WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

White Paper

The Future of Nuclear Security

March 2016

REF 010316

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

World Economic Forum White Paper
The Future of Nuclear Security

March 2016

Contents

Background and Overview

“One thing a person cannot do, no matter how rigorous his analysis or heroic his imagination, is to draw up a list of things that would never occur to him.”
– *Thomas Schelling, Nobel Laureate*

The Nuclear Futures exercise uses scenario-planning methodologies to challenge the assumption prevailing during much of the last quarter century that the threat posed by nuclear weapons is in terminal decline. By creating and assessing plausible and provocative scenarios (that are in some cases likely), a working group from the World Economic Forum's Global Agenda Council on Nuclear Security hope to raise awareness of the *breadth, urgency, complexity and potential deleterious consequences of the multidimensional nuclear security challenges facing political and military leaders throughout the world*.

To advance the council's work, the working group (this White Paper's authors and council members Graham Allison, Leon Fuerth and Tate Nurkin) called upon experts for input. A workshop was hosted in Washington DC with cybersecurity experts to help the council articulate the role that emerging technology and cybersecurity threats play in shaping the future nuclear security environment. Engagement with multiple and multidisciplinary experts ensures that the analysis incorporates a sufficiently diverse range of perspectives on this critical, often emotionally tinged and urgent issue.

About the Scenarios

Each of the exercise's three phases was designed to isolate a particularly powerful driver of nuclear risk (outlined in the Figure). Each phase also includes a different approach to scenario writing and analysis: specific scenario pathways are articulated in the Geopolitics Gone Awry section, while more general summaries are used in the other two sections. *None of the scenarios developed in this exercise was designed to be predictive.* The council does not suggest that these futures are inevitable. However, they are based on real-world processes that are either ongoing, expected in the near future or, even if less likely, plausible. They are designed to question current assumptions about nuclear security and to highlight policy or actions of important actors that could increase the risk of a nuclear crisis. These scenarios are best viewed as objective and innovative devices to get beyond current analytical filters, challenge existing assumptions and expand thinking about current and future challenges.

Figure: Three Phases of Nuclear Risk Drivers

Phase One: Geopolitics Gone Awry	Phase Two: Technology Gone Awry	Phase Three: Nuclear Security and Non-State Actors
• Development and consideration of scenarios to better identify and assess how geopolitical competition can drive unintentional escalation, miscalculation and, ultimately, crises with a nuclear dimension. These scenarios will also explore how geopolitical drivers can challenge the non-proliferation regime.	• Development and consideration of scenarios to better identify and assess how the introduction, evolution and application of commercial and dual-use technologies can pose threats to nuclear security. These scenarios also explore how the development and proliferation of advanced military capabilities can generate escalation, incentives for preemption and, ultimately, nuclear crisis.	• Development and consideration of two categories of non-state armed groups acquiring nuclear weapons or radiological material. This category of analysis includes examination of non-state armed group motivation and capacity to acquire these weapons.

Executive Summary

This White Paper has identified five key themes, scenario elements and insights that are relevant across multiple scenario groups:

1. **Intersecting (not independent) drivers**: Geopolitics, technology, non-state actors and new mindsets about nuclear risk and use should be viewed as intersecting, rather than independent, drivers of deteriorating nuclear security.

2. **Rapidly increasing complexity and velocity**: Intensifying geopolitical competition, as well as the introduction and availability of new military and commercial technologies to state and non-state actors, are increasing the complexity of nuclear crises and the pace at which they unfold. Two challenges emerge as the time available to discuss and respond to fast-moving nuclear crises dwindles ever closer to zero. First, the ability of people to accurately discern and appropriately respond to nuclear crises will be diminished. Second, and as a result, humans may enhance their reliance on technical solutions, including artificial intelligence, to digest relevant information quickly. Combined, these two challenges will make it difficult to stop nuclear response protocols once they begin, and will create an environment in which miscalculation, accidental escalation and even pre-emption become more likely.

