Tri-Lab Support to STRATCOM Analytical Agenda FY23

Q3: How do non-state entities taking actions in a crisis or conflict impact escalation and deterrence?[1]

Anna Péczeli
Senior Fellow, CGSR, LLNL

Introduction

The term 'non-state actor' includes a wide range of groups that have generated a growing interest in the discipline of international relations. In security studies, analytical work on non-state actors usually focuses on terrorists, warlords, militias, rebel groups, criminal networks, private military companies, local self-defense forces, corporations and other business entities, non-governmental organizations, and financial institutions.[2] These actors generate many new challenges for the state-centric international order, and very often show the limitations of our theories and strategies to truly understand their impact. Since the end of the Cold War, the proliferation of actors has increased, and questions regarding the behavior of these actors and their impact on war and peace are of growing concern for governments.

This paper dives into a small subset of these concerns by examining the relevance of non-state actors for nuclear escalation and the practice of deterrence. The analytical focus is on a crisis or conflict situation where the tensions are already high. The main goal is to outline what kind of outcomes might emerge from the actions of non-state actors, what types of risk reduction and mitigation measures these outcomes require, and how these outcomes affect escalation and deterrence.

The structure of this paper follows the logic of the main question. It starts with a general overview of nuclear escalation pathways to show what factors could trigger nuclear use and how non-state actors are relevant in this regard. Since this issue is not a new phenomenon, the second chapter outlines the historical context and the primary concerns about non-state actors in the Cold War period. The third chapter talks about the current security environment and the new trends that increase the risks associated with non-state actors. The next part introduces a typology of possible outcomes with illustrative examples. The last two chapters focus on mitigation strategies and risk reduction, and the broader implications for escalation dynamics and deterrence.

[1] This work was performed under the auspices of the United States Department of Energy by Lawrence Livermore National Laboratory under Contract DE-AC52-07NA27344. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States government or Lawrence Livermore National Security, LLC. LLNL-TR-851252

[2] Andreas Kruck, and Andrea Schneiker, *Researching Non-state Actors in International Security Theory and Practice*. New York, NY: Routledge, 2017.

Pathways to Nuclear Escalation

Over the last decade, concerns about nuclear escalation have enjoyed an increased attention in official diplomatic circles and academic research efforts. The primary driver of this new focus is the growing consensus that nuclear dangers are on the rise. While there is a long list of reasons why the international community perceives that nuclear risks have increased, there is still a lack of consensus about who is generating those risks and what should be done about them.[3]

In a 1984 article, Joseph Nye argued that "*efforts to reduce the risk of nuclear war must start with an understanding of the likely paths by which a nuclear war might begin*."[4] This statement is just as true today as it was in the 1980s. Although the security environment has changed a lot in the past four decades, the different pathways to nuclear use still fall in largely the same categories. The main difference is in the shifting significance of these scenarios. In order to examine the relevance of these pathways in the current context, this paper adopts the framework developed by the United Nations Institute for Disarmament Research (UNIDIR). In a 2020 report, UNIDIR cataloged four main nuclear use scenarios:

- *"**doctrinal use** refers to use as outlined in declared policies, primarily based on retaliatory possibilities, with allowance for ambiguities in those policies;*
- ***escalatory use** refers to use linked to an ongoing tension or conflict, or to the introduction of nuclear weapons in times of crisis;*
- ***unauthorized use** refers to non-sanctioned use, including by rogue State actors, as well as use linked to non-State actors, including of lost, stolen, diverted, or crude nuclear devices; and*
- ***accidental use** refers to use linked to error, including technical malfunction and related human fallibility."*[5]

Identifying which scenario is the most likely today is heavily dependent on the context. Certain pathways have been more likely in the past, but due to significant changes in the security environment or successful risk mitigation strategies they are not in the forefront of attention anymore. For example, at the end of the Cold War the United States and Russia have banned classes of weapons, enhanced the safety and security of nuclear weapons and materials, and changed operational practices—such as alert postures and targeting—in order to reduce nuclear risks. These measures have successfully reduced the likelihood of many pathways that would fall under the unauthorized or accidental use scenarios.

In addition to the historical context, actors and regions can also determine which pathway is more likely to occur. Possible nuclear use scenarios are going to look very different in the India-Pakistan context, than in a NATO-Russia scenario. Another important factor is nuclear force posture—states that have a

[3] Ugne Komzaite, Anna Peczeli, Benjamin Silverstein, and Skyler Stokes, "Nuclear Risk Reduction in an Era of Major Power Rivalry." Center for Global Security Research Workshop Summary. Livermore, CA: Lawrence Livermore National Laboratory, February 2020. https://cgsr.llnl.gov/content/assets/docs/Nuclear-Risk-Reduction-Workshop-Summary.pdf

[4] Joseph S. Nye, Jr., "U.S.-Soviet Relations and Nuclear-Risk Reduction." *Political Science Quarterly* 99, no. 3 (1984): 404.

[5] Wilfred Wan (ed.), "Nuclear Risk Reduction: Closing Pathways to Use." United Nations Institute for Disarmament Research. Geneva: UNIDIR, April 2020. https://unidir.org/publication/nuclear-risk-reduction-closing-pathways-use

diverse arsenal with a secure second-strike capability are going to weigh nuclear use options differently than states with a small and vulnerable arsenal that could be completely eliminated in a preemptive strike.

It is also important to note that these pathways are not binary or mutually exclusive. There are several underlying risk factors that could feed into multiple use scenarios, or one scenario could trigger other use scenarios. With the great powers' inclusion of a broad range of non-nuclear strategic capabilities in their military toolkit, some of the conventional-nuclear firebreaks have disappeared and there is growing ambiguity about doctrinal red lines and escalatory thresholds. In a crisis situation, these uncertainties and ambiguities could be exploited by malicious actors to trigger unintended escalation.

