CONCEPTUALIZING INTEGRATED DETERRENCE TO ADDRESS RUSSIAN CHEMICAL, BIOLOGICAL, RADIOLOGICAL, AND NUCLEAR (CBRN) ESCALATION

Natasha Lander
Ryan Arick
Christopher Skaluba

Atlantic Council
SCOWCROFT CENTER
FOR STRATEGY AND SECURITY

Atlantic Council

SCOWCROFT CENTER
FOR STRATEGY AND SECURITY

The Scowcroft Center for Strategy and Security works to develop sustainable, nonpartisan strategies to address the most important security challenges facing the United States and the world. The Center honors General Brent Scowcroft's legacy of service and embodies his ethos of nonpartisan commitment to the cause of security, support for US leadership in cooperation with allies and partners, and dedication to the mentorship of the next generation of leaders.

The Scowcroft Center's Transatlantic Security Initiative brings together top policymakers, government and military officials, business leaders, and senior experts from Europe and North America to share insights and develop innovative approaches to the key challenges facing NATO and the transatlantic community.

Cover photo: Marines walk to a chemical weapons site during a joint explosive ordnance disposal exercise at Marine Corps Training Area Bellows, Hawaii, Sept. 21, 2022. Photo by Marine Corps Cpl. Patrick King.

ISBN: 978-1-61977-292-2

CONCEPTUALIZING INTEGRATED DETERRENCE TO ADDRESS RUSSIAN CHEMICAL, BIOLOGICAL, RADIOLOGICAL, AND NUCLEAR (CBRN) ESCALATION

TABLE OF CONTENTS

Introduction 4
- Background 4
- Research Question 4

Key Findings Summary 4

Methodology 4
- Scenario-Building Workshop 5
- Interviews with Officials and Experts 5

Insights from the Scenario-Building Workshop 5
- Part I: Understanding the Effect of Russia's Conventional Warfare Capabilities and Regime Stability on CBRN Escalation 6
- Key Takeaways from Part I 6
  - *CBRN weapons are an attractive option for Russia to showcase its strength* 6
  - *Hybrid warfare remains a temptation for Russia to achieve its geopolitical agenda* 7
  - *Emerging technologies present new opportunities—and new challenges* 9
- Part II: Conceptualizing Integrated Deterrence Among the United States and its European Allies to Address CBRN Weapons Use 10
- Key Takeaways from Part II 10
  - *Civil-military coordination in critical sectors presents a key opportunity for allies and partners* 10
  - *Greater recognition of recurring challenges will overcome barriers to more effective coordination* 10
  - *Resilience in the information space is an important tool to combat Russian hybrid warfare* 10
  - *Technological developments offer important opportunities for CBRN attack counter-responses* 10

Insights from Interviews 11
- Allied Alignment Over the Severity of Russian CBRN Threats 11
- Existing Cooperation Among Allies Supports US Goals 12
- Areas for Improved Cooperation with Allies and Partners 13
  - *Information and intelligence sharing* 13
  - *Awareness of in-theater CBRN assets* 13
  - *Opacity of US Government can hinder closer cooperation* 13
  - *Expanding education about CBRN threats to a broader community* 13
  - *Improving civil-military cooperation* 13
  - *Mixed Understanding of Integrated Deterrence as a Concept* 14

Key Findings and Recommendations 14

Conclusion 16

Appendix A. Interview Participants 17

Appendix B. Scenario Workshop Methodology and Detailed Results 17
- Scenario Workshop Methodology 17
- Part I: Understanding the Effect of Russia's Conventional Warfare Capabilities and Regime Stability on CBRN Escalation 18
- Part II: Conceptualizing Integrated Deterrence Among the United States and Its European Allies to Address CBRN Weapons Use 19

Appendix C. Biographies and Acknowledgements 20
- Author Biographies 20
- Acknowledgements 21

INTRODUCTION

This report presents the findings and recommendations of the Atlantic Council project *Conceptualizing Integrated Deterrence to Address Russian Chemical, Biological, Radiological, and Nuclear (CBRN) Escalation*. The objective of this project was to develop an approach for incorporating European allies and partners into the US model of integrated deterrence against Russian CBRN use.

