RAND CORPORATION

Perspective

Expert insights on a timely policy issue

False Alarms, True Dangers?

Current and Future Risks of Inadvertent U.S.-Russian Nuclear War

Anthony M. Barrett

In the post–Cold War era, it is tempting to see the threat of nuclear war between the United States and Russia as remote: Both nations' nuclear arsenals have shrunk since their Cold War peaks, and neither nation is actively threatening the other with war. A number of analysts, however, warn of the risk of an inadvertent nuclear conflict between the United States and Russia—that is, a conflict that begins when one nation misinterprets an event (such as a training exercise, a weather phenomenon, or a malfunction) as an indicator of a nuclear attack or a provocation. According to recently declassified documents, the United States and Russia came dangerously close to an inadvertent nuclear conflict in 1983, when Soviet leaders temporarily misinterpreted a NATO exercise—code-named Able Archer—as a cover for a nuclear strike (Jones, Blanton, and Harper, 2015).

While U.S. and Russian nuclear arsenals may be diminished, they are still by far the largest in the world, and both nations remain capable of retaliating with hundreds of nuclear missiles within a matter of minutes of a perceived attack. The use of a single nuclear missile in a populated area would be devastating; the use of substantial fractions of U.S. and Russian nuclear arsenals could trigger a global catastrophe. Understanding how miscalculations and misperceptions can lead to the use of nuclear weapons is an important step toward reducing the probability of an inadvertent nuclear conflict.

At present, the United States does not appear to have a consistently used method for assessing the risk of inadvertent nuclear war. To address this gap, this report synthesizes key points from the literature on the pathways by which, and the conditions under which, misinterpretations could lead to a nuclear strike, either by U.S. or Russian forces. By shedding light on these risks, this report hopes to inform decisionmakers about measures that both nations can take to reduce the probability of an inadvertent nuclear conflict.

Three Pathways to an Inadvertent Nuclear Conflict

This report uses simple fault tree models—top-down, graphical depictions—to examine three primary scenarios in which an inadvertent nuclear conflict is a possible outcome: an early warning system's false alarm; an escalation of a conventional conflict in Russia's "near abroad" (i.e., in a former Soviet Union state, a Russian ally near Russia, or another area near Russia deemed critical to its national security interests); or a false indication of a nuclear attack by Russia's "Dead Hand" system, an automated system that allows for a nuclear launch without oversight or real-time commands from national leadership. An early warning false alarm could lead to a nuclear launch by either U.S. or Russian forces, but the other two scenarios involve a launch by only Russian forces.

An important underlying factor in all three scenarios is the ebb and flow of tension levels between the United States and Russia. It is generally assumed that the risk of nuclear use, accidental or otherwise, is higher during a conventional conflict or during a period of increased tension or crisis: In both of these situations, leaders may be more psychologically or strategically predisposed to launch missiles in response to apparently credible indicators of an attack. The closest we have come to a nuclear disaster was the Cuban Missile Crisis, in which both the United States and Russia (the USSR) raised nuclear alert levels and engaged in a standoff. But another dangerous possibility, especially with regard to an inadvertent conflict, is a one-sided crisis—for example, the 1983 Able Archer incident, in which only one side perceived (or misperceived) the situation as a crisis.

Both the United States and Russia have systems in place to warn of missile attacks.

Early Warning False Alarm Scenario

Both the United States and Russia have systems in place to warn of missile attacks. These systems have traditionally included both satellites (to detect hot plume gases from a missile launch) and radar (to detect missiles flying through space). Because both satellite and radar sensors are susceptible to false positives, these early warning systems look for events that resemble a missile launch on both satellite and radar systems, at the same time. If an indication of an attack seems sufficiently convincing, leaders are contacted and briefed on the situation and then must decide whether to launch their own missiles in response.

Ideally, having to corroborate an event on both satellite and radar systems—known as *dual phenomenology*—allows system operators to screen out false alarms that arise from only satellite or only radar sensors. This process, however, does not prevent false alarms from events arising outside the satellite and radar systems (for example, a 1980 NORAD incident in which a faulty computer chip indicated that missiles were being launched at the United States) or from events that could produce genuine-seeming launch indications on both satellite and radar systems (for example, from the proliferation of various types of ballistic missiles around the world, or from U.S. conventional prompt global strike weapons using repurposed intercontinental ballistic missiles [ICBMs]).

What Might a Future Early Warning False Alarm Look Like?

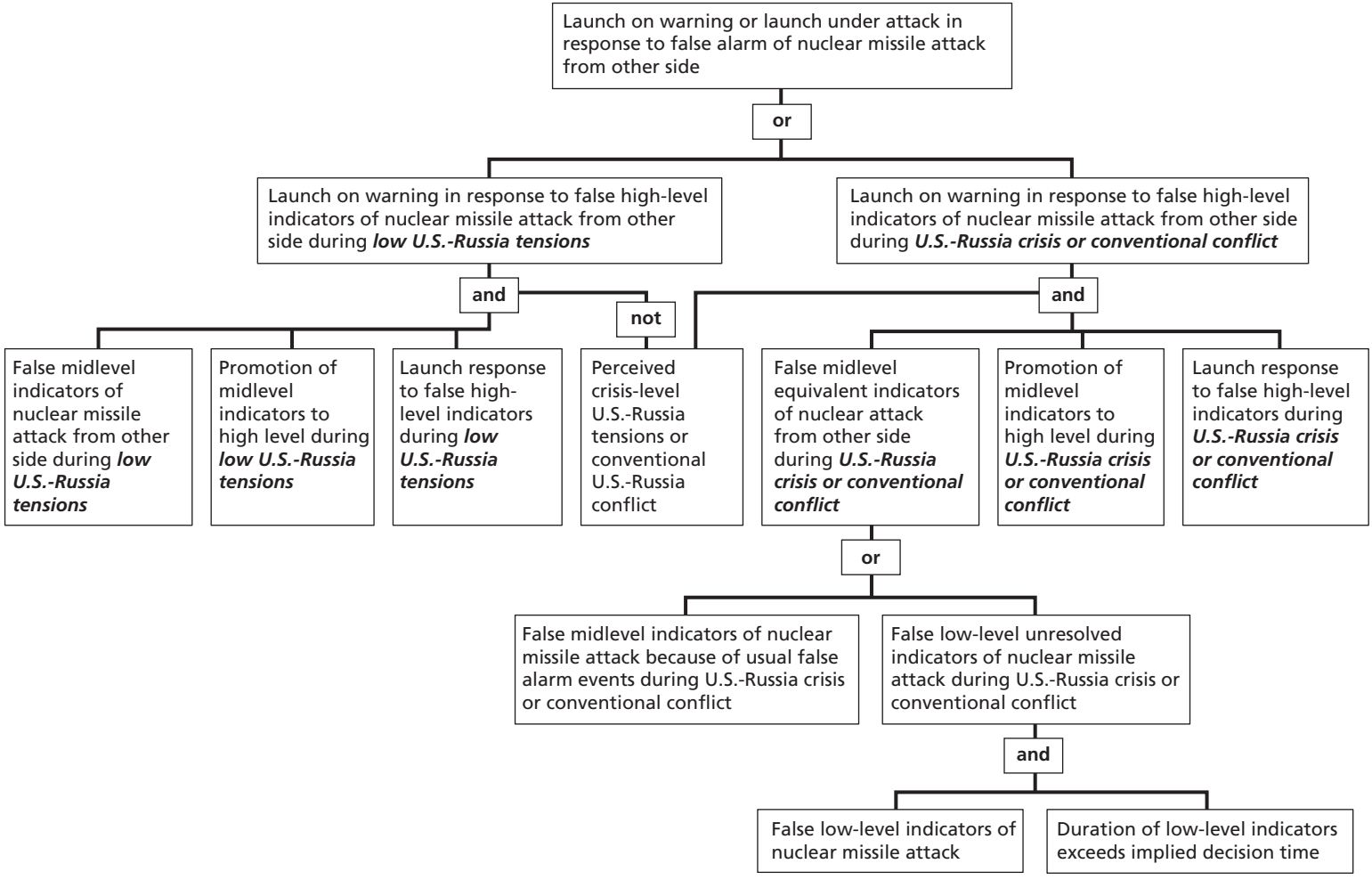
This scenario could take place over the next three years: Falling oil and gas prices make it difficult for Russia to maintain its early warning system components. One of the northern-facing Russian radars begins failing some of its reliability tests, and a month later the Russian early warning satellite constellation loses its only geostationary satellite. A combination of technical problems and budget pressures prevent either a radar overhaul or a launch of a replacement satellite for at least a year. Two months after the geostationary satellite loss, one of several remaining Russian early warning satellites in a highly elliptical Molniya orbit detects flares of some kind in the area of the ICBM fields in the northern United States. At that moment, the satellite is the only component of the Russian early warning satellite constellation that is in an orbital position allowing it to see the northern United States. The satellite cannot immediately determine whether the flares are due to launches at ICBM bases or to something else, such as fires at oil or gas facilities in the same region, or perhaps the reflection of sunlight off high-altitude clouds. The satellite is able to transmit its flare-detection signal to other parts of the Russian early warning system, alerting system operators in Russia. However, the Russian satellite is then struck by orbital debris, and it instantly ceases communication with Russian early warning system operators. Russian early warning system operators must quickly decide what to tell their leaders. Did the satellite detect a launch of U.S. ICBMs? Was the loss of communications capabilities caused by sabotage? Could Russian radar systems rule out the possibility of incoming ICBMs? These questions could be quite serious during a period of seeming calm between the United States and Russia, but they would be especially urgent during a period of heightened tension or crisis.