3. **New catalysts for nuclear crisis**: This fast-moving and complex environment will produce new triggers of crises and conflict that could escalate to nuclear confrontation – most notably climate change, but also cyberconflict and cascading proxy conflicts between nuclear-armed geopolitical competitors.

4. **Human factors, artificial intelligence and nuclear security**: Recent high-profile scandals related to the security of the United States' nuclear arsenal have generated growing concern about the effective implementation and monitoring of training protocols across organizations responsible for nuclear security in all nuclear-armed states. Moreover, insider threats were seen as a growing challenge to information technology and physical infrastructures relevant to nuclear security. Insider threats were also assessed to be an increasingly plausible mechanism for proliferating nuclear and radiological materials and know-how to non-state groups by lone wolves and insiders that share an ideological sympathy with these groups.

5. **New actors and new thinking about nuclear weapons requiring new solutions**: New mentalities and capabilities will require adjustments to long-held concepts of deterrence and dissuasion. Military planners will need to reconsider questions about the sufficiency of an arsenal's size and disarmament in order to establish and maintain nuclear stability in this environment.

In addition, discussion during the exercise covered several components of a broader approach to risk mitigation:

- **Transparency**: The need for enhanced transparency on the size of arsenals, nuclear doctrine and concepts of operations of advanced and destabilizing capabilities, such as hypersonics, was repeatedly stressed, as was increased intelligence sharing during nuclear crises. This is primarily because actions can be seen as predictable.
- **Training and education**: Analysis stressed increased emphasis on educating general populations about the severity of nuclear insecurity, especially to a younger generation that has no active memory of the Cold War risks of nuclear conflict.

- **Technical solutions**: Development of technical solutions to help slow down crises and increase transparency were seen as critical to mitigating risks associated with a deteriorating nuclear security environment.
- **Intelligence**: Horizon scanning analysis, including scenario planning, were seen as valuable tools for increasing the detection horizon for a nuclear-related crisis. They can generate robust signposts that a nuclear crisis is likely to occur.

Geopolitics Gone Awry

"Great power competition has returned."
– *Robert Work, US Deputy Secretary of Defense, in November 2015*

The working group developed three scenarios related to the Geopolitics Gone Awry phase. Each scenario abstract included in this section should be considered as a discrete challenge. Dynamics unfolding in one scenario are not necessarily relevant for the others. The scenario time frames are intentionally ambiguous in order to convey both the urgency and durability of the highlighted nuclear security challenges. Those include reckless escalation, miscalculation and failing geopolitical and security frameworks resulting from, in short, geopolitics gone awry. All the scenarios could occur in the next 6 to 24 months, and all are shaped by underlying competitive dynamics that could play out over a longer time horizon of several years.

North Atlantic Treaty Organization/Russia scenarios: The most frequently discussed scenarios leading to a nuclear crisis focused on those in which Russia is assumed to provide support for armed Russian separatist movements in member states of the North Atlantic Treaty Organization (NATO).

Conflict in the Baltic States was viewed as a particularly daunting and revealing path of escalation. The former Soviet republics of Estonia, Latvia and Lithuania have become particularly nervous because of Russia's annexation of Crimea, increased Russian surveillance flights over the Baltic Sea and the continuing conflict in Ukraine. Underscoring this critical situation is the Baltic States' geographic proximity to Russia, the Russian exclave of Kaliningrad and the large Russian populations residing in each of these states.

Initially, Russian nationalists protest in the Baltic States, at first and most intensely in Estonia, against the increased NATO presence in their skies. These protests lead to violence between state security forces and Russian protestors that quickly turn into armed separatist conflict. The ensuing, escalating spirals of inflammatory rhetoric; duelling statements of support by the United States and NATO (for its Baltic Allies) and by Russia (in defence of the right of self-determination of Russian separatists); and mobilization of military and security assets by both sides lead to a standoff – a pause before what appears to be an inevitable conflict between NATO and Russia. Baltic allies request assistance from NATO, under the North Atlantic Treaty's Article 5, to combat the growing challenges to sovereignty stemming from separatist conflict and to deter the possibility of direct Russian action. The United States puts its tactical nuclear forces in Europe on high alert, explicitly introducing a nuclear dimension to this escalating crisis. Russia has little choice but to heighten its nuclear readiness in response.