Background

Russia's foreign policy has grown increasingly destabilizing to US interests as its economic decline, adverse demographic trends, and conventional capability inferiority vis-à-vis NATO have led to an aggressive pursuit of military modernization. Of particular concern is Russia's routine flouting of arms control, disarmament, and nonproliferation norms. For instance, Russia violated its arms control commitments by developing and using a novel fourth-generation nerve agent, Novichok, in the United Kingdom in 2018.[1] Russia's exit from the New START Treaty in 2023 constituted a further move away from accepted arms control and verification standards.[2] These actions, combined with Russia's persistent false claims of US and Ukrainian development of biological weapons in Ukraine, contribute to an environment of volatility and instability, especially about the prospect of the Kremlin choosing to use CBRN weapons for punishment or compellence to seize military advantage, or to deter allied support for Ukraine.[3]

The hollowness of Russia's conventional capability, combined with its military doctrine and dangerous rhetoric, reinforces the important role that CBRN capabilities will likely play in Russian defense strategy in the coming years. However, there is currently a gap in US and European understanding of the manifestation of this risk in the near- to mid-term. Moreover, it remains uncertain how allies and partners fit into the United States' approach to mitigating CBRN risks through integrated deterrence, a cornerstone of the 2022 National Defense Strategy (NDS). As defined in the NDS, integrated deterrence entails "*working seamlessly across warfighting domains, theaters, the spectrum of conflict, all instruments of US national power, and our network of Alliances and partnerships.*"[4] This report explores how the United States can include allies and partners in integrated deterrence strategies to counter potential CBRN escalation by Russia.

Research Question

The research question guiding this project was, "What is the risk of Russian CBRN weapons use in Europe in the next five to ten years, and how can the United States counteract or mitigate such risk?" The project team considered several aspects of this research question to establish how best to involve allies and partners in ongoing and new US efforts to mitigate Russian CBRN threats, including the following:

- How the activities of NATO allies could fit into a US campaign plan to deter Russian escalation in Ukraine and beyond
- How the United States could maintain resolve among its allies while coordinating allied activities to support integrated deterrence objectives
- What specific steps the United States could take now to ensure European allies are part of a broader integrated deterrence strategy five to ten years from now

KEY FINDINGS SUMMARY

The Atlantic Council sought to identify and develop approaches for incorporating European allies and partners into the US model of integrated deterrence against Russian CBRN threats. We derived five key findings, summarized below, which incorporate the opportunities and critical challenges we discovered from the scenario-building workshop, insights from expert interviews and roundtable discussions, and background research. The *Key Findings and Recommendations* section explains each of these findings in detail, outlining actionable recommendations to address these challenges.

1. Allies and partners already significantly contribute to US approaches to counter Russian CBRN threats in Europe. Future cooperation—bilaterally, multilaterally, and through NATO—should focus on areas of greatest need as mutually identified by the United States and its European allies and partners.
2. As a concept, integrated deterrence is a useful frame for examining cooperation with European nations to counter Russia's CBRN threats, but the US Government should use this framing to identify new opportunities, rather than detract from or encapsulate ongoing cooperation.
3. Civil-military cooperation across a variety of sectors is essential to respond to CBRN threats, especially among public health agencies and law enforcement. To fully realize integrated deterrence in the next five to ten years, greater coordination among civilian and military communities—within the United States and among its European allies and partners—is essential to enhancing resilience.
4. Technological advances present significant opportunities and challenges for US cooperation with allies and partners to counter CBRN threats, especially as these threats become more complex. The United States and its European allies should remain vigilant about emerging threats, while leveraging new technological developments in detection and attribution systems and emergency response mechanisms to build comprehensive defenses against CBRN threats.
5. As Russia deploys hybrid warfare tactics to support and conceal potential CBRN escalation, the United States and its European allies must prepare to combat malign influence efforts, such as information influence activities, targeted assassinations, energy sabotage, and economic coercion, related to CBRN use as part of the US strategy of integrated deterrence.