This Perspective represents the various pathways for a false alarm scenario for both nations in one fault tree (Figure 1), given the assumption that both Russia and the United States have similar procedures to respond to early warning alarms and use roughly analogous categories of low-, mid-, and high-level alarm events. The outcome of concern here, of course, is the launch of nuclear missiles when one country mistakenly concludes that it is under attack by the other.

As shown in the second level of the tree, a launch in response to a false alarm could occur either during a U.S.-Russian crisis or during a period of low tension. The next layer in the tree shows that a launch in response to a false alarm could occur if a midlevel false alarm is promoted to a high level and involves senior national leadership who choose a launch response. Each of those steps in the decision process for false alarms has an associated node in the fault tree that is a key risk factor in the model. That all applies to both crisis and noncrisis periods. However, as is shown farther down the tree, during crisis conditions, the effective total rate of false alarms includes both midlevel false alarm events and any low-level events whose resolution (identification as a false alarm) cannot be completed before the "use them or lose them" point where a launch response decision needs to be made by leaders.[1]

Two key risk factors in the early warning false alarm scenario are whether there is a perceived crisis at any point in time and how likely Russia would be to assume either a launch-on-warning or launch-under-attack posture. Both postures rely on launching missiles in response to a perceived attack once attack indicators are provided and before the perceived attack is expected to affect or disable command and communications capabilities (that is, neither posture relies on "riding out" an attack before launching a counter-

Figure 1. Fault Tree for Launch Response to False Indicators of Missile Attack



RAND *PE191-1*

attack). The primary difference between the two postures is in the level of evidence required to pass the signal detection threshold for an attack indication (at which point "decision time" begins), as well as the amount of time required to obtain that level of evidence. Some Russian analysts have argued that it is better for Russia to be able to launch its weapons on warning of a U.S. attack rather than in a responsive second strike (Quinlivan and Oliker, 2011, p. 25). This would ensure the deterrent value of Russian nuclear forces, despite the possibility that Russian forces would not survive a disarming first strike. Similar arguments led to the original development and potential use of launch-on-warning postures by the United States and the USSR during the Cold War. All else equal, a launch-on-warning posture generally has a higher potential for false indications of attack than a launch-under-attack posture, which requires more early warning information (from a larger number of independent sensor systems).

Historically, a range of events have led to false alarms, and different parts of the early warning system are susceptible to different kinds of false alarms, as illustrated by four well-known instances: the 1979 incident in which a training tape inadvertently played on NORAD early warning system computers, indicating a large Soviet missile strike (an example of system operator error); the 1980 NORAD computer chip incident described above (a communication system component failure); the 1983 incident in which Russian satellites mistook reflected sunlight for an indication of an ICBM launch; and the 1995 Norwegian rocket launch, which apparently resembled a submarine-launched ballistic missile (SLBM) launch on Russian radar.[2]

Potential future attack scenarios that could be mistaken for the ICBM or SLBM attacks that U.S. and Russian early warning systems look for include a terrorist launch of rockets resembling those of either the United States or Russia. These could be the actual nuclear-armed rockets of either nation or a nonnuclear missile, such as the one launched by Norway in 1995, in an attempt to fool the system. Cyberattacks by terrorists or other actors could also target early warning or command and control systems (Fritz, 2009). Previous analysis, however, suggests that the probability of a nuclear terrorist attack triggering an early warning false alarm would be low in comparison to other events (Barrett, Baum, and Hostetler, 2013), though the possibility still ought to be accounted for by U.S. and Russian leaders and early warning system operators. Terrorists and other intelligent adversaries might try to use unexpected means to exploit early warning systems and responses.

Certain U.S. conventional prompt global strike scenarios could be a source of false indicators of attack aimed only at Russia (Podvig, 2006a, pp. 75–77; Podvig, 2006b; Committee on Conventional Prompt Global Strike Capability, 2008). These scenarios include the use of U.S. ICBMs or SLBMs converted to conventional warheads while retaining ballistic trajectories, which critics argue could resemble (to Russian early warning systems) nuclear ICBM and SLBM attacks, especially if the warheads' projected flight paths were to cross over or near Russia. Although Russian satellites and radar might be able to determine that only one missile was being launched, or that the U.S. warhead's ballistic trajectory would not strike a target in Russia, Russian leaders still might have significant concerns. For example, perhaps Russian leaders become concerned that the U.S. "conventional strike" is actually a ruse for a debilitating electromagnetic pulse (EMP) attack on Russia. (Similar Russian EMP-strike concerns were apparently the basis for the surprisingly high-level attention given to the single rocket

launched in the 1995 Norwegian rocket incident.[3]) The United States has also been developing launch or reentry vehicles with non-ballistic trajectories, whose use could be easier for Russian satellites and radar to distinguish from traditional U.S. nuclear ICBMs and SLBMs. However, if these weapons are used in a way that Russia perceives as an attack, they could pose essentially the same false alarm hazards as an ICBM- or SLBM-based conventional prompt global strike.

Inadvertent or Accidental Escalation of a Conventional Conflict Scenario

Any future conventional conflict with a nuclear power, Russia or otherwise, has the potential to escalate into a nuclear conflict (Morgan et al., 2008; Morgan, 2012). *Inadvertent escalation* from conventional operations to use of nuclear weapons could occur if leaders do *not* predict ways in which their ordered conventional operations "come into direct contact with the nuclear forces of an adversary and substantially affect the victim's confidence in his future ability to operate these forces in ways that he had counted upon" (Posen, 1991, p. 2). This could be especially likely when conventional attacks have "degraded the basic nuclear retaliatory capability of the victim—his second strike capability," but other actions could also be viewed as major escalation—for instance, conventional damage to early warning systems of a nation dependent on launch-on-warning postures (Posen, 1991, p. 2). Essentially, one side could inadvertently place the other in a "use them or lose them" position, where the second side may indeed use its nuclear forces for preemptive, damage-limitation purposes. *Accidental escalation* is a situation in which leaders understand escalation thresholds well enough but some part of their forces mistakenly crosses these thresholds (Morgan et al., 2008). A mistake like this could occur because leaders have given subordinate forces inappropriate rules of engagement, or because of poor discipline, or because otherwise well-prepared operators make some kind of error—for example, bombing the wrong targets or straying across geographical boundaries (Morgan et al., 2008, p. xiv).