Western Pacific crisis: This scenario describes a pathway to nuclear crises through escalating military confrontations and conflicts over the contested borders and boundaries in the Western Pacific. It explores a specific path to conflict, first between Japan and China over control of maritime boundaries in the East China Sea, and then of the United States being quickly drawn into direct armed conflict with China as part of its treaty obligations to Japan.

The escalation of the conflict evolves in line with currently understood US and Chinese strategies and concepts of operation for prosecuting an anti-access/area denial versus power projection conflict in East Asia. Elements of the US 7th Fleet are driven back by China's DF-21D anti-ship ballistic missiles, successfully deployed among other anti-ship weapons launched from platforms on land, sea and air. The United States targets China's mainland military assets as part of the Air-

Sea Battle strategy, which was renamed in January 2015 as the Joint Concept for Access and Maneuver in the Global Commons. Strikes against China's homeland lead to the threatened or actual detonation of a nuclear device over a remote portion of the Pacific Ocean, designed to dissuade further military strikes against assets in Chinese territory.

Cascading proliferation: In this scenario, the number of actual, virtual, imminent or aspirational nuclear powers, especially in the Middle East/North Africa and East Asia, increases significantly and rapidly. An Iranian nuclear deal is the main trigger, considered as "too big to fail" particularly by the P5+1 states (China, France, Russia, the United Kingdom, the United States plus Germany). It also raises concerns among regional actors that this will enable Iran to join a small club of "latent" nuclear powers possessing the technological sophistication to develop nuclear weapons quickly. A simultaneous proliferation-related crisis on the Korean Peninsula creates a parallel level of unease in East Asia.

These crises combine with a series of events that starkly demonstrate the US inability to arrest both the deterioration of the security environment across the Middle East *and* the escalation of maritime border and boundary disputes in the Western Pacific. This leads to eroding confidence in US security guarantees and "nuclear umbrellas" among allies in both regions. Transparency is reduced in an increasingly unsettled environment by more available advanced military capabilities, such as long-range, precision-strike missiles and associated command and control infrastructure, as well as advanced computation, modelling and simulation that may eliminate the need for traditional testing.

This scenario's effects cascade metaphorically and literally beyond buttresses that have constrained proliferation in the past. Various types of proliferation – actual, virtual and partial – occur rapidly in this scenario, leading to at least four new "nuclear actors" pursuing proliferation in different ways and at different paces, with varying degrees of transparency. Such an environment invites a new and destabilizing calculus of deterrence and dissuasion. This scenario ends with the growing possibility of pre-emptive intervention in the Middle East to stop suspected nuclear proliferation.

Key Insights

1. **Escalation, miscalculation and a world in transition**: All scenarios highlight the growing potential for spiralling and frequently unintended escalation and miscalculation that arise from the intersection of two prevailing trends.

   First, the predominant geopolitical and security frameworks of the post-Cold War period are being challenged and revised. These include treaties governing proliferation of nuclear weapons-related materials, delivery systems and doctrines eschewing first use. Intense, overlapping and complex competition between regional actors marks the current geopolitical context; those actors frequently possess more and better capabilities, and more actors either possess or pursue nuclear weapons to some degree. These actors may have novel mindsets about nuclear weapons and the development of strategic systems that are materially different from the primarily bilateral concepts prevailing during the Cold War.

   The current geopolitical context also includes global powers entangled in geostrategic competition that is playing out in multiple regions simultaneously, increasing the number of alternative geographies and pathways for escalation. When pressure is applied to one geographic area of heightened geopolitical tensions, the potential for crises and conflict to

radiate out from the initial point of concern also increases. For example, the working group considered NATO/Russia escalation scenarios playing out in the Arctic, Middle East and parts of Eastern Europe (other than the Baltic States), where NATO's membership either overlaps with or borders Russia's conception of its near abroad.