METHODOLOGY

Two primary analytic approaches guided the research for this project: a scenario-building workshop and a series of interviews with subject matter experts and officials. The team also conducted secondary source research, including official publications from the US Department of Defense (DoD) and NATO, as part of our background research to corroborate information and insights from workshop and interview participants. Background research on scenario planning was also critical to developing the workshop methodology. Finally, the project team used Atlantic Council roundtable discussions with senior US and European officials to gauge perspectives on CBRN escalation risks and methods through the lens of integrated deterrence.

Scenario-Building Workshop

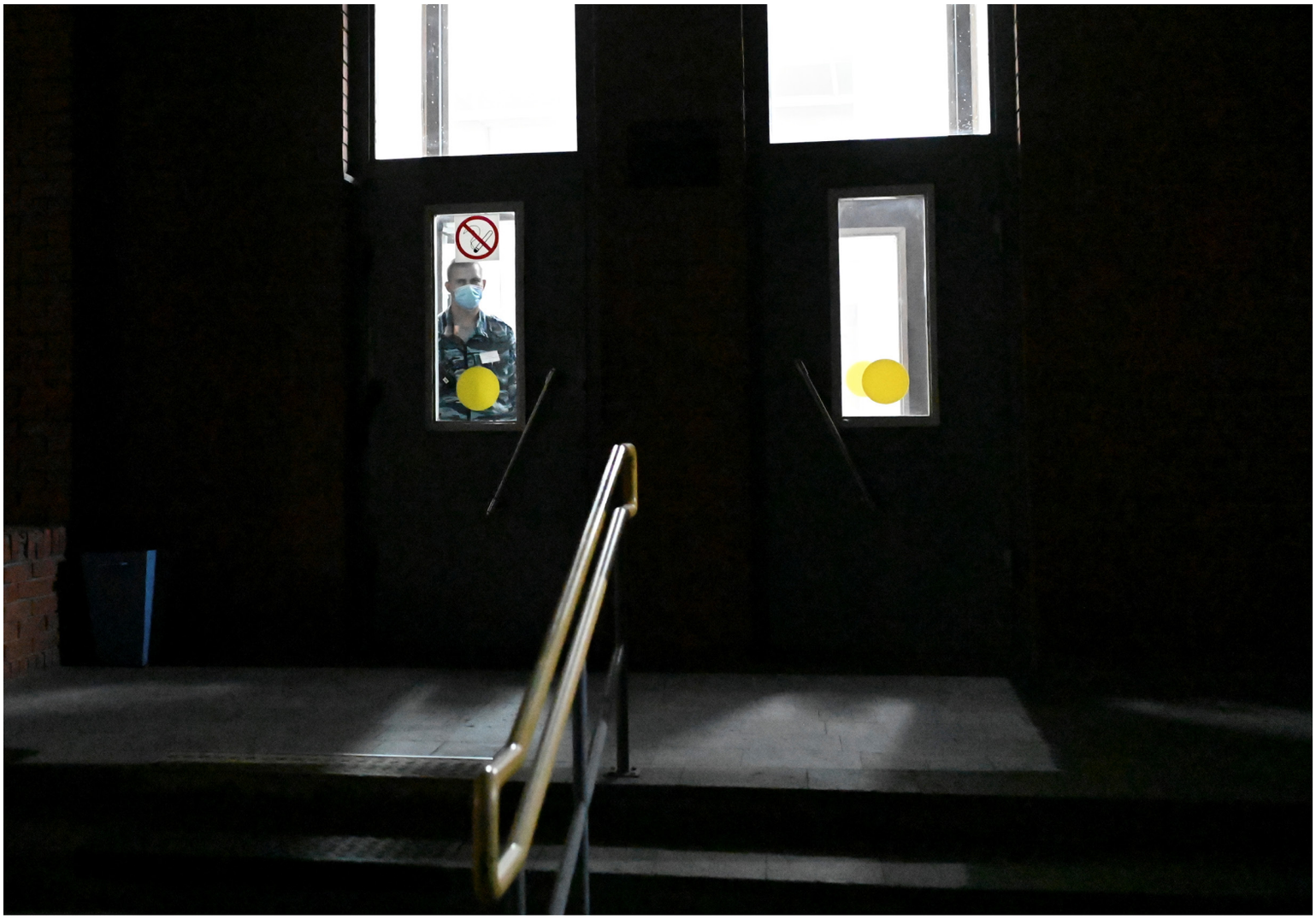
The Atlantic Council convened a group of experts and officials from the United States and Europe in December 2022 to participate in a scenario planning exercise to conceptualize integrated deterrence with respect to Russia's potential CBRN weapons use in Europe. Using strategic foresight scenario planning methodology, which involves a structured exploration of multiple plausible futures to inform present decision-making,[5] the workshop identified four possible futures for Russian CBRN use in Europe over ten years for which the transatlantic community will have to prepare. A more detailed explanation of strategic foresight planning is included in Appendix C.