From the perspective of non-state actors, the most direct pathway is unauthorized use, where rogue actors or non-state groups would acquire nuclear materials or devices to use them against their adversaries. However, non-state actors have the potential to interact with all other nuclear use scenarios as well. They could take direct actions to trigger escalation, or they could interfere in an ongoing conflict indirectly to manipulate outcomes and influence the behavior of actors. Malicious actions could add to the fog of war and incentivize nuclear use by reinforcing existing threat perceptions, exploiting human fallibility, or conducting false flag operations that could be misattributed to the opposing state. Due to the great variety of possible use scenarios and the different ways non-state actors could impact conflict dynamics, risk reduction measures and strategies also have to be tailored to the specific actors and problems.

Third-party escalation in a historical context

The risk that non-state actors could detonate nuclear devices or trigger nuclear escalation is not new to the 21st century. Nuclear-armed states have faced this threat from the early years of the Cold War. Studies about the impact of non-state actors on global security go back to the 1960s.[6] In the nuclear context, concerns about escalation due to the actions of a third party initially focused on small or new nuclear powers that could trigger a nuclear escalation between the United States and the Soviet Union—this was generally referred to as the 'N country problem.'[7] From the mid-1970s, these concerns came to include non-state actors, as the threat of nuclear terrorism started to rise. In 1962, Donald Kobe introduced the concept of a 'catalytic nuclear war'[8] which referred to the possibility that the actions of a third party could be misattributed, setting in motion a major nuclear exchange between the United States and the Soviet Union.

---

[6] Harry Eckstein, "On the Etiology of Internal War." *History and Theory* 4, no. 2 (1965): 133–163.
Ted Robert Gurr, *Why Men Rebel*. Princeton, NJ: Princeton University Press, 1970.
Grant Wardlaw, *Political Terrorism: Theory, Tactics and Counter-Measures*. New York, NY: Cambridge University Press, 1982.
Martha Crenshaw (ed.), *Terrorism, legitimacy, and power: The consequences of political violence*. Scranton, PA: Wesleyan University Press, 1983.

[7] Fred C. Ikle, Hans Speier, Bernard Brodie, Alexander L. George, Alice Langley Hsieh, and Arnold Kramish, *The Diffusion of Nuclear Weapons to Additional Countries: The 'Nth Country' Problem*. Santa Monica, CA: RAND Corporation, 1960.

[8] Donald H. Kobe, "A Theory of Catalytic War." *The Journal of Conflict Resolution* 6, no. 2 (1962): 125–142.

In such a scenario, the third party (a non-state actor or another state) would act as a catalyzing agent that would trigger a chain reaction of attacks and counterattacks between the superpowers. The main conditions that contributed to this threat included psychological factors—such as mutuals fears of pre-emption or feelings of vulnerability—and a new wave of nuclear proliferation. Despite the favorable conditions, many scholars questioned whether this was a plausible strategy since it was a very risky plan that would guarantee serious retaliation in case the plot was discovered. Furthermore, the improvements in nuclear early-warning systems and the establishment of direct communication channels between the United States and the Soviet Union made it very difficult to successfully implement such a plan.[9]

While the above considerations probably had a deterrent effect on rational actors (especially states), the possibility remained that certain non-state actors might actually prefer chaos and disruption, and would not be deterred by threats to their own survival. The rise of nuclear proliferation led to a number of nuclear weapon programs where states pursuing these capabilities did not always have strong safety and security standards for nuclear materials and devices. This coincided with a growing threat of terrorism in North America and Europe during the 1970s and 1980s. In this regard, the U.S. intelligence community concluded that terrorists might acquire the technical capacity to detonate a nuclear bomb due to several new risk factors: the growing sophistication of terrorist activities that often included increased lethality, the growing evidence of state support to terrorist organizations, the storage and deployment of nuclear weapons in areas that had intense terrorist activity, the increased number of potential targets (including forward-deployed nuclear weapons and nuclear power plants), and the advent of black markets that enabled the trade of nuclear equipment and materials.[10] However, the intelligence community also adopted the thesis that despite these risk factors, the threat of nuclear terrorism was still low. The core argument was that terrorists would probably not want to detonate a nuclear bomb because it would alienate public sympathy due to the mass and indiscriminate destruction of these weapons.[11] (This argument was mostly held until the rise of Aum Shinrikyo and al Qaeda in the 1990s that significantly changed the threat landscape since both organizations seemed to be intent on devising attacks with mass casualties.)

In response to the threat from non-state actors, risk mitigation strategies in the Cold War period mostly focused on strengthening U.S. nuclear security regulations to improve physical protection and material control and accounting.[12]

---

[9] James Johnson, "'Catalytic nuclear war' in the age of artificial intelligence & autonomy: Emerging military technology and escalation risk between nuclear-armed states." *Journal of Strategic Studies*, January 2021. https://doi.org/10.1080/01402390.2020.1867541

[10] Paul Leventhal and Yonah Alexander, *Preventing Nuclear Terrorism*. Lexington, MA: Lexington Books, 1987: 8.

[11] Matthew Bunn, Martin B. Malin, Nickolas Roth, and William H. Tobey, "Preventing Nuclear Terrorism: Continuous Improvement or Dangerous Decline?." Belfer Center for Science and International Affairs. Cambridge, MA: Harvard Kennedy School, March 2016. https://www.hks.harvard.edu/publications/preventing-nuclear-terrorism-continuous-improvement-or-dangerous-decline

[12] Ibid.

Revisiting the Issue of Non-State Actors in the Current Security Environment

Although the post-Cold War period has brough dramatic changes in the security environment, the same categories of nuclear use (doctrinal, escalatory, unauthorized, and accidental) are still applicable today. There are, however, important changes in the risks associated with these pathways. James Johnson identifies[13] four new trends that contribute to increased risks from non-state actors in the current environment: information complexity, greater automation of NC3 systems, disinformation, and nuclear multipolarity.