Second, military modernization programmes can create destabilizing vulnerabilities and competition among nations over their technological prowess. Such programmes do this by prioritizing the development of systems designed to deliver very fast and low observable precision strikes at long distances (e.g. hypersonic weapons); moreover, they shorten crisis decision-making timelines and undermine nuclear stability. Efforts to develop advanced technologies designed to enhance "traditional" nuclear structures, such as India's ongoing testing of the Agni V canisterized missile, will also destabilize nuclear security and stability. In addition, emerging technologies (in many cases commercially available and foreseen to proliferate) are designed to challenge the effectiveness of networks and critical communication nodes (e.g. cyberweapons and electromagnetic spectrum disruption weapons). This will complicate, restrict and/or accelerate command and control in a time of crisis. While the relationship between many of these technologies and nuclear security will be explored in more depth in the second phase of the Nuclear Futures exercise, military modernization and proliferation of advanced capabilities were significant factors in driving escalatory dynamics in each scenario. Factors also included still-evolving or untested concepts in using these new capabilities, demonstrating the interconnectedness of the scenario categories investigated.

2. **Climate change as a trigger for nuclear crises**: In this complex and competitive context, new triggers of crisis and conflict will emerge that could escalate to nuclear confrontation. The magnitude of disruption associated particularly with climate change, local environmental degradation and related resource pressures (water, food and energy) will play a more prominent role in driving new theatres of competition, as well as enhancing strategic and existential vulnerabilities for nuclear-armed states. For example, three of them (China, India and Pakistan) are critically dependent on water flowing from the Himalayan glaciers. Any unilateral action to alter the existing balance of distribution could lead to confrontation; this, in turn, could set off a sequence of escalatory interactions that could overwhelm decision-makers' inhibitions and introduce nuclear weapons into a rapidly evolving regional crisis. Similarly, competition between nuclear-armed actors could increase in the Arctic, as warming conditions and receding ice enable more shipping traffic through, extraction of natural resources in and military operations across the region.

3. **Constraints on escalation**: The working group determined that opportunities to constrain escalation are already in place in some contexts, especially in the Western Pacific, where the US and China have developed more extensive military-to-military exchanges. Those can be built upon to limit and slow down, if not fully prevent, the escalation of a crisis. Currently, these tools may be insufficient to dampen trigger events that, after multiple rapid escalation cycles, could lead to a nuclear security crisis. They can serve, however, as a sound platform for building mechanisms to constrain and limit escalation and miscalculation.

   In contexts where these tools do not exist, as in the current taut and confrontational relationship between the United States and Russia, building measures for increasing transparency and elongating decision-making timelines during a crisis are urgently needed, even when geopolitical relationships are deteriorating. Developing and using these measures must involve government-to-government engagement, as well as private and informal dialogue

between non-governmental experts. Engagement and dialogue inject creative thinking into the process through mutually agreed analyses of critical issues and alternatives for intervention.

4. **Rethinking nuclear use**: The scenarios demonstrated that nuclear "use" should be considered more broadly than just the detonation of a strategic nuclear weapon against a population centre or critical infrastructure. Concepts of "use" should also include actors leveraging actual, virtual or aspirational nuclear arsenals for coercive geopolitical, political or economic advantage in a highly competitive geopolitical environment. The detonation of a small nuclear weapon in the Western Pacific scenario provides a stark example of the destructive power these weapons have, even without proximate loss of life. Concepts of nuclear "use" could also expand to include the development or employment of tactical nuclear weapons as a deterrent and a capability to wage war, especially against hardened targets increasingly inured to the effects of conventional "bunker-busting" weapons.

   The taboos and constraints on proliferation, including formal treaty constraints, will degrade without effective strengthening and recalibration of current nuclear security regimes, amplifying concerns about nuclear security, stability and proliferation.

5. **Deterrence and dissuasion**: Long-held concepts of deterrence and dissuasion must be revisited to account for this new and complicated environment, as in, how are arsenal sizes calculated that are sufficient to deter multiple actors with different interests? And, what delivery and deterrence systems are required to establish and maintain nuclear stability? This environment will also demand increased transparency, especially on the security of nuclear weapons materials and safeguards among all nuclear powers, to ensure state control of weapons in an environment with more proliferation.