The workshop encouraged participants to think creatively about possible future scenarios with respect to Russia's development and use of CBRN weapons. Using analytic tools prescribed by strategic foresight methodology,[6] participants explored options for future Russian decision-making around CBRN use and the consequent impact on the security landscape in Europe. Participants were divided into groups and asked to define the likelihood of Russia's use of CBRN weapons in the year 2032 using the parameters outlined in each of the four scenarios based on the interaction of two pre-selected factors: Russia's regime stability and Russia's conventional warfare capabilities. After briefing the plenary session on the results from the four scenario groups, participants were invited to identify opportunities for US-European cooperation through integrated deterrence strategies.

Interviews with Officials and Experts

To build on insights obtained from the workshop, the project team conducted 13 interviews with US, NATO, and European government officials, military officers, and civilian security experts from eight NATO member states. The list of organizations represented by the interviewees is included in Appendix A. These interviews provided firsthand perspectives to better understand possible scenarios for Russia's use of CBRN weapons and options for enhancing cooperation with allies and partners against CBRN threats.

A security guard looks through a door of a hospital, where Russian opposition leader Alexei Navalny receives medical treatment in Omsk, Russia. Navalny was taken ill with suspected poisoning en route from Tomsk to Moscow on a plane, which made an emergency landing in Omsk.
Alexey Malgavko via Reuters, 21 August 2020



INSIGHTS FROM THE SCENARIO-BUILDING WORKSHOP

To conceptualize integrated deterrence with respect to Russia's potential CBRN weapons use in Europe, the Atlantic Council's virtual scenario-building workshop presented four scenarios in a ten-year timeframe with respect to CBRN escalation. Comprehensive accounts of each of the four scenarios that participants designed, based on the parameters provided, are outlined for both Part I and Part II in Appendix B. The workshop illuminated several key themes, concepts, and takeaways, which we describe in detail below.

PART I: Understanding the Effect of Russia's Conventional Warfare Capabilities and Regime Stability on CBRN Escalation

For the first part of the workshop, participants considered the strengths and/or weaknesses of the Russian regime and Russia's conventional capabilities assigned to their scenario. Participants also considered how those characteristics could affect Russian decision-making around using CBRN weapons and the consequent impact on the security landscape in Europe. In advance of the workshop, the project team predefined these characteristics as the key drivers of change based on extensive background research.[7] The conditions of each scenario, as well as the key perspectives from participants and lessons learned, are included in Table 1 on page 7.

Key Takeaways from Part I

CBRN weapons are an attractive option for Russia to showcase its strength

Part I revealed participants' views that Moscow perceives opportunities to use CBRN weapons as a tactic to supplement conventional methods to achieve its geopolitical objectives. While Russia maintains a vast nuclear arsenal,[8] questions remain regarding the scope and scale of Russia's biological and chemical weapons capabilities.[9]

Table 1: Results from Part I of the Scenario-Building Workshop

Scenario 1: High Regime Stability and Strong Conventional Warfare Capabilities

Conditions: The Russian threat is acute due to the country's strong military capabilities and stable regime, which enjoys significant support at home. These characteristics could make the use of CBRN weapons more attractive to Russia, especially as a method to complement its conventional military strength.

Key Perspectives:

- Russia may employ technological advances, such as bioengineering, artificial intelligence, machine learning, and additive manufacturing, alongside strong conventional capabilities to increase its CBRN capabilities, especially with respect to tactical nuclear weapons and bioengineered weapons.
- Russia might also use CBRN weapons to demonstrate strength or as a means to expend fewer conventional forces in times of conflict.

