 2).[10] Yet, as nuclear weapons are so hazardous, even rare instances of combined technical and human operator failure contain potential for the detonation of nuclear weapons in populated areas.

One problem is that organizations suffer from biases of various kinds—just as individuals do—and have a tendency to 'develop myths, fictions, legends, folklore, and illusions'[11] that impede learning or improvements to safety, even when lessons suggest themselves. This tendency extends to bureaucratic and political imperatives. In the 1970s, for example, the United States Air Force resisted proposals from nuclear scientists at the Sandia National Laboratory to install additional safety measures in nuclear warheads because the military wanted to spend its budget on new weapons, not on fixing problems with existing ones—despite demonstrable risk of serious accident.[12] The United States also kept obsolescent and liquid-fuelled (and thus especially hazard-prone) land-based Titan intercontinental ballistic missiles in service longer than it was safe to do so, as bargaining chips for arms control negotiations with the Soviet Union (see Box 3).[13] These examples illustrate that organizations or their leaders cannot always be counted upon to do what is safest in risk-reduction terms where nuclear weapons are concerned.

‘Normal’ accidents

Even if these issues could always be dealt with through organizational management and improvement, a major issue is also the nature of the systems themselves involved in the control of hazardous technologies like nuclear weapons. Because of the way in which such systems are tied together, unexpected failures can quickly multiply and interact in ways that no one can predict, or respond to quickly or effectively enough to avert disaster because of their incomprehensibility for a time to the operators.

This is the essence of the ‘normal’ or ‘system’ accident, a term coined by the American sociologist, Charles Perrow, who studied the control of hazardous technologies such as nuclear power plants.



A Black Brant 12 sounding rocket, launching from Wallops Flight Facility. This was the same type of rocket that caused the Black Brant scare (see Table 2) in 1995 (Photo: National Aeronautics and Space Administration).

Perrow noted that the failure of individual components or items is a ubiquitous feature of almost all systems. However, in complex systems component failures can create complex interactions, which are unfamiliar, or unplanned or unexpected sequences in the system that are either not visible or not immediately comprehensible to operators. This is what happened on 3 June 1980 at a time of high tension during the cold war when a computer chip failed at the United States military’s North American Aerospace Defense Command (NORAD) headquarters: NORAD’s computers told operators that the Soviet Union had just launched a massive nuclear missile attack against the United States. It was a false alarm, but it took some time to establish this and trace the problem (see Table 2).[14]

Just as seriously, common-mode components of a system can fail; that is, components that have more than one function. This is something that can make quick, accurate diagnosis of a fault, or efforts to fix it, especially difficult. Automation of controls can sometimes help. But automation decreases the flexibility of the operator to correct minor failures before they become major ones, or it can mask problems altogether.

Complex systems are not necessarily prone to catastrophic failure: it depends on how tightly they are coupled. Tight coupling means that ‘there is no slack or buffer or give between two items. What happens in one directly affects what happens in the other.’[15] Because of the tightly coupled nature of nuclear weapons on high-alert status, some governments and experts have long called for nuclear de-alerting—in effect, to make the alert and launch control systems for nuclear weapons less responsive.[16] However, for the reasons explained above, catastrophic failures involving nuclear weapon detonation are conceivable not just in high-alert situations (although the risk may be particularly acute then) but also more generally. This is a situation the end of the cold war and nuclear arms reductions do not fundamentally alter, especially as the United States and Russia each still have approximately 1,640 strategic nuclear warheads deployed[17] (not to mention the smaller nuclear forces of seven other nuclear weapon possessor states).

Eric Schlosser, an American investigative journalist, documented many accidents involving nuclear weapons in a recent book focusing on United

States command and control of its arsenal during the cold war. Fortunately none of these cases resulted in nuclear weapon detonations, although some appeared to come close (see Box 3). Schlosser argued that, rather than this being a cause for confidence in the systems in place or complacency, it should instead be cause for alarm about the characteristics of these systems in the first place. Moreover, to use Perrow's terminology, the many examples show how resistant these systems are to efforts to purge them of potential for multiple failures that can rapidly spiral toward disaster. And the United States is by no means alone, although as one expert recently noted, 'information about other nuclear weapon states is rather scarce and fragmented. But what we do know about Soviet nuclear weapons largely confirms the general pattern seen in the United States—the Soviet Union and now Russia have also had their share of close calls and nerve-wracking experiences.'[18]

United States B-52 bomber aircrafts on the line in 1967, armed with AGM-28 Hound Dog Missiles as air crew enters first aircraft (Photo: United States Air Force).