6. **Transparency**: The future nuclear security environment is also likely to be more opaque in three key areas:
   - The actors that actually possess nuclear weapons capabilities or could develop these capabilities rapidly
   - The nature and level of sophistication in the capabilities of specific actors, including uncertainty around arsenal sizes, robustness of command and control practices, safeguarding procedures and the available delivery systems
   - The shifts in formal military doctrine on nuclear use in both old and new nuclear powers

   Lack of transparency in a changing landscape can lead to destabilizing assumptions and behaviours, especially in a world marked by nuclear proliferation. This could undermine deterrence and drive crisis and conflict rather than deter it.

7. **Pre-emption and first use**: Each of alternative futures introduced incentives for "first use" of nuclear weapons and/or conventional military pre-emption that target nuclear weapons or nuclear weapons development programmes. Particularly powerful drivers of pre-emption are nuclear delivery systems at high states of alert, as in the NATO/Russia scenarios, or the need to dissuade additional conventional conflict and strikes against the homeland of a nuclear power, as in the Western Pacific scenario. The cascading proliferation scenario presents two types of opportunities for nuclear-related pre-emption crises. In one, several new states with small nuclear arsenals lacking redundancy and resilience may incentivize first use. In the other, multi-actor, multi-speed and opaque proliferation of nuclear weapons would almost certainly invite escalatory rhetoric and behaviours, and possibly conventional or nuclear pre-emption.

Among the scenarios discussed but not featured in this White Paper was a Caroline Case scenario, which invokes the name of a security crisis in North America between the United States and Great Britain in 1837. Guidelines established as a result of the crisis became the foundations for international law on pre-emptive self-defence. In 1842, US Secretary of State Daniel Webster wrote in a letter to British Foreign Secretary Lord Ashburton that pre-emptive self-defence must be "instant, overwhelming, leaving no choice of means, and no moment of deliberation" for it to be justifiable.

This criterion is increasingly relevant and of concern as shifts in attitudes about the proliferation and use of nuclear weapons intersect with the rapidly diminishing time for responding to crises. States may be increasingly at risk of invoking this justification for pre-emptive self-defence, as decision-makers make the rational if hasty determination that fast-moving geopolitical crises and seemingly existential threats are "instant" and "overwhelming", and provide "no moment of deliberation".

Technology Gone Awry

"Space science, like nuclear science and all technology, has no conscience of its own."
– *John F. Kennedy, President of the United States (1961-1963), in a speech given at Rice University, 1962*

Through internal discussions and a one-day workshop held in Washington DC with members of the Global Agenda Councils on Nuclear Security and Cybersecurity, as well as the Meta-Council on Emerging Technology, the working group identified three distinct categories of nuclear security scenarios related to the Technology Gone Awry phase:

- **Spoofing/cyber**: In this scenario, a cyberattack from either a state or non-state actor is used to "spoof" a nuclear-armed state into believing that a (fictitious) nuclear strike has been launched against it. In the targeted state, all networked systems indicate that an attack has been launched, leading to the triggering of response protocols that, barring external intervention, will lead to a "retaliatory" strike.

- **Sabotage**: The use of cybertechnologies, robotics and electromagnetic pulse or other emerging technologies (or combinations of these technologies) to create physical damage to nuclear reactors or, especially, storage facilities, was considered a plausible scenario. For example, the cyberhijacking of a commercial airliner (a scenario laid out in a US General Accountability Office report in April 2015) and crashing of that airliner into a spent nuclear fuel pool would create a significant radiological effect. Similarly, participants explored scenarios that involved targeting spent fuel pools with difficult-to-detect and commercially available drones armed with explosives, or swarms of drones capable of overwhelming air and ground defences. Another sabotage scenario discussed was large-scale cyberattacks against non-nuclear critical infrastructure that could lead to a nuclear response.