Scenario 2: High Regime Stability and Weak Conventional Warfare Capabilities

Conditions: The Russian regime maintains control over political and social life, potentially drawing from continued authoritarianism and political repression. However, with weakened conventional power, Russia may turn to drastic measures to achieve its goals, including employing CBRN weapons.

Key Perspectives:

- To offset weak conventional capabilities, Russia may consider using CBRN weapons in targeted instances—such as political assassinations or direct attacks on critical infrastructure—with greater incentives to create unconventional weapons not governed by international norms.
- Russia may look to augment its nuclear capabilities to prop up its military power. Russia could refuse to relinquish control of its nuclear weapons arsenal or agree to future arms control treaties as a last means to maintain global legitimacy and offset the global posture of the United States.

Scenario 3: Low Regime Stability and Weak Conventional Warfare Capabilities

Conditions: Russia's regime becomes more fragile as its conventional capabilities weaken, raising the specter of instability in Eurasia. These factors leave fewer options for Russian decision-makers to achieve their geopolitical goals and, as such, Russia may employ CBRN weapons in both targeted assassinations and on the battlefield to achieve its geopolitical agenda.

Key Perspectives:

- With an unstable regime and weak conventional capabilities, Russia could lose its position as a world power, setting it on a course toward isolationism and instability. Its participation in and support for multilateral institutions, including arms control regimes and disarmament treaties that monitor compliance regarding CBRN weapons, are in question.
- Russia may place greater emphasis on its existing nuclear capabilities as a deterrent, consider isolated use of chemical and biological weapons to target political opponents, or employ tactical nuclear weapons against key targets to compensate for conventional weakness.

Scenario 4: Low Regime Stability and Strong Conventional Warfare Capabilities

Conditions: The Russian regime is vulnerable to both the Russian public and the international community, which could cause Russian decision-makers to rely on all available means to restore power and legitimacy, including through its strong conventional warfare and existing CBRN capabilities.

Key Perspectives:

- To reestablish or defend its regime stability from further erosion, Russia will seek to suppress democratic movements and growing support for opposition candidates. As a solution, Russia may turn to targeted CBRN attacks using chemical agents to neutralize opponents and further deter efforts that would challenge the Russian regime.
- As Russia's central authority weakens, illegal markets may surface where organized crime groups and terrorist organizations transport and transfer CBRN weapons, materials, and technology to malign actors, thus broadening the possibility of CBRN escalation and conflict beyond Russia.

As Russia becomes deadlocked or begins to lose the conventional war against Ukraine, Moscow may use CBRN weapons to achieve its objectives.

Regardless of whether Russia's conventional capabilities are strong or weak, two key trends emerged:

- When Russia is losing in a conventional war, the Kremlin will seek any potential opportunities to showcase its strength. While Moscow may not turn to large-scale deployment of CBRN weapons on the battlefield, it may turn to more frequent targeted strikes with CBRN weapons in the near term.
- Even if Russia is winning a conventional war, the Kremlin will maintain its CBRN weapons capabilities to project legitimacy and its status as a great power. Russia will also rely on CBRN weapons as a demonstration of strength and as a method of deterrence.

Hybrid warfare remains a temptation for Russia to achieve its geopolitical agenda

Throughout Part I, each scenario featured a significant emphasis on Russia's use of hybrid warfare to achieve its broader security goals.[10] Russia reinforces its conventional capabilities in war with hybrid warfare tactics, such as political executions and manipulation, foreign malign influence in the information space, economic coercion, cyberattacks, and energy sabotage.[11] This phenomenon extends to CBRN agents, with an emphasis on assassination attempts and information influence campaigns.