In terms of information complexity, emerging technologies—especially artificial intelligence (AI) and machine learning (ML)—are widely used to enhance capabilities and military operations. In the nuclear domain, these tools underpin every aspect of nuclear operations: 1) the operations and maintenance of nuclear forces, 2) the performance of nuclear forces, 3) the performance of non-nuclear forces that support nuclear operations, 4) analysis, planning, and decision support, and 5) active air and missile defenses.[14] While these advanced technologies can significantly enhance nuclear weapons surety (safety, security and positive control), increase the survivability and resilience of nuclear forces, expand leadership decision-time, and help to de-escalate a crisis or conflict, they also create unique vulnerabilities and risks. These advanced technologies interact in complex and sometimes unpredictable ways, shortcomings in training data and poor alignment between tools and tasks can undermine performance, and AI-enabled systems are also vulnerable to adversary actions. The main dangers include: 1) human dependence on the information provided by these systems can undermine decision-making if these systems are compromised, 2) information asymmetry can close the crisis bargaining window and cause deterrence failure, and 3) these technologies can also become sources of accidents and errors. Due to the nuclear-armed states' increased reliance on these systems, non-state actors no longer need physical contact with nuclear weapons to cause escalation. A dangerous and new threat vector in the current security environment is that non-state actors could penetrate or manipulate these systems through offensive cyber operations.[15]

The second risk factor is the greater automation of nuclear command, control, and communications systems (NC3). NC3 systems have historically faced problems with false alarms, accidents, close calls, and other risks due to human errors, computer mistakes, and technical malfunctions.[16] In the digital age, a new source of concern is automation. While some degree of automation in NC3 systems is almost inevitable, there is a broad scale between relying on AI for launch detection or delegating nuclear launch authority to machines. Nuclear-armed states usually make these decisions based on their technical capacity, and based on broader political factors, such as threat perceptions, or political structure. In general, there are many reasons to automate certain processes. AI can provide better and more comprehensive data analytics and produce faster responses to attacks than humans can ever do. But

---

[13] James Johnson, "'Catalytic nuclear war' in the age of artificial intelligence & autonomy."
[14] Mary Chesnut, Tim Ditter, Anya Fink, Larry Lewis, and Tim McDonnell, "Artificial Intelligence in Nuclear Operations: Challenges, Opportunities, and Impacts." Center for Naval Analyses, April 2023. https://www.cna.org/reports/2023/04/ai-in-nuclear-operations
[15] James Johnson, "'Catalytic nuclear war' in the age of artificial intelligence & autonomy."
[16] Eric Schlosser, *Command and Control*. New York, NY: Penguin Group, 2014.
Matthew Bunn, and Scott D. Sagan (eds.), *Insider Threats*. Ithaca, NY: Cornell University Press, 2017.

larger automation also creates more opportunities for malicious actors to exploit these systems. In the current security environment, where the speed of warfare has significantly increased and decision-making timelines have shrunk, stronger reliance on AI-enabled systems can increase the chances of accidents and provide new vulnerabilities for exploitation. Modern NC3 systems have many redundancies, which makes it very hard for non-state actors to interfere. However, in the midst of a crisis, non-state actors could launch AI-enabled false flag cyber operations to disrupt, deny, distort or destroy information to create misperceptions that could lead to unintentional nuclear escalation. The most extreme version of these attacks could include a penetration of NC3 systems to directly launch an unauthorized attack.[17]

The third risk factor is disinformation, misinformation and information manipulation. While the exploitation of the previous risk factors remains relatively difficult because the entry barriers are high (nuclear forces are heavily protected, NC3 systems are redundant and resilient), this category is much easier to access for non-state actors. With the growing sophistication of disinformation and misinformation tools, AI technologies can generate photorealistic audio and video materials that can be used to spread propaganda, enrage the public, and misplace blame. These tools are relatively low cost, they are widely available, and they can be spread on a massive scale. In a crisis or conflict, when tensions are already high, there might not be enough time to validate these video or audio sources. Growing pressures for retaliation could push a national leader into a corner and trigger actions based on false information. Malicious third-party actors running false flag operations are likely to put decision-making processes under a lot of stress, and they could increase the chances of unintended escalation.

The fourth risk factor is nuclear multipolarity. In the current security environment, there are many new competitive nuclear relationships. In most instances, risk reduction measures are completely absent, there are no mechanisms for de-escalation, there is a lack of transparency, and nuclear doctrines and escalation thresholds are ambiguous. Under these circumstances, nuclear risks are present, and any conventional conflict carries the threat of rapid escalation. Growing tensions between nuclear-armed states can potentially provide new opportunities for non-state actors to manipulate the situation and trigger a nuclear exchange. Since national leaders already presume the worst about their adversaries, in a crisis or conflict, misperceptions could be the engines of inadvertent escalation. These risk factors are especially dangerous in highly asymmetrical nuclear relationships, where fears of a pre-emptive strike and worries about vulnerable NC3 systems would create first-strike incentives and further aggravate the situation.

Compounding these four main risk factors are human sources of error. These include: biases and pre-existing beliefs that could be manipulated with false information, information overload due to the sheer volume and speed of information, and automation bias whereby false positives or negatives could go unnoticed due to the excessive trust that humans put in AI tools.[18]

As a result of these risk factors, in the current security environment malicious actors have a larger toolkit at their disposal, many of which are low cost and easy to access. In comparison to the Cold War period, there are many new possible scenarios for nuclear escalation with new threat vectors that non-state

[17] James Johnson, "'Catalytic nuclear war' in the age of artificial intelligence & autonomy."
[18] Ibid.

actors could exploit. Due to the developments in AI tools and the increasing complexity of nuclear systems, there is a growing pressure to automate certain processes, which might undermine rational decision-making. If ISR capabilities are compromised, the degradation of the quality of information would create confusion and weaken decision-making processes.