What Might a Future Inadvertent Escalation Involving U.S. and Russian Forces Look Like?

This scenario could take place in eight years: Multiple nations have increased their exploitation of undersea oil and gas in the Arctic. Russian, Canadian, and Norwegian civilian firms jostle for access to part of a newly identified undersea oil reservoir, which is in an area where new national claims have been recently made but not settled. Russian, Canadian, and Norwegian naval vessels are all in the area. In foggy weather, a Norwegian military vessel strikes a Russian military vessel, causing minor injuries and damage. Russian leaders protest and move more vessels to the area, while Norwegian leaders claim that Russian leaders misinterpreted an unfortunate accident. Several NATO members conducting Arctic gas exploration move additional naval vessels near the area to help protect their own civilian vessels. The next time Norwegian civilian vessels move into the disputed area, accompanied by Norwegian naval vessels, Russian vessels fire warning shots. The Norwegian vessels do not turn back, waiting for directions from superiors, and the Russian vessels move quickly to demonstrations of force involving actual targeting of the Norwegian vessels, killing both civilians and naval officers. Other NATO member vessels respond, firing on the Russian vessels. The next day, two of the NATO members invoke NATO articles, calling on other NATO members to consult

and take action, and most NATO countries take steps to close their embassies in Russia in the face of popular unrest. Russia responds by moving more naval forces into the disputed area, moving land and air forces near NATO-member borders with Russia, and closing its own embassies in Western capitals. The situation simmers for three days. Then, for unrelated reasons, there is a collapse of the government in Ukraine, which had been quite friendly with Russia during that Ukrainian presidential administration. Both NATO members and Russia move small numbers of troops into the country, mainly into specific areas with relatively large numbers of stranded travelers, expatriates, and sympathetic Ukrainians—though each side also suspects the other of sneaky preparations to gain control. (Little of the discussion and coordination between NATO members and Russia that normally would take place to prevent misunderstandings can be arranged, because of the Arctic crisis.) The forces in Ukraine begin to fire on one another, first sporadically as they encounter each other's locations, then in earnest as Russian forces move in an attempt to encircle Kiev. As part of an effort to dislodge Russian forces, NATO air forces target Russian command and control nodes in the region. Russian leaders interpret that as an attempt to deny Russia an option of using theater nuclear weapons, which Russians view as grounds for a nuclear response (something that NATO planners did not expect when they ordered the air attacks on Russian command and control).

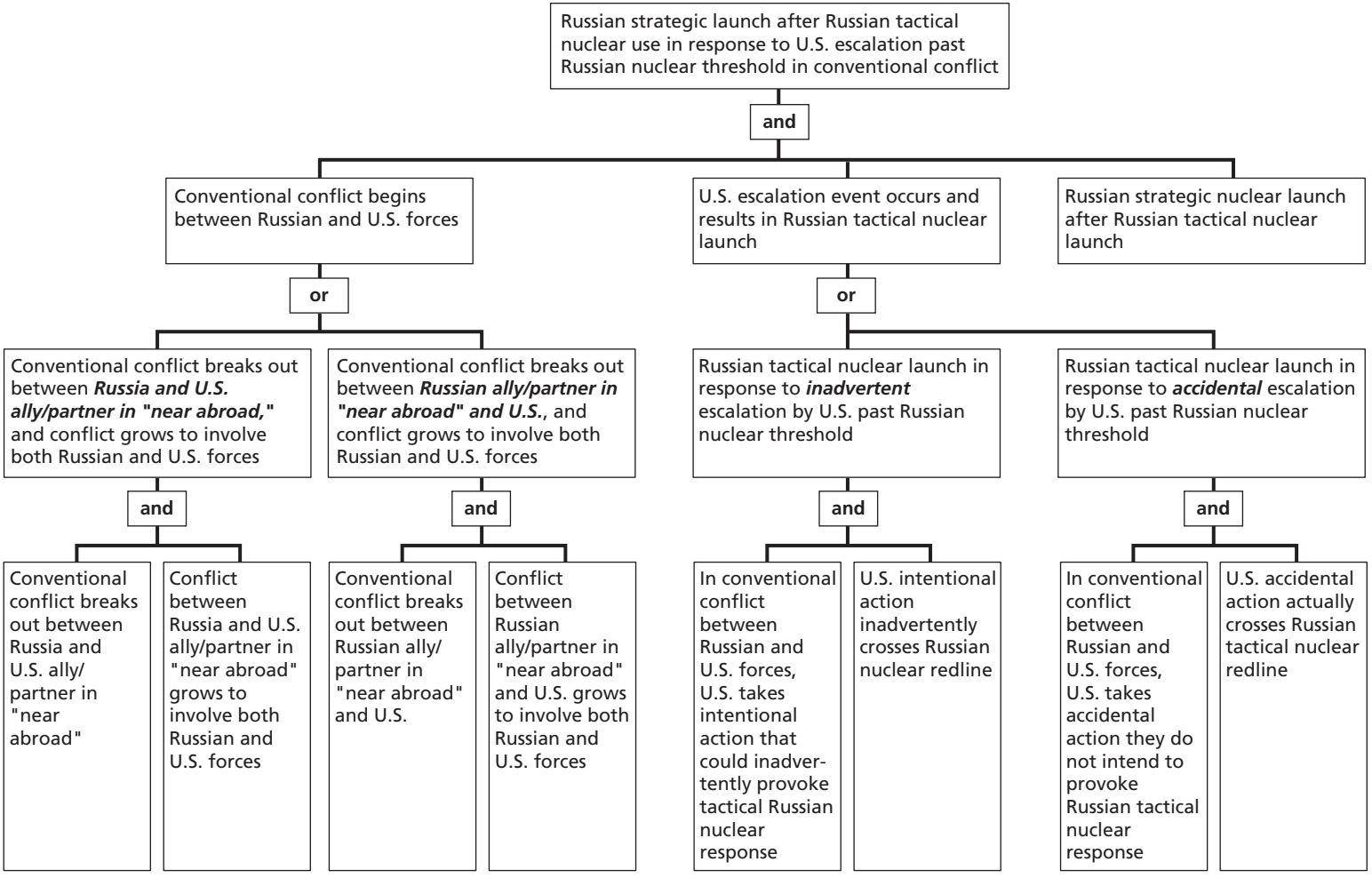
Inadvertent escalation can occur in part because it is often difficult to "divine" what acts an adversary will consider to be a provocation meriting a nuclear response (Morgan et al., 2008, p. xiii). Some analysts argue that in order for the United States to manage the risks of inadvertent escalation, it is necessary to clarify thresholds on all sides of a conflict, use intelligence to determine an enemy's "salient" escalation thresholds, and explicitly state what actions the United States would consider to be seriously escalatory. If escalation thresholds are sufficiently clarified, then both sides face the difficult decision of whether to effect deliberate escalation, or how to design escalation mechanisms, but at least neither would be blundering into escalation situations unknowingly.