In all four scenarios, Russia leaned into hybrid warfare tactics to enhance its broader military strategy. The project team observed two key trends in this area:

- Russia may use CBRN weapons in a limited fashion to protect its domestic authority from political opposition, potential "color revolutions," and exiled activists. If the Russian regime is under threat from viable political opposition or active dissidents, the Kremlin may turn to targeted attacks using biological and chemical weapons in assassination attempts intended to neutralize any political threats to the Russian regime. This behavior is consistent with Russia's previous attacks—both inside Russia and within NATO member states, which targeted Viktor Yushchenko (2004), Alexander Litvinenko (2006), Sergei and Yulia Skripal (2018), and Alexey Navalny (2020), among others.[12]
- Over the last decade, Russia has turned to foreign malign influence efforts, especially within the information space, to support and amplify its geopolitical agenda. In particular, the Kremlin has injected escalatory rhetoric and inflammatory campaigns related to potential CBRN use and continues to circulate foreign malign influence efforts and propaganda to support its agenda.[13] These tactics target and weaken international regimes and treaty organizations that govern arms control, disarmament, and nonproliferation efforts, undermining public trust in multilateral organizations and leaving little room for recourse and accountability. Russia's malign influence tactics within the information space are intended to sow doubt and confusion among the public, deny responsibility for Russia's use of CBRN weapons, and undermine the effectiveness of an international response.[14]

A member of the CBRN unit decontaminates a boat, during the Baltic Tiger 2022 binational military exercise, which is a contribution at NATO's eastern flank, at the harbor in Tallinn, Estonia.
Lisi Niesner via Reuters, 24 October 2022

Table 2: Results from Part II of the Scenario-Building Workshop

Scenario 1: High Regime Stability and Strong Conventional Warfare Capabilities

Conditions: Russia could integrate CBRN weapons into its strong conventional capabilities. The United States and its European allies and partners would need comprehensive counter-responses to this threat, especially given Russia's regime stability in this scenario.

Key Perspectives:

- Allies must look beyond specific military preparations to incorporate civilian preparedness with respect to readiness related to potential CBRN attacks. These efforts would include strategic communication efforts to push back on escalatory rhetoric and maintain cohesion among allies.
- When Russia's conventional warfare capabilities are strong, it is more difficult for NATO to take a hardline stance to deter both conventional and hybrid warfare tactics. Greater coordination among allies is crucial, especially for detection and attribution of the use of CBRN weapons below NATO's Article 5 threshold, where an attack on one ally is an attack on all, resulting in a NATO-wide response.[15]

Scenario 2: High Regime Stability and Weak Conventional Warfare Capabilities

Conditions: Russia will likely pursue development of unconventional weapons to offset its weakened conventional warfare capabilities, including enhanced CBRN weapons not governed by international conventions. The United States and its European allies and partners would need to identify effective methods to counteract Russia's potential use of CBRN weapons to achieve geopolitical goals.

Key Perspectives:

- Allies should consider prioritizing greater integration of civil-military relations on critical security infrastructure, such as power grids, public health systems, cyber infrastructure, and other domains, to reinforce defenses against potential attacks with CBRN weapons.
- To combat CBRN-related threats at all levels, cooperation among the United States and its European allies and partners needs to extend beyond strategic-level decision-making. The United States could better coordinate and integrate operational and tactical planning in bilateral settings with its European allies as well as in multilateral platforms, such as NATO.

Scenario 3: Low Regime Stability and Weak Conventional Warfare Capabilities

Conditions: In this scenario, Russia is the most unpredictable in its behavior given its weakened conventional warfare capabilities and dwindled regime stability. This scenario would prompt the United States and its European allies and partners to prepare for any possible scenario in which Russia uses CBRN weapons.

Key Perspectives:

- The United States and its European allies and partners must prepare forces to fight through a contaminated environment to ensure complete and comprehensive readiness against CBRN threats.
- Conceptually, the United States and its European allies and partners should consider how deterrence against CBRN weapons use could be adapted and expanded beyond traditional forms of deterrence. Coordination at the multilateral level, such as within NATO, in which there is one central authority in charge of key priorities, may be effective.

Scenario 4: Low Regime Stability and Strong Conventional Warfare Capabilities

Conditions: In this scenario, Russia maintains strong conventional capabilities, but lacks centralized political control. The United States and its European allies and partners should prepare for potential scenarios in which the Russian military looks to the use of CBRN weapons to reassert political control.