With regards to the escalatory pathways, these risk factors are relevant for all major nuclear use scenarios. However, even in the current digitized environment, it remains very difficult to penetrate NC3 systems and directly launch an unauthorized nuclear attack. It is more plausible that non-state actors would attempt to indirectly exploit an ongoing crisis situation by manipulating information, using deepfakes, and weaponizing pre-existing threat perceptions to create the conditions for escalation due to miscalculations or human errors. In the UNIDIR categories, these cases would fall under the escalatory use and the accidental use scenarios.

Matrix of Outcomes

While the above chapter focused on the risks that provide new opportunities to non-state actors to affect escalation, it is also important to note that the role of non-state actors is not necessarily negative. By focusing on the actual outcomes of the actions of non-state actors, it is possible to categorize the outcomes based on two sets of criteria. On the one hand, actions of non-state actors can lead to positive or negative outcomes, and on the other hand, these outcomes can be intentional or unintentional. This chapter provides some illustrative examples to highlight how these actions could play out in real life. Since the analytical focus of this paper is a crisis or conflict situation, all of these examples reflect this context.

Table 1. The matrix of outcomes

Outcomes	**Intentional**	**Unintentional**
Positive	e.g. civil society's open source monitoring and verification methods	e.g. sanctions affecting the broader military balance, or services provided by companies are used for military advantages
Negative	e.g. nuclear terrorism, or the spread of misinformation by non-state entities	e.g. sanctions leading to increased reliance on nuclear weapons, or companies contributing to unintended escalation

On the intentional side of the spectrum, it is relatively easy to find illustrative examples for both positive and negatives outcomes resulting from the actions of non-state actors. On the unintentional side, however, the scenarios are a bit more difficult to identify and they are more speculative.

One example for a positive intentional outcome is open-source intelligence (OSINT) provided by civil society. Due to the rapid technological advancements in the current security environment, there is a growing array of intelligence sources—such as satellite images or trade data—that are now available for NGOs and researchers to purchase. New sensors and data sources allow civil society to take a larger role

in verification and monitoring activities. According to Melissa Hanham,[19] these non-state actors could play a positive role in verifying future arms control agreements, including one with North Korea. A big advantage of OSINT is that it is shareable—since there are no classification concerns, information can be shared freely with allies and international organizations. Information is also shareable with adversaries, and it can help to kickstart a new type of conversation about arms control and disarmament objectives. OSINT is also publicly verifiable, and findings can be discussed in a transparent way. Since many of these discussions are already happening on social media, it allows global participation, and these debates are happening in real time. Hanham argues that civil society could help to build trust prior to an agreement with North Korea by providing OSINT on military activities on the Korean Peninsula. This, however, could also help to de-escalate a crisis situation where a likely pathway to nuclear use would stem from miscalculation or accidents. Especially when non-state actors have already accumulated enough trust, their public analysis of a situation, backed by real time OSINT might help to diffuse tensions in a crisis scenario and reduce the risks of misunderstandings.

For intentional negative outcomes, there are two different examples that are worth mentioning. The first one is nuclear terrorism. Despite several successful risk mitigation steps to secure nuclear materials and weapons, nuclear terrorism is still a major threat today. In 2009, President Obama called nuclear terrorism "*the most immediate and extreme threat to global security*."[20] In the framework of the four Nuclear Security Summits between 2010-2016, significant progress has been made to address this threat, but the danger has not been eliminated entirely.[21] The Biden administration's 2022 Nuclear Posture Review warns that "*nuclear terrorism continues to pose a threat to the United States and our allies and partners*."[22] According to Matthew Bunn, terrorists still have the possible motive, capability and opportunity to detonate a nuclear bomb.[23] Violent Islamic extremists are motivated to strike back at the "crusader forces," and both the Islamic State and al Qaeda have demonstrated that they are not afraid to conduct attacks that result in mass killings. Bunn also notes that if a sophisticated and well-funded group acquires the needed plutonium or highly enriched uranium (HEU), they might be able to put together a crude nuclear bomb. The successes of the counterterrorism campaigns of the last two decades have reduced the terrorists' ability to realize such a plan but there are still a number of terrorist-controlled regions in the world where this could happen. In terms of opportunity, global stockpiles of HEU and plutonium are more secure than two decades ago, but domestic violence and insider threats continue to require high-level attention. Nuclear smuggling paths are not completely eradicated, and state-sponsored terrorism is still present. In the UNIDIR typology, this scenario would fall under the unauthorized nuclear use case.

---

[19] Melissa Hanham, "Using Open-Source Intelligence to Verify a Future Agreement With North Korea." Carnegie Endowment for International Peace, July 2021. https://carnegieendowment.org/2021/07/27/using-open-source-intelligence-to-verify-future-agreement-with-north-korea-pub-85006

[20] Barack Obama, "Remarks By President Barack Obama In Prague As Delivered." Office of the Press Secretary, The White House, April 2009. https://obamawhitehouse.archives.gov/the-press-office/remarks-president-barack-obama-prague-delivered

[21] Matthew Bunn, Martin B. Malin, Nickolas Roth, and William H. Tobey, "Preventing Nuclear Terrorism: Continuous Improvement or Dangerous Decline?."