Escalation events could result in the use of nonstrategic or small nuclear weapons in a theater of conflict near Russia, rather than in the use of larger, strategic nuclear weapons that could be launched via ICBMs at the United States. However, this Perspective posits that it is possible that Russian nonstrategic nuclear use could lead to the use of strategic nuclear weapons (see Figure 2). During the Cold War, it was often assumed that the use of nonstrategic nuclear weapons would eventually escalate to East-West strategic nuclear exchanges (Quinlivan and Oliker, 2011, p. 72). In the current environment, the use of nonstrategic nuclear weapons by Russia would not necessarily lead to the use of strategic nuclear weapons, because this might be seen as further escalation. However, there seems to be a recognition within Russia of brinkmanship hazards—namely, that Russian nuclear use could get out of hand and result in further escalation (Quinlivan and Oliker, 2011, p. 72).

Analysts have argued that there would be substantial risks of inadvertent escalation in certain conflicts between U.S. or NATO

It is possible that Russian nonstrategic nuclear use could lead to the use of strategic nuclear weapons.

Figure 2. Fault Tree for Russian Strategic Launch After U.S. Escalation Past Russian Nuclear Threshold



RAND *PE191-2*

forces and Russian forces. The risks could be especially great in conflicts involving Russia's near abroad, which could pit Russia's perceived interests and resurgent assertiveness against expanding NATO security commitments to states near Russia's borders (Morgan, 2012, pp. 18, 34–35, 40). Similar potential flashpoints include Ukraine, as well as Estonia and Latvia, the new NATO members and Baltic states (Morgan, 2012, pp. 35, 40). Conflicts could also occur over exploitation of newly accessible energy reserves in the Arctic (Morgan, 2012, p. 35).[4] There is a significant chance that either Russian or Western leaders would engage in escalatory actions while assuming that the other side would back down, fearing the runaway consequences of further escalation (Morgan, 2012, p. 37).

Standard Western doctrines employed against Russian forces in Russia's near abroad or in Russia could result in considerable risks of inadvertent escalation, even if all sides would like to avoid escalation (Morgan, 2012, pp. 37–38). For instance, a hypothetical NATO intervention in a conflict on Russia's border would likely entail an air campaign against Russian military targets. If NATO air commanders followed U.S. Air Force and joint doctrine, they would seek to establish air supremacy by aggressively attacking Russia's air defense system, and they would strike key Russian command and control nodes (Morgan, 2012, pp. 37–38). Russian nuclear doctrine states that nuclear weapons can be deployed in response to the use of conventional weapons that "threaten the very existence of the state" (Morgan, 2012, p. 38). Russia could use some of its inventory of tactical nuclear weapons to dissuade further Western advances or deescalate a conflict, despite NATO's conventional superiority (Morgan, 2012, pp. 38–39). Russian perception of whether NATO's strikes would threaten the Russian state's existence would depend on the intensity, breadth, and nature of the strikes, as well as other factors, such as avoidance of humiliation and preservation of Russia's international prestige (Morgan, 2012, p. 39). As a result of changes in Russian military and nuclear doctrines, there is some uncertainty about the circumstances under which Russia would consider using nuclear weapons, as well as the type of nuclear weapons it would consider using (Quinlivan and Oliker, 2011, p. xii).

According to its military doctrine, Russia could also use nuclear weapons in response to a conventional attack on its allies, if the attack were to pose a threat to the existence of that ally (Quinlivan and Oliker, 2011, pp. xi, 18–19, 69). Similarly, Russia states an explicit interest in protecting Russian citizens, "wherever they may be," and countries with whom it has "shared historical relations" (Quinlivan and Oliker, 2011, p. 71). Escalation to Russian nuclear use might not occur for these reasons, given Russia's understanding of the risks involved, but it would be a possibility (Quinlivan and Oliker, 2011, p. 69).

Dead Hand (Perimeter) Scenario

Cold War concerns about the survivability of Russian leadership and their nuclear command and control systems in the event of a U.S. first strike purportedly led to the development, in the 1980s, of "dead hand"[5] mechanisms and procedures, also known as Perimeter. These allow for a Russian nuclear response to an attack without the need for real-time launch commands from Russian national leadership (Blair, 1995, pp. 51–56; Yarynich, 2003, pp. 156–166; Podvig, 2004, pp. 65–66; Thompson, 2009). The Dead Hand system was intended to enable a retaliatory response in the event that nuclear weapons had decapitated Soviet leadership.

Western analysts have disagreed about how far development and implementation efforts on the Dead Hand system went. Some feel (Blair, 1995, p. 56) that the Dead Hand procedures were developed but only partially deployed, while others argue that the procedures were more extensively deployed. It may seem strange that so little information has been available in the West about whether Russia ever built or implemented such a system. Indeed, the very idea of a secret Dead Hand system calls to mind the absurdly dangerous "doomsday machine" in the 1964 movie *Dr. Strangelove or: How I Learned to Stop Worrying and Love the Bomb*. As Strangelove himself points out, such a system will be useless for deterring Western attack if Western decisionmakers do not know that the system exists. However, the most important audience for the Dead Hand system's existence may have been Russian, not Western: Dead Hand systems were intended to give Russian generals sufficient confidence in Russia's assured-retaliation capability that they would allow Dead Hand operation as an alternative to preemptive attack or launch on warning (Blair, 1995, pp. 50–55; Hoffman, 2009, pp. 151–152; Thompson, 2009).

Though details on the Dead Hand system are few, and accounts differ somewhat, the general outline is as follows: A network of special sensors detects nuclear detonation by measuring light radioactivity, seismic shocks, and atmospheric overpressure. The system would usually be turned off during periods of low tension but would be enabled in a crisis. If the system detected a nuclear detonation (e.g., in the proximity of any of several redundant nuclear command nodes near Moscow), and if its communication links to national leadership went dead, the system would interpret this as evidence of a nuclear attack on Russia. While a human operator in a hardened underground system facility (potentially a Russian defense official who had moved into the bunker at the beginning of the crisis) would make the final decision on whether to launch nuclear weapons at the United States, the operator would have little information to work with beyond the system's indications of nuclear detonation detection or communication-link failure.

What Might a Future Russian Dead Hand Scenario Look Like?

This is a potential Russian Dead Hand scenario: First, presumably, Russian leaders perceive a crisis with the United States. The United States has perhaps reinstated European Phased Adaptive Array (EPAA) Phase 4 interceptor missile defense development, and disagreements over oil and gas negotiations erupt into a standoff between Russia and multiple NATO members. Along with raising nuclear alert levels, Russian leaders secretly institute Dead Hand procedures, giving a designated official in a bunker near Moscow the ability to launch nuclear weapons if the bunker loses communications with headquarters and if nuclear detonations are detected nearby. Although the bunker is connected to headquarters and to nuclear command systems via separate sets of multiple communications channels, these channels suffer unpredictable problems because of the increased usage load, as well as apparent cyberattacks of increasing tempo. Two days after the Russian nuclear alert, apocalyptic terrorists detonate a nuclear weapon near Washington, D.C., followed two minutes later by a nuclear attack in the Moscow region. The nuclear blast in Moscow triggers Dead Hand nuclear detonation sensors nearby and also severs the communications links between the bunker and headquarters (as well as conventional radio and television reception links). However, the blast does not eliminate all of the bunker's nuclear command system

The possibility of a nuclear terrorist attack being interpreted by Dead Hand sensors as a U.S. attack might be especially high if terrorists use nuclear weapons constructed by a nuclear state.