Key Perspectives:

- There is a greater need to develop a holistic response following a CBRN event, including the design of decontamination, protection, and evacuation procedures. Specific safeguards can protect against and deter CBRN attacks, such as increased border security, intelligence capabilities, and investigative mandates.
- The United States and its European allies and partners must find opportunities to suppress and counter hybrid warfare and Russian malign influence. Strong counter-messaging strategies that debunk and proactively share truthful information before false flag scenarios can materialize and escalate could prevent Russia from turning to CBRN weapons.

Emerging technologies present new opportunities—and new challenges

Regardless of the strength of Russia's conventional warfare capabilities, participants agreed that the country will continue to explore technological advancements to aid its military modernization. In each scenario detailed above, Russia placed greater emphasis on dual-use material and technology, which have both civilian and military purposes, and pursued greater development of CBRN weapons.[16]

When Russia possesses few avenues for deploying conventional warfare capabilities, dual-use technologies and equipment present new opportunities for the Kremlin to achieve its geopolitical goals. For example, Russia may turn to increased imports and further refinement of nuclear technology and material; chemical and biological agents; missiles and unmanned aircraft systems; and associated materials and equipment. Such activities would permit, or at a minimum conceal, Russia's continued development of CBRN weapons.

In addition, the COVID-19 pandemic demonstrated how biological agents could cause destruction and disruption around the world. Russia inherited a portion of the Soviet-era biological weapons research program,[17] and while Moscow denies any continuation of the bioweapons program, allegations of its continuance remain.

Additionally, current developments in biology and chemistry, especially with respect to engineered organisms, viruses, pathogens, and other diseases, offer an avenue to create biological weapons with heightened virulence and infectivity that can threaten society.[18] Moscow could employ such technologies against its adversaries.

New technologies, such as artificial intelligence and machine learning, also introduce new challenges. Because CBRN capabilities and technologies have rapidly evolved, many developments are not explicitly covered in existing frameworks that govern responsible use. In each scenario, Russia may exploit these ambiguities to avoid export controls, treaty obligations, and other regulatory measures to improve these capabilities.

PART II: Conceptualizing Integrated Deterrence Among The United States and its European Allies to Address CBRN Weapons Use

For the second part of the workshop, participants considered how the United States could use integrated deterrence to incorporate European allies and partners into US strategy to respond to a scenario in which Russia would consider the use of CBRN weapons in Europe. The conditions of each scenario, as well as the key perspectives and lessons learned, are described in Table 2 on page 8.

Key Takeaways From Part II

Civil-military coordination in critical sectors presents a key opportunity for allies and partners

One important aspect of using integrated deterrence to address potential CBRN attacks from Russia is the need for greater dialogue and cooperation between civilian and military sectors. In Part II of the exercise, civilian institutions played a critical role in designing mitigative, preventative, and responsive measures to potential deployment of CBRN weapons. Organizations that coordinate disaster relief and humanitarian assistance might rely on military technologies and capabilities to respond to security threats, such as evacuation protocols from air and sea, medical support capabilities, and crisis response mechanisms. One perspective from the workshop highlighted that the United States has an ability to support and strengthen specialized training procedures for law enforcement personnel in Europe—especially in states that border Russia—to respond to hazardous environments, including those that are contaminated with CBRN agents. Greater integration between civilian and military organizations could better prepare civilian elements that might respond to a possible attack from Russia using CBRN weapons.

Public health agencies play an important role in developing, acquiring, and deploying medical countermeasures against Russia's potential use of CBRN agents. Naturally occurring and human-made biohazards can inflict a significant amount of damage and disruption on broader society. Throughout Part II, participants placed a greater emphasis on developing an effective response to bioweapons, which demonstrated the need for the United States and its European allies and partners to prioritize coordination among public health and medical agencies as well as with the armed forces in times of crisis.[19]

Critical infrastructure—including energy, transportation, information technology, and communications systems—plays an important role in combatting CBRN threats, implementing critical responses, and protecting broader societal resilience.[20] In particular, the energy sector plays a crucial role in managing nuclear power and materiel capabilities and in the event of a potential CBRN attack, these facilities will require additional safeguards. Military forces depend on both the civilian and commercial sectors when responding to CBRN attacks to provide key services, such as transportation, communications, and energy reliability all while ensuring that sectors can withstand external attacks and internal disruptions. Workshop participants pointed to greater coordination among public and private sector partners as an opportunity to address vulnerabilities and increase overall preparedness. Increasing cybersecurity and mitigating risk within the cyber domain could reduce potential vulnerabilities and the risk of cyberattacks while protecting from potential CBRN attacks.