[22] U.S. Department of Defense, "Nuclear Posture Review." October, 2022. https://media.defense.gov/2022/Oct/27/2003103845/-1/-1/1/2022-NATIONAL-DEFENSE-STRATEGY-NPR-MDR.PDF

[23] Matthew Bunn, "Twenty years after 9/11, terrorists could still go nuclear." *Bulletin of the Atomic Scientists*, September 2021. https://thebulletin.org/2021/09/twenty-years-after-9-11-terrorists-could-still-go-nuclear/

The other illustrative example for intentional negative outcomes by non-state actors is the case of misinformation. In 2017, Russian social media circulated a deepfake video of a U.S. B-52 bomber, alleging that the United States had accidentally dropped a 'dummy nuclear bomb' on a Lithuanian building.[24] In a crisis situation, these types of deliberate misinformation campaigns could significantly increase the fog of war, and they could potentially lead to unintended escalation. Non-state actors could use these tools to generate photo-realistic video or audio deepfakes of national leaders or military commanders and disseminate false orders or intelligence. Due to the democratization of many of these technologies, these scenarios are not even so speculative anymore. In 2017, for example, fake mobile alerts and social media messages were sent to U.S. military families and DoD personnel containing orders to evacuate the Korean Peninsula.[25] In the midst of a crisis, these types of misinformation campaigns can create confusion, enrage the public, and potentially contribute to unintended escalation.

Regarding the unintentional consequences of the actions of non-state actors, it is much harder to find obvious examples, especially those that are relevant for nuclear escalation in a crisis situation. These cases are more speculative, and the effects might not be immediate. Since President Putin launched a war against Ukraine in February 2022, an unprecedented level of sanctions and export control measures have been imposed on Russia. The sanctions that Western governments imposed have been followed by second and third order sanctions from over a thousand companies that decided to cease operations in Russia or limit their business activities in the country.[26] The cumulative effect of all these sanctions is that Russia's military industrial base has faced shortages of higher-end foreign components, and it is forced to find lower-quality alternatives for substitution. As a short-term effect, Russia will face difficulties in manufacturing, sustaining, and delivering advanced weapons and technology to continue its war in Ukraine. Despite these difficulties, so far, Russia has been successful in adapting to the sanctions and it is able to continue the war, but it has opted for a slower-paced attritional campaign.[27] While it is too early to judge how this will affect the nuclear domain, unintentional effects could be both positive and negative. On the positive side, in certain cases Russia was already forced to rely on nuclear delivery systems to sustain conventional missile strikes.[28] If these trends continue, the war could have a negative long-term effect on Russia's theater strike capabilities, and improve the military balance in favor of its adversaries. However, on the negative side, Russia still has a massive and diverse nuclear stockpile

[24] DFRLab, "American bomber did not drop a bomb on a house in Lithuania." *Medium.com*, June 2017. https://medium.com/dfrlab/fakenews-american-bomber-didnot-drop-a-bomb-on-a-house-in-lithuania-6ae64241fe9e135

[25] Dan Lamothe, "U.S. families got fake orders to leave South Korea. Now counterintelligence is involved." *The Washington Post*, September 2017. https://www.washingtonpost.com/news/checkpoint/wp/2017/09/22/u-s-families-got-fake-orders-to-leave-south-korea-now-counterintelligence-is-involved/

[26] Chief Executive Leadership Institute, "Over 1,000 Companies Have Curtailed Operations in Russia—But Some Remain." Yale School of Management, June 2023. https://som.yale.edu/story/2022/over-1000-companies-have-curtailed-operations-russia-some-remain

Carrie Mihalcik, Sarah Lord, and Corinne Reichert. "Companies That Have Left Russia: The List Across Tech, Entertainment, Finance, Sports." *Cnet.com*, June 2022. https://www.cnet.com/news/politics/companies-that-have-left-russia-the-list-across-tech-entertainment-finance-sports/

[27] Max Bergmann, Maria Snegovaya, Tina Dolbaia, Nick Fenton, and Samuel Bendett, "Out of Stock? Assessing the Impact of Sanctions on Russia's Defense Industry." Center for Strategic and International Studies, April 2023. https://www.csis.org/analysis/out-stock-assessing-impact-sanctions-russias-defense-industry

[28] Ibid. p.8.

that is largely intact. If Russia gets to the verge of defeat conventionally, President Putin might judge that he can only change the tides of war with a limited nuclear strike. Since the beginning of the invasion, Russia has laid the ground for such an attack through repeated threats and a public narrative that Russia is under an existential attack, which in the Russian military doctrine is a possible condition for nuclear use.[29] In the nuclear domain, another negative trend is that once the war comes to an end, Russia will need to reconstitute its conventional military forces, which under the current sanctions regime will take a long time. In the interim period, it is very likely that Russia will rely more heavily on its nuclear stockpile to achieve its national security objectives. If a crisis emerged under these circumstances, this increased reliance could actually contribute to a lower threshold for nuclear use.

The picture is similarly ambiguous when it comes to judging the effect of private companies that were contracted to provide assistance to Ukraine. The DoD contract with SpaceX's Starlink was aimed to provide broadband communications for Ukraine, and according to its original intent, the service was meant to be humanitarian. But the Ukrainian military found a way to leverage Starlink for drone operations against Russian troops.[30] This example demonstrates that while private companies may not want to affect military operations on the ground, their services might be used for military purposes. The cumulative effect of these types of contracts could make a difference on the frontlines, and they might help Ukraine to push Russian troops out of the country. If Russia accepts defeat, these effects are unintentional positive consequences, but if Russia resorts to nuclear use due to its conventional defeat, then one could make the argument that non-state actors played an unintentional negative role in escalation.

Practical Measures to Mitigate the Risks

As the previous chapter demonstrates, there are many different ways non-state actors could influence escalation in a crisis, and those actions affect different pathways to nuclear use. Therefore, responses and risk mitigation measures should also include a variety of actions that are tailored to the specific problem set. In the matrix of outcomes, positive outcomes obviously do not require a risk mitigation strategy. However, since non-state actors are becoming increasingly important in international politics, and their influence is growing, it would be wise to explore how governments can better take advantage of the opportunities they provide, and how they can coordinate with them in a crisis situation.