- **Speeding up**: The development of advanced military technologies designed to deliver kinetic force from long distances and at great speeds – e.g. hypersonic weapons that travel between Mach 5 and Mach 10, or 5 to 10 times the speed of sound – could greatly destabilize nuclear security if concepts of operations and doctrines of use are not clearly stated and made transparent. Launching these missiles against a nuclear power would further reduce the time frames for determining the nature of the incoming threat (nuclear or conventional) and deciding on an appropriate response.

Key Insights

1. **Velocity, complexity and crisis stability**: Emerging technologies – those commercially available or for advanced military use – are amplifying threats to nuclear and geopolitical crisis stability by increasing the complexity of highly sensitive systems designed to avoid, slow down or de-escalate nuclear crises and the speed at which they unfold. The combination of technology-driven complexity and velocity is overwhelming human cognition and the ability to control these systems. This is especially the case given deficiencies in training and complacent mindsets among nuclear operators, as documented in the United States and elsewhere.

2. **The expanding threat spectrum and the asymmetric curve**: Many emerging technologies, such as cybertechnologies and cyber know-how, are increasingly commercially available or available to non-state actors, and provide a highly asymmetric means of exploiting nation states' vulnerabilities. The cost of developing technologies and practices to defend against a

cyberattack, for instance, far outweighs the cost of designing and executing such an attack. In addition, the current competitive dynamics of the global defence trade ensure that advanced military technologies are being transferred to emerging export markets. More actors can affect strategic and operational environments throughout the world because of the democratization of their ability and capabilities up and down the growing threat spectrum – from ideologically inspired and technologically savvy individuals all the way to modern nation states. In many cases, this allows the creative deployment of emerging technologies, enabling actors to affect these environments with limited financial or logistical burden.

3. **Lone wolves and new mindsets**: Lone-wolf actors, small motivated groups, transnational networks or insider threats were seen as the most likely source of the first two categories of threat-spoofing and sabotage. These actors would be motivated by the following mindsets (by one or a combination of them) that would legitimize cyberattacks targeting very secure nuclear systems to start a nuclear conflict or generate a nuclear/radiological disaster:

    - Nihilism
    - Extremist ideological or religious dogma that stresses the battle between good and evil, and "end of days" narratives
    - "Black hat" mentalities that venerate those capable of hacking the most secure systems, especially among a generation of young hackers that are at least a generation removed from the existential nuclear risks and fears of the Cold War period

Participants also noted the changed and changing mindsets of political and military leaders around the world that may view these capabilities merely as some of the many tools available to them to pursue interests, and therefore as weapons that could be used in a crisis.

Solutions: Several ideas were put forward for anticipating, precluding and mitigating risks during nuclear crises:

- **Air gap defences** could be implemented, through which critical industrial control systems are entirely disconnected from networks.
- **An international intelligence clearinghouse** would allow states that believe they are under a nuclear attack to rapidly access a “snapshot” of other countries’ intelligence that can either confirm an attack may be under way or indicate it is a spoofing/cyberattack instead. Participants understood that such a clearinghouse would be very difficult to engineer given intelligence-sharing concerns, but also suggested that some version of this capability should be considered
- **Increased education** about the risks associated with nuclear weapons and the potential for an accidental or intentionally manipulated nuclear launch should be pursued. This is especially important among a growing generation of young, highly technically proficient individuals who have little direct experience with or memory of heightened nuclear concerns.
- **Expansion of the detection horizon** via both technical and intelligence solutions should be a primary focus of nuclear-armed states. This would provide the maximum time available to gain the most complete situational awareness possible. Horizon scanning analyses, including scenario planning, were seen as valuable tools to create robust signposts and help enhance the abilities of defence and policy communities around the world to anticipate a nuclear crisis.