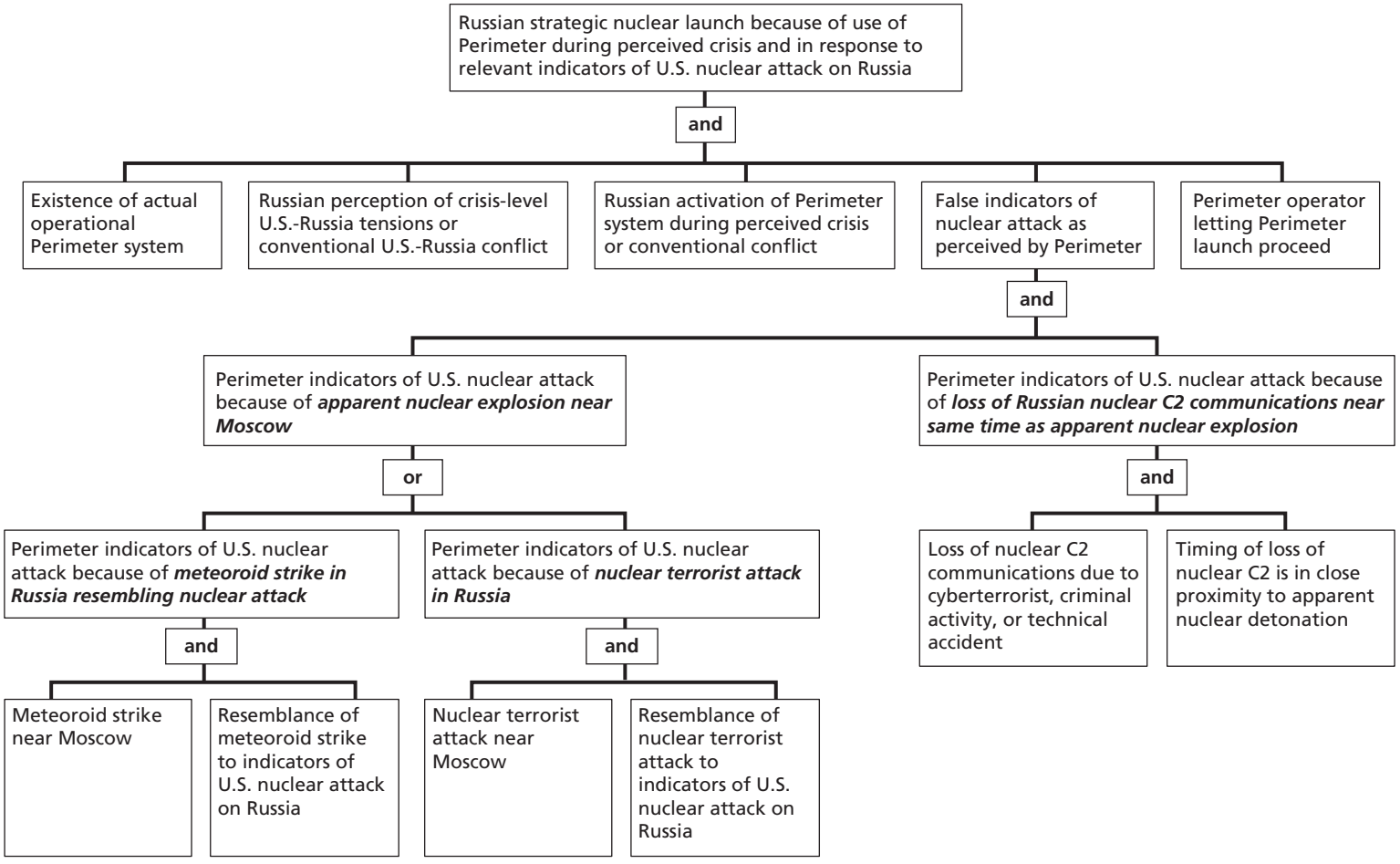
links. The Russian official in the bunker has felt the Moscow blast, sees on the system that it registers as a nuclear explosion, and sees that the communication links to headquarters have gone down (but does not know about the nuclear blast in Washington). The official's system console says that all necessary indications that Russia is under nuclear attack have been satisfied, and the official is able to launch Russian nuclear weapons at the United States in the next hour but must make that decision without any additional information. The possibility of a nuclear terrorist attack being interpreted by Dead Hand sensors as a U.S. attack might be especially high if terrorists use nuclear weapons constructed by a nuclear state. Russian decisionmakers might attribute a nuclear attack to the United States even if there were a lack of accompanying ICBM or SLBM attack indications.

Other events that could trigger Dead Hand sensors include meteorite strikes in Russia, whose explosion effects, such as light and pressure waves, could resemble a nuclear event and cyber-attacks or network failures that result in a of loss of communications capabilities (see Figure 3).

Meteorite impacts with some resemblance to a nuclear explosion have occurred in the past. An October 1990 asteroid explosion above the central Pacific Ocean, with energy greater than one kiloton, was originally detected as a potential nuclear event by U.S. satellites; not until several months later did the Department of Defense determine the true nature of the event (Tagliaferri et al., 1994, pp. 200–201). On average, approximately eight asteroid detonations with at least one kiloton of equivalent energy occur each year, and approximately one asteroid detonation with at least 20 kilotons of equivalent energy occurs each year (Tagliaferri et al., 1994, p. 201). Although one kiloton is a very low yield as nuclear weapons go, super-EMP weapons are actually designed to have low yields, comparable to those observed in recent North Korean nuclear tests, which might have been tests of super-EMP weapons (Pry, 2012).

While the Dead Hand system is a closed network, separate from the Internet, it still has multiple points of vulnerability. For instance, email spoofing could lead to the installation of a virus on an open network; someone with access to a closed network could then unknowingly transfer the virus by way of a removable computer drive between the two networks. According to a U.S. deputy secretary of defense, in 2008, a foreign intelligence agency compromised U.S. classified military systems by inserting into a U.S. military laptop a removable flash drive infected with a virus (Lynn, 2010, p. 97). More recently, removable computer drives reportedly enabled the transfer of a virus between unclassified and classified systems, infecting the "cockpits" of U.S. Air Force unmanned aerial vehicles (Schactman, 2011a; Schactman, 2011b; Schactman, 2011c).

Figure 3. Fault Tree for Russian Launch Because of Dead Hand



NOTE: C2 = command and control.

RAND *PE191-3*

Since mid-2014, events involving Russia, Ukraine, NATO, and the United States suggest a potential increase in the likelihood of a conventional conflict between Russia and U.S. allies or partners near Russia.

Another possibility is attack from a third-party nation, such as China. Third-party attacks could be particularly dangerous because they could be likely to involve near-simultaneous explosive attacks and attacks on communications systems, which are exactly what the Dead Hand system would regard as evidence of a U.S. nuclear strike. One would hope that both Russian leadership and Dead Hand operators would be aware of the potential of an attack from countries besides the United States (including surprise attacks) and would not necessarily launch nuclear weapons at the United States in such a case.

How Risk Levels Could Rise in the Future

Since mid-2014, events involving Russia, Ukraine, NATO, and the United States suggest a potential increase in the likelihood of a conventional conflict between Russia and U.S. allies or partners near Russia. This eventuality would increase the annual probability of a nuclear conflict, inadvertent or otherwise. In terms of the risks of a launch in response to an early warning system false alarm, readers might legitimately expect that improvements in technology and procedures have reduced false alarm rates from what they were decades ago. Yet Russia's early warning system has significantly degraded since the Cold War and is currently at a historical low point in terms of coverage, thus decreasing the probability that Russian leaders will be continually reassured that no U.S. strike is occurring.

Until fairly recently, Russia has operated three or more early warning satellites in highly elliptical earth orbit (HEO) and one satellite in geostationary earth orbit (GEO), all placed so that at least one HEO or GEO satellite is continuously monitoring U.S. ICBMs for indications of launch (Podvig, 2002, p. 49; Podvig, 2013).[6] However, as of November 2015, Russia only has one operational HEO and no GEO early warning satellites. While Russia has been implementing plans for next-generation early warning satellites, which could provide additional coverage of oceans, and thus SLBM launches (Podvig, 2004, p. 577), there have been delays (Podvig, 2014a).[7] If Russian early warning systems do not improve, or if they degrade again, future false alarm rates could increase relative to historical averages. And, in turn, if Russian early warning false alarm rates increase, the annual probability of a Russian early warning false alarm launch response—or Dead Hand false alarm launch response—is also likely to increase.