On the negative side of the spectrum, the two key themes are strengthening deterrence and improving resilience. While both strategies have a relevance for intentional and unintentional outcomes, nuclear deterrence has serious limits against terrorist organizations, or non-state entities such as malicious actors in cyber space. Therefore, in most of these cases, improving resilience should be at the center of attention. In addition to these two strategies, states can also choose to collaborate with each other to

[29] Kevin Ryan, "Why Putin Will Use Nuclear Weapons in Ukraine." Russia Matters, Belfer Center for Science and International Affairs. Cambridge, MA: Harvard Kennedy School, May 2023. https://www.russiamatters.org/analysis/why-putin-will-use-nuclear-weapons-ukraine

[30] Joey Roulette, "SpaceX curbed Ukraine's use of Starlink internet for drones – company president." *Reuters*, February 2023. https://www.reuters.com/business/aerospace-defense/spacex-curbed-ukraines-use-starlink-internet-drones-company-president-2023-02-09/

make it harder for malevolent non-state actors to trigger escalation. This chapter provides a number of recommendations under these themes.

On the **deterrence side**, nuclear deterrence has a very limited role to play against non-state actors. Due to credibility problems and legal considerations (including issues with proportionality and distinction), historically nuclear threats have not played a central role in these scenarios. This, however, does not mean that classic deterrence theory (where states are deterred from attacking each other due to the fear of retaliation) has no applicability to non-state actors. In the post-9/11 world, the Cold War understanding of deterrence has been expanded to address the new threats of the 21st century security environment. Counter-terrorism strategies have incorporated both variants of deterrence: deterrence by punishment (where the credible threat of punitive measures affects an adversary's intention to carry out an attack) and deterrence by denial (where an adversary's ability to carry out an attack is neutralized by defensive measures or by a policy to deny the acquisition of the capabilities that are needed for an attack). The application of deterrence by punishment is difficult against terrorist organizations because terrorists may not care about their survival, they do not necessarily fit the rational decision-making model, and since they are regularly hiding among civilian populations, military threats may not be considered credible. The Bush administration tried to circumvent these problems by declaring that any state that supports or enables terrorist organizations in the acquisition of WMD capabilities, would be held fully accountable[31]—this policy basically connected the non-state actor problem to state responsibility. While deterrence by punishment had more credibility against state actors, this strategy still left a number of open questions, like for example, does this state responsibility extend to negligence as well—what happens when terrorist organizations acquire nuclear weapons due to the lack of adequate safety and security measures.[32]

Applying the deterrence by denial logic to the nuclear terrorism problem was a much better fit. Most efforts in the post-9/11 period focused on implementing export controls to limit access to technology, improving the physical security of nuclear materials, weapons and facilities, and taking steps to prevent illicit trade. This strategy achieved important successes in nuclear safety and made it harder for terrorist organizations to acquire or use nuclear weapons. But despite these achievements, the threat of nuclear terrorism is still present. To strengthen deterrence against terrorist groups, the United States and its allies should invest more in the protection of high-value targets, and improve intelligence on terrorist cells.[33] It is also important to commit to stringent nuclear security principles, revitalize programs to implement effective and sustainable nuclear security, expand efforts to strengthen security culture, and combat complacency, revive an effective nuclear security dialogue with partners, and make nuclear security a priority again.[34]

---

[31] George W. Bush. "Defending Against Weapons of Mass Destruction Terrorism." The Bush Record, White House Archives, 2006. https://georgewbush-whitehouse.archives.gov/infocus/bushrecord/factsheets/terrorism.html
[32] Robert S. Litwak. *Deterring Nuclear Terrorism*. Washington, DC: Woodrow Wilson International Center for Scholars, 2016. https://www.wilsoncenter.org/publication/deterring-nuclear-terrorism
[33] Brad Roberts. "Deterrence and WMD Terrorism: Calibrating its Potential Contributions to Risk Reduction." Alexandria, VA: Institute for Defense Analyses, June 2007. https://apps.dtic.mil/sti/pdfs/ADA470305.pdf
[34] Matthew Bunn, Martin B. Malin, Nickolas Roth, and William H. Tobey, "Preventing Nuclear Terrorism: Continuous Improvement or Dangerous Decline?."

On the deterrence by punishment side, improving forensics capacity to attribute nuclear attacks is an important first step. Improving the credibility of deterrence threats also requires the ability to develop and execute military options in a timely manner, which requires better integration of deterrence capacities across the U.S. government. In this regard, declaratory policy also plays an important role. Since different groups perceive signals in different ways, declaratory policy might need to be adjusted based on how deterrence messages are perceived by adversary groups and their supporters.[35]

The lessons of nuclear terrorism have important implications for deterring other non-state actors. Since non-state actors include such a great variety of actors, there is no single formula of deterrence or coercion that would work against all actors. Punitive threats can be directed against leaders of an organization, supporting networks, or state sponsors. The penalties can include death, harm, imprisonment, or economic loss. Denial measures can complicate planning, impede activities, demoralize group members, or discourage hostile activities. Measures that could achieve these effects include military attacks, legal measures, economic measures such as sanctions, and better protection of potential targets. It is also important that actions against a single organization should always take into account the broader strategy to counter similar groups. While generic declaratory policy statements are unlikely to work against all non-state actors, these statements might still play a role in deterring state sponsors of non-state actors from assisting, or in any way facilitating strategic attacks that could trigger nuclear escalation. Therefore, clearly stating red lines and thresholds, and threatening punitive measures against state sponsors could help to complicate the risk-benefit calculus of adversary states and deter them from supporting major attacks by non-state actors.[36]

Due to the limitations of deterrence strategies, and the great variety of threat vectors that non-state actors could exploit, **improving resilience** is a crucial aspect of risk mitigation. These measures can work in tandem with deterrence, and fill the gaps where deterrence simply does not have credibility against non-state actors. As the chapter on risk factors outlined, the current security environment provides new threat vectors to nuclear escalation due to four main trends: information complexity, greater automation of NC3 systems, disinformation, and nuclear multipolarity. The United States and its allies can take many concrete measures to improve their resilience in the face of these new threats.