Nuclear Security and Non-State Actors

“An event has happened, upon which it is difficult to speak, and impossible to be silent."
– *Edmund Burke, British Parliamentarian (1774-1794)*

As the third phase of possible future nuclear crises, Nuclear Security and Non-State Actors focuses on such actors acquiring and using nuclear weapons or radiological devices. Discussion of nuclear-armed non-state actors frequently drifts to either of two areas: alarmist analyses highlighting the myriad pathways to acquisition, or dismissive reminders of the many logistical and technical obstacles non-state organizations face in acquiring and using these weapons. However, the working group believes that any discussion of future nuclear risk must include an earnest examination of the risks of proliferation of nuclear materials to non-state actors, particularly those inspired by millenarian or extremist religious ideologies.

The working group identified and discussed two types of future scenarios concerning nuclear-armed non-state actors, distinguished by the non-state actors' **strategic motivations** for acquiring and using nuclear weapons or materials: the "end of days" and "chaos catalyst" scenarios. The following section describes the conditions for these scenarios and provides general descriptions of representative pathways for non-state actors to acquire and use nuclear weapons.

End of days: The most urgent nuclear non-state concern is that a group espousing an apocalyptic ideology, such as Islamic State (IS), will acquire and subsequently use nuclear or radiological weapons to hasten the end of days and the victory of the group’s purportedly righteous ideology over the unrighteous. The 1995 Aum Shinrikyo sarin gas attack in Tokyo is a useful analogue for the end of days nuclear scenario.

While no credible evidence exists indicating IS (or another non-state armed group) has acquired or is close to acquiring or developing nuclear or radiological weapons, a series of recently published articles suggest the growing interest in and possible pathways for IS, in particular, to acquire nuclear weapons.

In May 2015, *Dabiq*, IS’s online propaganda magazine, featured an article stating that the group could use its considerable financial resources to obtain a nuclear weapon from Pakistan "within a year", with the intent to use the device against a Western city. The article’s claim of such acquisition occurring by mid-2016 is apocryphal. However, the broader narrative of IS leveraging its wealth to capitalize on ideological sympathy in current or future nuclear states is plausible, especially in an environment of nuclear proliferation with more nuclear actors.

According to several international media sources, the US Federal Bureau of Investigation collaborated with Moldovan authorities in October 2015 to thwart at least three attempted sales by smugglers of nuclear material on Moldova’s black market for radiological material. The most recent incident (in February 2015) was reported to include the attempted sale of material to ISIS. While questions have been raised about the reports' validity, these networks and black markets are of such concern to law enforcement and security communities in the United States, Moldova and across the region that they could be a plausible enabler of proliferation to IS or another apocalyptic non-state actor.

Moreover, in December 2015, The Center for Public Integrity published an article, subsequently republished in *Foreign Policy*, detailing persistent concerns about the security of nuclear materials in India, which has the fifth-largest stockpile of fissile material.

Taken together, this representative sample of articles provides a framework for developing scenarios of extremist and non-state armed groups acquiring and using nuclear weapons. Proliferation could occur through lone wolves (or small groups) within military and nuclear security organizations of nuclear-armed states who share IS's ideology and possess sufficient influence, access and scientific know-how to help supply weapons, material or knowledge to IS. These individuals and groups could work in conjunction with established networks to transport nuclear material or weapons to IS, while IS could use its on-line presence and global networks to recruit individuals with appropriate scientific and technical knowledge for using a nuclear or radiological device. Even in this scenario, logistical challenges do persist, meaning that targets in the Middle East or Europe seem more likely than those outside of IS's immediate vicinity.

Chaos catalyst: Nuclear or radiological weapons could also be used as part of a fanatical plot to provoke a massive and destabilizing reaction from state powers that would undermine security and stability in a given region or throughout the world, generate chaos and benefit an aspiring new world order. Of course, end of days scenarios could also include using nuclear or radiological weapons to elicit an outsized, escalatory and destabilizing response from other actors. A critical difference, though, is the overall objective. Chaos catalyst seeks escalation to support improving the position of a non-state group relative to its adversaries in order to drive future strategic gain, while end of days looks to create an apocalyptic conflict that will bring the ultimate triumph of its vision of "good" over "evil".