Changes in crisis perception rates would result in corresponding changes in risk. If crisis occurrence rates rise, so would the annual probability of false alarm scenarios. However, even a low crisis perception rate would be of limited benefit if Russia were to launch in response to a false alarm in a low-tension period or keep the Dead Hand system turned on in a low-tension period: Both of these conditions would result in a nonzero probability of a false alarm launch response, even if the crisis perception rate drops to zero.

Early warning system degradation might just increase the likelihood of misperception.

Russian Crisis Perception Could Be Linked to Perception of U.S. First-Strike Capability

Current literature suggests a number of near-term issues that Russian leaders may see as more threatening than U.S. leaders realize—namely, the possibility that the United States could carry out a disabling first strike against Russian nuclear forces. Concerns about U.S. first-strike capability—and intent—increased in Russia after the 2006 publication of two articles by the U.S. analysts Keir Lieber and Daryl Press (2006a, 2006b), which argued that between its missile defenses and its nuclear and conventional capabilities, the United States could effectively launch a debilitating first strike against Russia's arsenal (Quinlivan and Oliker, 2011, p. 22).

In addition, Russian concerns about force survivability increase the probability that when presented with a serious-looking early warning system false alarm, Russian leaders would use a launch-on-warning response instead of riding out the apparently incoming attack. Presumably, there would be a higher probability that Russian leaders would use a launch-on-warning response to a false indication of an incoming attack during a crisis period (when Russia already has heightened expectation of incoming attack) than during a low-tension, noncrisis period. Some Russian analysts argue that a launch-on-warning posture would be the best way to ensure the deterrent value of Russian nuclear forces. Unfortunately, awareness of early warning system degradation does not necessarily mean that Russian leaders will move away from a launch-on-warning posture entirely, especially if they are increasingly concerned about the survivability of the Russian nuclear deterrent. Instead, early warning system degradation might just increase the likelihood of misperception, so that "launch on erroneous warning" becomes more likely (Quinlivan and Oliker, 2011, pp. 26–27).

Potential Risk-Reduction Measures

Some of the steps the United States could take to reduce the potential risks of an inadvertent nuclear conflict would have very significant trade-offs. For example, measures to reduce Russian concerns about U.S. first-strike capability could conflict with a requirement to maintain a level of U.S. counterforce capabilities, as specified by the 2013 U.S. Nuclear Employment Strategy (Secretary of Defense, 2013). In the following discussion of potential risk-reduction measures, I use the phrase *the United States should consider* in a literal way, without prejudice to conclusions.

Compensate for Potential Problems in Russian Early Warning Systems

To help reassure Russian leaders that no U.S. attack is occurring—and thus reduce the probability of Russian nuclear use in an early warning false alarm or Dead Hand scenario—the United States should consider steps to compensate for the current limitations in the coverage and reliability of Russian early warning systems. This could include keeping U.S. SSBNs (ballistic missile submarines) in areas covered by Russian early warning satellites (once coverage of a new Russian satellite network is extensive enough), reopening talks on a joint early warning center, or offering to let Russia put launch sensors on or near U.S. ICBM silos.

The United States should also acknowledge and encourage actions by Russia to make its own investments to improve early warning systems (to increase the probability that Russian leaders would be able to tell the difference between an early warning system false alarm and an actual incoming attack) and to improve the survivability of Russian forces and command and control systems (to reduce the perceived threat of a U.S. first strike). Probably the most important first step in this regard would be for Russia to launch a replacement for the geostationary-orbit early warning satellite it lost in early 2014, which had been its only operating geostationary satellite (Podvig, 2014a; Global Security Newswire, 2014). A replacement GEO would help Russia to regain simultaneous coverage from multiple viewing angles, which would help reduce false alarm rates from satellite sensors. It also could be valuable for Russia to keep more than one geostationary satellite in its early warning satellite constellation to avoid further loss of coverage in the event that another Russian satellite suddenly becomes inoperative.

The United States should also consider making observable but reasonable adjustments to its own forces to reduce its threat to Russian second-strike capability. Reducing the probability of Russian crisis perception could reduce the probability of a Russian launch-on-warning posture. Such adjustments could be made either unilaterally or as part of negotiated cuts. Adjustments might include using less accurate SLBM warheads, or even partial, verifiable de-alerting of some ICBMs.

EMP Capabilities Could Be Perceived as Contributing to U.S. First-Strike Capability

There could be significant risks from the use or even just the development of capabilities of any nonkinetic offensive technologies aimed at disrupting command, control, communications, and intelligence (C3I) systems, via means such as cyberattacks or EMP attacks (Lin, 2013). The use of these capabilities during a crisis could be interpreted by Dead Hand operators as evidence of a larger nuclear attack on Russia (either because the Russian operators believe that the C3I outage was caused by a large nuclear strike or because they believe that a nuclear attack would be preceded by a debilitating EMP attack to prevent coordinated counterattack). More perversely, just knowledge of the existence of EMP or cyberweapons could increase the probability that Russian Dead Hand operators would interpret a C3I disruption as being caused by or accompanying a U.S. nuclear strike. Accordingly, the United States should consider avoiding further development of EMP weapons that could seem aimed at Russian command and control disruption. This could help avoid increasing the probabilities of Russian crisis perception and of a Russian launch-on-warning posture.

The United States should also consider making observable but reasonable adjustments to its own forces to reduce its threat to Russian second-strike capability.

The United States should do what it can to reduce the probability that Russia will activate the Dead Hand system.

Russia Should Keep Dead Hand Risks from Rising

Recent discussions among Russian analysts suggest that further development of the Dead Hand system could in fact be beneficial, insofar as it could help Russia address its current concerns about nuclear force survivability (Quinlivan and Oliker, 2011, p. 33). From a Western perspective, at least one school of thought holds that Dead Hand procedures could be less dangerous than a Russian launch-on-warning posture (Blair, 1995, pp. 54–55). If the Dead Hand system were activated, and if Russian leaders were confident in its reliability, this could reduce the probability of Russian false alarm launch-on-warning scenarios in a crisis. Russian leaders might not feel the same level of use-them-or-lose-them pressures that contribute to the risk of a Russian launch-on-warning response to an early warning false alarm.

Moreover, a Dead Hand system that produced fewer false indications of attack would help avoid some of the hazards of early warning false alarm scenarios. For this level of reliability, Dead Hand nuclear-detonation sensors need to be able to distinguish between an attack from the United States and an attack from another nation (such as China), a terrorist strike, or a meteorite strike. Given the possibilities of tampering or simple command and control system failure, a reliable Dead Hand system would also need to be essentially immune to tampering or spoofing efforts. For example, the design of the system would need to prevent terrorists or other malefactors from activating it without Russian leadership.

For its part, the United States should do what it can to reduce the probability that Russia will activate the Dead Hand system (i.e., reduce rates of one-sided crises by reducing the appearance of preparation for a disabling first strike).

Use Risk Models to Help Manage Risks

Last, the United States should consider using fault tree models as part of a consistent, systematic approach to nuclear war risk analysis and avoidance. However, reduction of specific nuclear risks is not necessarily without trade-offs. For instance, some nuclear war risk-reduction steps could have significant financial costs. There is also the possibility that nuclear war risk-reduction steps might increase risks of other kinds of conflicts. If Russia or other nations perceive that the United States is more concerned about nuclear risks than in the past, this could increase incentives for attempts at nuclear coercion: Nuclear nations might seek to use risks for coercive leverage against the United States and its allies, and nonnuclear nations might become more inclined to seek nuclear weapons to gain such leverage. Additionally, while there is an argument to be made for keeping U.S. SSBNs in areas covered by Russian early warning satellites, presumably U.S. leaders would not want to allow U.S. SSBNs to be located so precisely as to make it much easier for Russia to attack them. Finally, modifications to U.S. SSBN patrol areas might conflict with force concepts of operations in such a way as to be unacceptable to U.S. decisionmakers. Analysis of these issues is beyond the scope of this report, but decisionmakers should consider such trade-offs before implementing measures intended to reduce nuclear risks.