Growing information complexity and the wide-spread use of AI and ML tools carry a number of opportunities and risks as well. One of the first tasks is to conduct further research to understand the cyber offense-defense relationship, to prevent algorithm manipulation, to optimize human-machine partnership, and to learn with simulated data. Efforts should be aimed at operationalizing AI systems with low technical risk in high-consequence applications, and engineering fail-safe systems. These goals will require new protocols for testing, evaluation, validation and verification.[37]

---

[35] Brad Roberts. "Deterrence and WMD Terrorism: Calibrating its Potential Contributions to Risk Reduction."
[36] Payne, Keith B., et al. "Deterrence and Coercion of Non-State Actors: Analysis of Case Studies." Study Group Report, Fairfax, VA: National Institute for Public Policy, October 2008. https://nipp.org/wp-content/uploads/2021/05/Summary-Report-of-Deterrence-and-Non-State-Actors.pdf
[37] Hruby, Jill, and Nina Miller. "Assessing and Managing the Benefits and Risks of Artificial Intelligence in Nuclear-Weapon Systems." Washington, DC: Nuclear Threat Initiative, August 2021. https://www.nti.org/wp-content/uploads/2021/09/NTI_Paper_AI_r4.pdf

To address the threats associated with the greater automation of NC3 systems, nuclear possessors will need to harden NC3 systems and processes. These steps should include developing new risk assessment tools to better understand the threats, implementing safeguards, and building more resilience into permissive action links (PALs). It is also important to improve NC3 control protocols, and mechanisms to reduce nuclear risks by adding redundancies, and enhancing procedures, launch protocols and authentication codes.[38] There are five overarching themes that should underline these measures: 1) software and network protection, 2) data integrity protection, 3) protection of hardware, 4) access/security control, and 5) cybersecurity awareness.[39] Lastly, NC3 resilience also has an important human component: enhancing safeguards should also include better training and education of personnel, and more transparency through information sharing and data exchanges in the aftermath of incidents to further improve safeguards.

In response to the threat of disinformation, misinformation and information manipulation, the United States and its allies need to improve their digital resilience. This problem is not new, false information and misleading narratives have been used in warfare since ancient times. But due to the global reach of the internet and social media platforms, there is a disinformation revolution that provides malicious non-state actors with an opportunity to spread fake news at low cost and with increased reach. Current approaches to counter disinformation rely on manual fact-checking, content removal, and damage-control. While these methods can help to set the record straight retroactively, in a crisis or conflict situation with nuclear escalatory dangers, this is not enough. Besides, human fact-checking is just not realistic in the face of the sheer volume of information, and humans are also subject to their own biases, errors, and misinterpretations.[40] In order to develop the right measures, the United States and its allies need to work to better understand the information environment. Proactive communications that present facts early and routinely can help to reduce the gaps where disinformation could capture audiences. Flagging common sources of disinformation can help to warn audiences to ignore specific websites or authors. Reporting and countering disinformation immediately on platforms where they appear can help to prevent their spread. Carefully considering which types of information are worthy to de-bunk is also important, because such efforts might backfire and increase the profile of the disinformation.[41]

In addition to deterrence and resilience measures, the United States should also champion **cooperative measures between states** to influence the risk-benefit calculus of non-state actors. In AI applications, the United States should work with its allies, industry partners, and academia to mitigate the risks and

[38] James Johnson, "'Catalytic nuclear war' in the age of artificial intelligence & autonomy."
[39] Afina, Yasmin, Calum Inverarity, and Beyza Unal. "Ensuring Cyber Resilience in NATO's Command, Control and Communication Systems." Research Paper, London: Chatham House, July 17, 2020. https://www.chathamhouse.org/2020/07/ensuring-cyber-resilience-natos-command-control-and-communication-systems
[40] Johns Hopkins University, Imperial College London & Georgia Institute of Technology. "Countering disinformation: improving the Alliance's digital resilience." *NATO Review*, August 12, 2021. https://www.nato.int/docu/review/articles/2021/08/12/countering-disinformation-improving-the-alliances-digital-resilience/index.html
[41] North Atlantic Treaty Organization. "NATO's approach to countering disinformation: a focus on COVID-19." July 17, 2020.

develop the right risk reduction measures.[42] AI-related concerns should also be discussed among nuclear possessors to highlight the technical risks, and the strategic stability and crisis stability implications of AI use in nuclear weapons. To ease public concerns about AI applications in nuclear systems, states should also consider declaratory policy statements about their vision for human/machine control for nuclear weapons.[43]

With regards to combatting disinformation, working with allies to engage audiences and build resilience is an important first step. The United States should also seek cooperation with other partners, such as international organizations, national and local governments, private companies, civil society, independent media, and others to fight disinformation. Working with these entities can also help to implement new resilience mechanisms and regulatory frameworks. Taking advantage of existing technologies and using them in innovative ways could save time and resources. For example, natural language processing algorithms can help to identify indicators of emotions in posts that are more likely associated with false importation specifically designed to enrage or inflame the emotions of users.[44] Government entities and international organizations such as NATO should also work to strengthen their public relations outreach efforts and improve their social media presence to reach the next generation, promote citizens' digital literacy, and improve the skills of the general public to identify disinformation.[45]