An example of the chaos catalyst scenario discussed during the exercise played out in South Asia. The scenario catalyst involved an attack by the militant group Lashkar-e-Taiba using a radiological device on the Rashtrapati Bhawan, the residence of the President of India, killing dozens of tourists and security personnel. The attack immediately amplified tensions between India and Pakistan, and set off a series of confrontations and miscalculations between the two nuclear-armed powers. India's subsequent deployment of significant military force along the Line of Control was seen in Islamabad as a prelude to a full-scale invasion and justified the pre-emptive launch of a nuclear-tipped missile on the Indian forces that were amassing on the Kashmir border (see Walter C. Ladwig III, "A Cold Start for Hot Wars? The Indian Army's New Limited War Doctrine", *International Security*, vol. 32, no. 3, Winter 2007/08, p. 164).

Key Insights

1. **Plausibility vs probability**: Discussion of nuclear use by non-state actors raises legitimate questions about the ability of these actors to acquire 1) nuclear weapons or materials, and 2) sufficient technical sophistication to safely handle and effectively use a nuclear or radiological device.

   However, the intersection of several prevailing trends and insights identified in previous sections and listed in the following points demand heightened awareness of the risks of and pathways to nuclear use by non-state armed groups, and make dismissal of this category of scenarios imprudent:

   - Institutional nuclear security controls are diminished, even within the largest and most established nuclear powers in the world.

   - New technologies, particularly social-media-related websites and applications, are powerful enough to recruit and inspire individuals to take action. These tools also facilitate coordination and planning of operations that circumvent law enforcement and the security community's intelligence, surveillance and reconnaissance activities.

- These technologies amplify the challenge posed by lone wolves, who include individuals with highly technical expertise and access to nuclear materials, and who sympathize with revolutionary and apocalyptic ideologies or seek to leverage their expertise for financial gain.
- Weapons could potentially proliferate to new state actors whose nuclear security controls are not developed.
- Global nuclear security risks are not fully appreciated.
- Mentalities change regarding use of nuclear weapons.
- The geopolitical environment is characterized by growing competitiveness.

2. **Human factors**: These scenarios reinforce the importance of human factors: training, best practice for control and transport of materials and weapons, and detection of insider threats. They also underscore the intelligence and security challenge associated with identifying or anticipating incidents in which human-factor vulnerabilities intersect with emerging technologies – in this case, information technologies and social media.
3. **Acquiring to use**: In both of these types of scenarios, nuclear weapons or materials are acquired with the intent to detonate them. Other scenarios, in which weapons are acquired with the intent to extort, were also considered. In all cases, however, non-state actors were viewed as acquiring weapons to use them, rather than to remedy military or deterrent imbalances.

Contributors

Authors

Members of the Global Agenda Council on Nuclear Security working group who contributed to this White Paper include: Graham Allison, Director, Belfer Center for Science and International Affairs, Harvard Kennedy School of Government, Leon Fuerth, Practitioner in Residence, Elliott School of International Affairs, George Washington University and Tate Nurkin, Senior Director, IHS Strategic Assessments and Futures Studies Center.

Acknowledgements

We would also like to acknowledge and thank the following people for the contributions to this report: Bernard S. Meyerson, Chief Innovation Officer and Vice-President, IBM Corporation (Meta Council on Emerging Technologies), Marc Porret, Legal Officer, Counter-Terrorism, Executive Directorate (representing Jean-Paul Laborde Executive Director, Counter-Terrorism Executive Directorate (CTED) United Nations (Global Agenda Council on Cyber Security) and Timothy Sandole, Research Assistant, Belfer Center for Science and International Affairs.

From the World Economic Forum: Jonathon Cini, Specialist, Knowledge, Networks and Analysis, Jonathon.Cini@weforum.org

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

The World Economic Forum, committed to improving the state of the world, is the International Organization for Public-Private Cooperation.

The Forum engages the foremost political, business and other leaders of society to shape global, regional and industry agendas.

World Economic Forum
91–93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland

Tel.: +41 (0) 22 869 1212
Fax: +41 (0) 22 786 2744

contact@weforum.org
www.weforum.org