Notes

[1] Although some aspects have likely changed over time, the broad outlines appear not to have changed much (Marsh, 1985; Wallace, Crissey, and Sennott, 1986; Sennott, 1988; Mosher et al., 2003; Podvig, 2004, pp. 567, 577–578; Podvig, 2006a; Blair, 2010).

[2] Details of these and other incidents are given by Blair, 1993, 1995; Sagan, 1993, Richelson, 1999, pp. 97–98, 246; Pry, 1999; Forden, Podvig, and Postol, 2000; Forden, 2001; and Mosher et al., 2003.

[3] The 1995 Norwegian rocket's trajectory reportedly appeared on Russian early warning systems resembling an SLBM launch that could have caused a high-altitude EMP to disable Russian early warning systems—an immediate precursor to a much larger nuclear attack on Russia (Forden, Podvig, and Postol, 2000; Mosher et al., 2003 p. 17). However, available historical information does not clearly indicate that top Russian leaders actually thought that the rocket was an SLBM for any specific period. Moreover, the National Research Council's Committee on Conventional Prompt Global Strike Capability (2008) study concluded that Russian misinterpretation of such launches would be quite unlikely.

[4] For discussion and maps of Arctic claims, including Russian claims regarding the underwater Lomonosov Ridge near the North Pole, see O'Rourke, 2013, pp. 15–16, and IBRU, 2013. O'Rourke, 2013, pp. 54–58, also discusses varying views of Arctic interests and security issues by NATO member states and Russia.

[5] Thompson explained, "The technical name was Perimeter, but some called it Mertvaya Ruka, Dead Hand" (Thompson, 2009).

[6] At the height of Soviet/Russian satellite coverage, from 1987 until 1996, there were eight or nine HEO satellites and one GEO satellite (Podvig, 2002, p. 49).

[7] The situation was even worse from 2014 to November 2015, when there were no operational Russian early warning satellites at all (Podvig, 2014a). Reportedly, Russia has begun launching its next-generation early warning satellite constellation, code-named Tundra, which, despite Tundra's planned highly elliptical orbit, "will have true look-down capability and will detect missiles launches originated from the sea as well as from the U.S. territory" (Podvig, 2014b). A successful launch occurred in November 2015 of the first new Tundra satellite, with more to follow (Podvig, 2015b), though Russian early warning satellite launches have often been delayed far past announced plans (Podvig, 2015a).

References

Barrett, A. M., Seth D. Baum, and K. R. 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.

Blair, Bruce G., *The Logic of Accidental Nuclear War*, Washington, D.C.: Brookings Institution, 1993.

———, *Global Zero Alert for Nuclear Forces*, Washington, D.C.: Brookings Institution, 1995.

———, "Could Terrorists Launch America's Nuclear Missiles?" *Time*, November 11, 2010. As of April 15, 2016:
http://www.time.com/time/nation/article/0,8599,2030685,00.html

Committee on Conventional Prompt Global Strike Capability, *U.S. Conventional Prompt Global Strike: Issues for 2008 and Beyond*, Washington, D.C.:, U.S. National Research Council, 2008.

Forden, Geoffrey, *Reducing a Common Danger: Improving Russia's Early-Warning System*, Washington, D.C.: Cato Institute, 2001. As of April 15, 2016:
http://www.cato.org/pubs/pas/pa399.pdf

Forden, Geoffrey, Pavel Podvig, and Theodore A. Postol, "False Alarm, Nuclear Danger," *IEEE Spectrum*, Vol. 37, No. 3, 2000.

Fritz, Jason, *Hacking Nuclear Command and Control*, Canberra, Australia: International Commission on Nuclear Non-proliferation and Disarmament, 2009. As of March 28, 2012:
http://icnnd.org/Documents/Jason_Fritz_Hacking_NC2.pdf

Global Security Newswire, "Russia Loses Another One of Its Early-Warning Satellites," Nuclear Threat Initiative, June 26, 2014. As of June 27, 2014:
http://www.nti.org/gsn/article/
russia-loses-its-last-early-warning-satellite-raising-risk-strategic-miscalculation/

Hoffman, David E., *The Dead Hand: The Untold Story of the Cold War Arms Race and Its Dangerous Legacy*, New York: Random House, 2009.

IBRU, "Maritime Jurisdiction and Boundaries in the Arctic Region," Durham, UK: Durham University, 2013. As of April 15, 2016:
https://www.dur.ac.uk/ibru/resources/arctic/

Jones, Nate, Tom Blanton, and Lauren Harper, eds., *The 1983 War Scare Declassified and for Real*, Washington, D.C.: National Security Archive, 2015. As of November 24, 2015:
http://nsarchive.gwu.edu/nukevault/
ebb533-The-Able-Archer-War-Scare-Declassified-PFIAB-Report-Released/

Lieber, Keir A., and Daryl G. Press, "The End of MAD: The Nuclear Dimension of U.S. Primacy," *International Security*, Vol. 30, No. 4, 2006a, pp. 7–44.

———, "The Rise of U.S. Nuclear Primacy," *Foreign Affairs,* Vol. 85, No. 2, 2006b.

Lin, Patrick, "Pain Rays and Robot Swarms: The Radical New War Games the DOD Plays," *Atlantic*, April 15, 2013. As of May 27, 2013:
http://www.theatlantic.com/technology/archive/2013/04/
pain-rays-and-robot-swarms-the-radical-new-war-games-the-dod-plays/274965/

Lynn, William J., III, "Defending a New Domain: The Pentagon's Cyberstrategy," *Foreign Affairs*, Vol. 89, No. 5, 2010.

Marsh, Barbara, *The Probability of Accidental Nuclear War: A Graphical Model of the Ballistic Early Warning System*, Monterey, Calif.: Naval Postgraduate School, 1985.

Morgan, Forrest E., "Dancing with the Bear: Managing Escalation in a Conflict with Russia," *Proliferation Papers*, Vol. 40, Winter 2012.

Morgan, Forrest E., Karl P. Mueller, Evan S. Medeiros, Kevin L. Pollpeter, and Roger Cliff, *Dangerous Thresholds: Managing Escalation in the 21st Century*, Santa Monica, Calif.: RAND, MG-614-AF, 2008. As of April 15, 2016:
http://www.rand.org/pubs/monographs/MG614.html

Mosher, David E., Lowell H. Schwartz, David R. Howell, and Lynn E. Davis, *Beyond the Nuclear Shadow: A Phased Approach for Improving Nuclear Safety and U.S-Russian Relations*, Santa Monica, Calif.: RAND Corporation, MR-1666-NSRD, 2003. As of April 15, 2016:
http://www.rand.org/pubs/monograph_reports/MR1666.html

O'Rourke, Ronald, *Changes in the Arctic: Background and Issues for Congress*, Washington, D.C.: Congressional Research Service, 2013. As of April 15, 2016:
http://www.fas.org/sgp/crs/misc/R41153.pdf

Podvig, Pavel, "History and the Current Status of the Russian Early-Warning System," *Science & Global Security*, Vol. 10, 2002, pp. 21–60.

———, ed., *Russian Strategic Nuclear Forces*, Cambridge, Mass.: MIT Press, 2004.