The limits of safety

Schlosser's research tallies with Sagan's earlier, detailed study on nuclear weapons accidents in the United States arsenal during the cold war. Sagan argued that such findings about what were in many cases system accidents should 'raise serious doubts about the central assumption that a nuclear war could not occur unless political leaders decided it was in their states' interests [...] the belief that nuclear deterrence can prevent nuclear war under all circumstances should be seen as exactly that: a belief, not a fact.'[22]

In his book, *The Limits of Safety*, Sagan found that the United States' nuclear weapons control complex had all of the characteristics of the type of 'normal accident' organization described in Table 1 in this paper. Moreover, his research detailed many incidents of ill-discipline, alcoholism, drug abuse and mental illness among personnel working with nuclear weapons as some of the sources of risk even elite organizations find difficult to screen out, and which could contribute to system accidents. A string of recent incidents and scan-

BOX 3

UNITED STATES NUCLEAR WEAPON ACCIDENTS

Eric Schlosser's book, *Command and Control*, described many accidents involving nuclear weapons during the cold war—a list that in the case of the United States alone ran into the thousands of incidents, although the full scope was not known until information was released later under the Freedom of Information Act. Events included plane crashes, fires, missile explosions, lightning, human error, 'even dropping a weapon from an aircraft parked on a runway were found to be potential causes of a nuclear explosion'.[19] American nuclear weapon designers did not understand some of these sources of risk until at least the 1960s. In one case, a B-52 bomber jettisoned two four-megaton nuclear bombs over Goldsboro, North Carolina in 1961: one of these began the detonation process, which was prevented only by a single low-voltage switch after all other safety systems failed.[20] In September 1980, a technician dropped a tool in the silo of a Titan II intercontinental ballistic missile near Damascus, Arkansas. The tool hit the bottom of the silo, bounced, struck the side of the missile, pierced the skin and caused a fuel leak. The Titan II was carrying the most powerful nuclear warhead ever built by the United States. Despite a heroic effort to save the missile, it exploded, though the warhead did not detonate.

Other nuclear weapon possessor states, including the United Kingdom, have been even more secretive about their safety records, although Ritchie has noted a number of accidents involving British nuclear weapons, some of which have shared American designs.[21] These accidents are not only sources of risk for people on the territories of nuclear weapon states, but also wherever the weapons are deployed.

TABLE 2

INCIDENTS OF NEAR NUCLEAR USE

DATE	INCIDENT	STATES INVOLVED	CAUSE
October 1962	Operation Anadyr	Soviet Union	Miscommunication
27 October 1962	British nuclear forces during the Cuban missile crisis	United Kingdom	Conflict escalation
27 October 1962	Black Saturday	United States	Conflict escalation and miscommunication
22 November 1962	Penkovsky false warning	Soviet Union	Espionage
October 1973	1973 Arab-Israeli war	Israel	Conflict escalation
9 November 1979	NORAD: Exercise tape mistaken for reality	United States	Exercise scenario tape causes nuclear alert
3 June 1980	NORAD: Faulty computer chip	United States	Faulty computer chip
25 September 1983	Serpukhov-15	Soviet Union	Technical error
7-11 November 1983	Able Archer-83	Soviet Union, United States	Misperception of military training exercise
18-21 August 1991	Failed coup	Soviet Union	Loss of command and control structure
25 January 1995	Black Brant scare	Russia	Mistaken identity of research rocket launch
May-June 1999	Kargil crisis	India, Pakistan	Conflict escalation
December 2001-October 2002	Kashmir standoff	India, Pakistan	Conflict escalation

Reproduced from P. Lewis et al, *Too close for comfort*, Chatham House 2014, p.7.

dals involving American military personnel with nuclear weapons responsibilities serves to underline the point that there are not robust internal learning mechanisms in place within the nuclear weapons complex.[23] Nor, from the limited available evidence, are the nuclear arsenals of other states spared from accidents, or these kinds of risk. There is every reason to believe that nuclear weapons complexes are far from high-reliability systems.

Shifting the burden of proof on nuclear deterrence

Sagan concluded that the burden of proof for demonstrating that nuclear weapons control systems are acceptably safe needs to shift: 'those who predict that nuclear weapons can be managed safely indefinitely into the future should have to prove their case and not simply refer back to a perfect safety record that never really existed.'[24]

Two decades later, such a shift in the burden of proof has yet to occur on nuclear weapons. Yet it is important since not enough is currently known or can be verified about the recent safety records of nuclear weapon possessors, especially as most seem reluctant to place this information in the public domain. Such a lack of transparency is not reassuring. Nor does it lend credibility to claims that nuclear deterrence is safe or sustainable without catastrophic failures occurring; that is, the detonation of nuclear weapons in populated areas with the massive harm and suffering it would cause.

Conclusion

To the extent that it has occurred, much of the global policy debate about nuclear weapons since the cold war's end has revolved around the efficacy of nuclear deterrence. It may be that this is the wrong question to prioritize, not least in view of competing bureaucratic agendas and continued lack of transparency in nuclear weapons control. As Podvig has noted, the question 'is not whether

a reliable, safe nuclear arsenal is imaginable, but whether the political and military institutions currently setting nuclear policy are capable of building one. The cold war record is not very encouraging, and neither are developments of the past several years.'[25]

Already, an achievement of the humanitarian initiative is that its emphasis on exploring the risks of nuclear weapon use brings into starker relief the limits of contingent, hypothetical scenarios rationalizing their utility in the international nuclear weapons control discourse. A logical and increasingly pressing question is what to do about the risks the continued existence and fallible management of those weapons pose.