The last risk factor of the current security environment is nuclear multipolarity. With increasing competitive dynamics among nuclear possessors, the risks of nuclear escalation have also gone up. In this environment, non-state actors have many new opportunities to manipulate a crisis situation and intervene to trigger escalation. To reduce these risks, nuclear possessors should engage in strategic dialogues and consultative mechanisms to discuss threat perceptions, nuclear doctrines and forces, increase transparency, and clarify thresholds. These discussions should include official diplomatic engagements, as well as mil-to-mil exchanges and technical dialogue. These efforts could serve as starting points to explore concrete risk reduction measures. The Biden administration has recently put forward a few proposals, including a formal P5 missile launch notification regime; a commitment to maintaining a "human-in-the-loop" for command, control, and employment of nuclear weapons; establishing crisis communication channels among P5 capitals; increasing transparency on nuclear policy, doctrine, and budgeting; and setting up guardrails for managing the interplay between nuclear forces and non-nuclear strategic capabilities.[46] If implemented, many of these measures would reduce the

[42] Mary Chesnut, Tim Ditter, Anya Fink, Larry Lewis, and Tim McDonnell, "Artificial Intelligence in Nuclear Operations: Challenges, Opportunities, and Impacts."
[43] Hruby, Jill, and Nina Miller. "Assessing and Managing the Benefits and Risks of Artificial Intelligence in Nuclear-Weapon Systems."
[44] Johns Hopkins University, Imperial College London & Georgia Institute of Technology. "Countering disinformation: improving the Alliance's digital resilience."
[45] Luke Englebert, Pedro Pizano, and Paul Fagan. "Recommendations to the NATO Alliance: How to Collectively Combat Misinformation." Washington, DC: McCain Institute. September 26, 2022. https://www.mccaininstitute.org/resources/blog/recommendations-to-the-nato-alliance-to-collectively-combat-misinformation/
[46] Jake Sullivan. "Remarks by National Security Advisor Jake Sullivan for the Arms Control Association (ACA) Annual Forum." National Press Club, June 2, 2023. https://www.whitehouse.gov/briefing-room/speeches-remarks/2023/06/02/remarks-by-national-security-advisor-jake-sullivan-for-the-arms-control-association-aca-annual-forum/

dangers of inadvertent escalation, and they could help to address misperceptions. They would also make it harder for non-state actors to manipulate a crisis and exploit first-strike incentives.

Altogether, none of the above measures provides a blanket solution to all the problems that non-state actors represent. But implementing a mix of deterrence, resilience and cooperative measures could significantly reduce these dangers. The biggest difficulty of cooperative measures is that they require willing partners. In order for the nuclear possessors to agree on any of the proposed steps, there has to be a common understanding of the risks and a mutual willingness to reduce those risks. Right now, these circumstances are largely absent, because several states believe that existing weaknesses and vulnerabilities provide opportunities for military advantage in a crisis. Until this attitude changes, those who are interested in reducing risks are forced to focus on strengthening deterrence and improving resilience.

Broader Implications

The study of non-state actors has gained increasing attention in the post-Cold War period. The growing variety and significance of these actors represents a host of new challenges and opportunities for international security. For a long time, the nuclear domain has been very state-centric and apart from the threat of nuclear terrorism, non-state actors were unlikely to play a substantial role in escalation dynamics. In the current security environment, however, a number of new trends have contributed to increasing worries about the consequences of their actions in a crisis or conflict situation.

Non-state actors can affect a nuclear crisis in a direct or indirect way. The idea that non-state actors could conduct a direct nuclear attack remains a very distinct threat. The entry barriers are still very high for an indigenous nuclear program, and there were a lot of important improvements in the safety and security of nuclear materials and weapons. Nuclear possessors have also implemented a number of safety protocols in weapons control and made their NC3 systems more resilient and redundant. Therefore, acquiring a nuclear device or hacking into an NC3 system to launch an unauthorized attack are very difficult to achieve. This, however, does not mean that risk mitigation strategies should completely ignore these problems. Due to the high-consequence-nature of these threats, nuclear possessor should always look for loopholes and invest in further enhancing nuclear safety and security.

The second route to affect a nuclear crisis is through indirect means, where non-state actors would not try to launch a nuclear attack, but instead they would interfere in a conflict to influence the behavior of states with the intention to trigger escalation. Conceptually, these nuclear use cases would fall under the doctrinal, escalatory, or accidental pathways. In the current security environment, these scenarios are more likely than direct nuclear attacks because non-state actors have a greater variety of tools to influence, and more opportunities to interfere. Due to growing information complexity, increasing automation of NC3 systems, more wide-spread use of disinformation campaigns, and rising nuclear multipolarity, new threat vectors have emerged to nuclear escalation. Emerging technologies provide non-state actors with dangerous new tools at low costs that can help to exploit tensions. In peacetime, inflammatory deepfakes, false information, or false flag operations are not likely to trigger nuclear escalation, because states have the time to respond after proper assessment of the situation. However,

in a crisis or conflict situation, when tensions are already high and states are paranoid, interference by non-state actors could result in more severe consequences. When leadership decisions need to happen under compressed timeframes, and public emotions might also come into play, mistakes are more likely.

At the same time, non-state actors can also play a positive role in a nuclear crisis and help states to stabilize the situation. Any comprehensive strategy to deal with non-state actors should aim to better understand both the opportunities and the risks associated with them. Collaboration with non-state actors is crucial to identify where mutually beneficial outcomes might be achieved, and it is also inevitable to implement the right risk mitigation strategies. Since deterrence alone is not adequate the handle the variety of problems that non-state actors represent, strengthening resilience and seeking cooperative measures are also essential to reduce escalatory dangers. The sky is not falling (yet), and there are many possible solutions to close the gaps, but in order to succeed, sustained leadership focus is needed.