———, "Reducing the Risk of an Accidental Launch," *Science & Global Security*, Vol. 14, 2006a, pp. 75–115.

———, *Russia and the Prompt Global Strike Plan*, PONARS Policy Memo No. 417, 2006b. As of April 15, 2016: http://csis.org/files/media/csis/pubs/pm_0417.pdf

———, "Early Warning," *Russian Strategic Nuclear Forces*, January 13, 2013. As of June 14, 2013: http://russianforces.org/sprn/

———, "Russia Loses Its Only Geostationary Early-Warning Satellite," *Russian Strategic Nuclear Forces*, June 25, 2014a. As of June 27, 2014: http://russianforces.org/blog/2014/06/russia_loses_its_only_geostati.shtml

———, "New-Generation Early-Warning Satellite, Tundra, to Be Launched in 2014," *Russian Strategic Nuclear Forces*, July 19, 2014b. As of September 8, 2014: http://russianforces.org/blog/2014/07/new-generation_early-warning_s.shtml

———, "New Date Set for New Early-Warning Satellite Launch," *Russian Strategic Nuclear Forces*, June 30, 2015a. As of July 1, 2015: http://russianforces.org/blog/2015/06/new_date_set_for_new_early-war.shtml

———, "First Launch of the Tundra Early-Warning Satellite," *Russian Strategic Nuclear Forces*, November 17, 2015b. As of November 25, 2015: http://russianforces.org/blog/2015/11/first_launch_of_the_tundra_ear.shtml

Posen, Barry R., *Inadvertent Escalation: Conventional War and Nuclear Risks*, Ithaca, N.Y.: Cornell University Press, 1991.

Pry, Peter Vincent, *War Scare: Russia and America on the Nuclear Brink*, Westport, Conn.: Praeger, 1999.

———, "PRY: North Korea EMP Attack Could Destroy U.S.—Now," *Washington Times*, December 9, 2012. As of July 22, 2013: http://www.washingtontimes.com/news/2012/dec/19/north-korea-emp-attack-could-destroy-us-now/?page=all

Quinlivan, James T., and Olga Oliker, *Nuclear Deterrence in Europe: Russian Approaches to a New Environment and Implications for the United States*, Santa Monica, Calif.: RAND Corporation, MG-1075-AF, 2011. As of April 15, 2016: http://www.rand.org/pubs/monographs/MG1075.html

Richelson, Jeffrey T., *America's Space Sentinels: DSP Satellites and National Security*, Lawrence: University Press of Kansas, 1999.

Sagan, Scott D., *The Limits of Safety: Organizations, Accidents, and Nuclear Weapons*, Princeton, N.J.: Princeton University Press, 1993.

Schactman, Noah, "Exclusive: Computer Virus Hits U.S. Drone Fleet," *Wired*, October 7, 2011a. As of July 1, 2013: http://www.wired.com/dangerroom/2011/10/virus-hits-drone-fleet/

———, "Get Hacked, Don't Tell: Drone Base Didn't Report Virus," *Wired*, October 11, 2011b. As of July 1, 2013: http://www.wired.com/dangerroom/2011/10/drone-virus-kept-quiet/

———, "Air Force Insists: Drone Cockpit Virus Just a 'Nuisance,'" *Wired*, October 12, 2011c. As of July 1, 2013: http://www.wired.com/dangerroom/2011/10/drone-virus-nuisance/

Secretary of Defense, *Report on Nuclear Employment Strategy of the United States Specified in Section 491 of 10 U.S.C.*, Washington, D.C.: U.S. Department of Defense, June 12, 2013. As of May 6, 2016: http://www.globalsecurity.org/wmd/library/policy/dod/us-nuclear-employment-strategy.pdf

Sennott, Linn I., "Overlapping False Alarms: Reason for Concern?" in Anatolii Andreevich Gromyko and Martin E. Hellman, eds., *Breakthrough: Emerging New Thinking*, New York: Walker and Company, 1988, pp. 39–44.

Tagliaferri, Edward, Richard Spalding, Cliff Jacobs, Simon P. Worden, and Adam Erlich, "Detection of Meteoroid Impacts by Optical Sensors in Earth Orbit," in Tom Gehrels, ed., *Hazards Due to Comets and Asteroids*, Tucson: University of Arizona Press, 1994.

Thompson, Nicholas, "Inside the Apocalyptic Soviet Doomsday Machine," *Wired*, September 21, 2009. As of June 28, 2013: http://www.wired.com/politics/security/magazine/17-10/mf_deadhand?currentPage=all

Wallace, Michael D., Brian L. Crissey, and Linn I. Sennott, "Accidental Nuclear War: A Risk Assessment," *Journal of Peace Research*, Vol. 23, No. 1, 1986, pp. 9–27.

Yarynich, Valery E., *C3: Nuclear Command, Control, Cooperation*, Washington, D.C.: Center for Defense Information, 2003.

About This Perspective

A risk analyst examines ways in which nuclear war between the United States and Russia could be caused inadvertently, potential future changes that could increase risks, and options for reducing risks.

The research reported here was conducted as part of the Stanton Nuclear Security Fellows Program at the RAND Corporation. The Stanton Nuclear Security Fellows Program was created to stimulate the development of the next generation of leaders on nuclear security by supporting interdisciplinary research that will advance policy-relevant understanding of the issues. Each fellow carries out a yearlong period of independent research, collectively producing studies that contribute to the general body of knowledge on nuclear security.

The Stanton Foundation, a creation of Frank Stanton, former president of CBS and a pioneering executive who led the television network for 25 years, supports Stanton fellows. In 1954, President Dwight D. Eisenhower appointed Stanton to a committee convened to develop the first comprehensive plan for the survival of the United States following a nuclear attack. Stanton led the effort to develop plans for national and international communication in the aftermath of a nuclear incident. Stanton also served as chair (1961–1967) and member (1957–1978) of the RAND Corporation Board of Trustees. The Stanton Foundation aims, through its support of the Stanton Nuclear Security Fellows Program, to perpetuate his efforts to meet these challenges. For more information about the Stanton Fellowship at RAND, visit www.rand.org/stanton.

The author appreciates the generous support of the Stanton Foundation and RAND, as well as the assistance and comments received from the Stanton fellowship mentors, Stanton fellows, and colleagues at RAND and elsewhere. These include Dan Gonzales, Sarah Harting, Paula Thornhill, Lynn Davis, Jim Bonomo, Paul Davis, Olga Oliker, Don Snyder, Pavel Podvig, Jeff Kaplow, Jaganath Sankaran, Graham Allison, Barry Posen, Al Carnesale, Andy Hoehn, Todd Sechser, Evan Saltzmann, Carter Price, David Frelinger, David Mosher, Lowell Schwartz, Jim Quinlivan, Forrest Morgan, Dave Shlapak, Ted Warner, Seth Jones, Jim Scouras, Martin Hellman, Carl Lundgren, Carl Shulman, Kelly Hostetler, Seth Baum, Libby May, Rebecca Fowler, and Kimbria McCarty, among others. Any remaining errors or omissions are the sole responsibility of the author.

This report includes or adapts some material that was previously published in A. M. Barrett, Seth D. Baum, and K. R. 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. However, this report represents a substantial extension of the earlier material. Reused material is included by permission of Taylor & Francis.

Comments are welcome and may be addressed to the author, at tony@gcrinstitute.org.

About the Author

Anthony M. Barrett is cofounder and director of research of the Global Catastrophic Risk Institute and senior risk analyst at ABS Consulting. His work aims to inform risk management policy decisions regarding catastrophe risks in a variety of areas, including terrorism, emerging technologies, and nuclear warfare. He was a Stanton fellow at RAND in 2012–2013.

For more information on this publication, visit www.rand.org/t/PE191.

www.rand.org