Endnotes

1 See European Commission, Risk Assessment and Mapping Guidelines for Disaster Management, 2010, pp. 15-16. The author is also indebted to Seth Baum for his points in this regard.

2 K.N Waltz, 'Nuclear Myths and Political Realities', American Political Science Review, vol. 84, pp. 731-745.

3 See B. Tertrais, In Defense of Deterrence: The Relevance, Morality and Cost-Effectiveness of Nuclear Weapons, IFRI Security Studies Centre, 2011, p. 26.

4 See A.M. Barrett, S.D. Baum and K. Hostetler, 'Analyzing and reducing the risks of inadvertent nuclear war between the United States and Russia, Science and Global Security, vol. 21 no. 2, 2013, pp. 106-133. See also R.K. Posner, Catastrophe: Risk and Response, Oxford University Press, 2004.

5 M. Hellman, 'Risk Analysis of Nuclear Deterrence', The Bent of Tau Beta Pi, Spring 2008) pp. 14-22, pp. 17-18.

6 N. Bostrom and M.M. Ćirković (eds), Global Catastrophic Risks, Oxford University Press, 2008, pp. 28-29.

7 B.G. Blair, The Logic of Accidental Nuclear War, The Brooking Institution, 1993, p. 8.

8 S.D. Sagan, The Limits of Safety: Organizations, Accidents, and Nuclear Weapons, Princeton University Press, 1993, p. 13.

9 Ibid, p. 16.

10 P. Lewis, H. Williams, B. Pelopidas and S. Aghlani, Too close for comfort: cases of near nuclear use and options for policy, Chatham House, 2014.

11 J.G. March and J.P. Olsen, 'The uncertainty of the past: organizational learning under ambiguity' in March, Decisions and Organizations, p. 349, quoted in Sagan, p. 42.

12 E. Schlosser, Command and Control, Allen Lane, 2013, pp. 331-334.

13 P. Podvig, 'No such thing as a safe nuclear arsenal', Bulletin of the Atomic Scientists, 12 January 2014: http://thebulletin.org/no-such-thing-safe-nuclear-arsenal.

14 Schlosser, pp. 367-368.

15 C. Perrow, Normal Accidents: Living with High-risk Technologies, Basic Books, 1984, p. 90.

16 See Reframing Nuclear De-Alert: Decreasing the Operational Readiness of U.S. and Russian Arsenals, EastWest Institute, 2009, and H.M Kristensen and M. McKinzie, Reducing Alert Rates of Nuclear Weapons, UNIDIR, 2012.

17 United States Department of State, New START Treaty Aggregate Numbers of Strategic Offensive Arms, 1 October 2014: http://www.state.gov/t/avc/rls/232359.htm.

18 Podvig.

19 E. Schlosser, 'Nuclear weapons: An Accident Waiting to Happen' The Guardian, 14 September 2013: http://www.theguardian.com/world/2013/sep/14/nuclear-weapons-accident-waiting-to-happen.

20 BBC, 'US Plane in 1961 nuclear "near miss"', 21 September 2013: www.bbc.com/news/world-us-canada-24183879.

21 N. Ritchie, Nuclear risk: the British Case, Article 36, 2014.

22 Sagan, p. 262.

23 Associated Press, 'When do Nuclear Missteps Put Security in Jeopardy?', 18 January 2014: http://bigstory.ap.org/article/when-do-nuclear-missteps-put-security-jeopardy.

24 Sagan, p. 264.

25 Podvig.

26 N.N. Taleb, The Black Swan: The Impact of the Highly Improbable, Random House, 2007, p. 40. Taleb notes that in Russell's example a (hypothetical) chicken was used.

27 Ibid.

TITLES IN THIS 'VIENNA PAPERS' SERIES

The International Law and Policy Institute (ILPI) and the United Nations Institute for Disarmament Research (UNIDIR) produced this series of papers for the third conference on the humanitarian impacts of nuclear weapons (HINW) in Vienna, Austria, from 8 to 9 December 2014:

1. NICK RITCHIE, The story so far: the humanitarian initiative on the impacts of nuclear weapons.
2. JOHN BORRIE, A harmful legacy: the lingering humanitarian impacts of nuclear weapons testing.
3. JOHN BORRIE, A limit to safety: risk, 'normal accidents', and nuclear weapons.
4. SIMON BAGSHAW, Population displacement: displacement in the aftermath of nuclear weapon detonation events.
5. ANNE GURO DIMMEN, Gendered impacts: the humanitarian impacts of nuclear weapons from a gender perspective.
6. GRO NYSTUEN, Legal aspects of nuclear weapons: a 'birds-eye view' of international law and nuclear weapons.

The papers were edited by John Borrie (jborrie@unog.ch) and Tim Caughley (tcaughley@unog.ch) of UNIDIR, and Torbjørn Graff Hugo (tgh@ilpi.org) of ILPI. Production of this paper series was made possible thanks to the support of the Governments of Norway and Ireland.

Electronic copies of these papers can be downloaded for free from www.unidir.org and www.ilpi.org.

For more information, including commentary and news about international developments related to the humanitarian initiative on nuclear weapons, visit unidir.ilpi.org.