Greater recognition of recurring challenges will overcome barriers to more effective coordination

Throughout Part II, Russia had the opportunity to inflict further damage by exploiting weaknesses in the absence of coordination among the United States and its European allies. By sharing expertise and maximizing resources, the United States and Europe can address these vulnerabilities and build broader resilience efforts.

In Part II, participants recommended implementing methods to promote regular and coordinated intelligence sharing, especially related to CBRN attacks. One participant emphasized that formal and regular channels for exchanging information and sharing best practices would support a comprehensive response to CBRN threats from the United States and Europe. Another key point raised during the discussion was that as CBRN threats become more complex and more difficult to detect, the United States and its European allies should consider designating common standards and equipment across jurisdictions.

Resilience in the information space is an important tool to combat Russian hybrid warfare

In each scenario, Russia turned to hybrid warfare as a political tool to complement its conventional warfare tactics, sow doubt and confusion among the broader public, distort reality and objectivity, and ultimately offer cover for possible military intervention. To combat Russian malign influence and employ integrated deterrence against Russian threats, one participant suggested that a multipronged approach in the information space might encourage greater digital resilience on social media platforms, facilitate strategic communications efforts, and enhance media literacy programs. Proactive messaging among allies to counter escalatory rhetoric—especially with respect to CBRN capabilities and potential escalation—is especially critical. If the Russian regime becomes less stable and pursues any possible avenue to achieve its geopolitical agenda, the United States and its European allies and partners should consider methods to invest in and implement proactive messaging. Several opportunities exist for the United States and its European allies and partners to counter hybrid warfare such as through investing in early detection capabilities, augmenting information-sharing systems, and countering foreign malign influence and propaganda emanating from Russia.

Technological developments offer important opportunities for CBRN attack counter-responses

In each scenario in Part II, Russia turned to technological advancements to bolster its military capabilities, and new developments with CBRN capabilities were an important component of Russia's

Marine Corps Lance Cpl. Randy Negrillo uses Identifier U and a MultiRAE portable chemical detector to scan for hazardous material during exercise Toxic Bayou at Naha Military Port, Okinawa, Japan, Aug. 11, 2022. The exercise helped Marines refine skills in counter weapons of mass destruction operations across unique and challenging environments.
Marine Corps Lance Cpl. Weston Brown

overall force posture.[21] Participants recommended that in response, the United States and its European allies and partners utilize new technologies to enhance broader capabilities to deter, counter, and combat Russian CBRN attacks. One participant argued for greater collaboration through potential partnerships with the private sector, which is often at the forefront of research and development of emerging technologies.

INSIGHTS FROM INTERVIEWS

Our interviews with subject matter experts and government officials illuminated four major themes related to integrated deterrence of CBRN threats from Russia. The following section describes these themes in greater detail.

Allied Alignment Over the Severity of Russian CBRN Threats

The officials interviewed for this report took seriously the threat of Russia using CBRN weapons in the near-to-mid future. Specifically, respondents referred to the possibility of chemical weapons use, including through assassinations, further use of riot control agents in urban combat, or the deployment of tactical nuclear weapons.

Multiple interviewees also highlighted Russia's use of foreign malign influence as another aspect of its overall CBRN threat. Russia has a long history of making false claims that the United States and Ukraine are developing biological weapons, and this has continued during its war in Ukraine.[22] Some respondents feared Russia could conduct a false flag attack with chemical weapons. In such a scenario, Russia would promote false claims that Ukraine intends to use chemical weapons as a pretense for its own use of these weapons on Ukrainian soil. Russia made these claims in the lead-up to its February 2022 invasion of Ukraine, which renewed the credibility of Russian CBRN threats.[23]

Interviewees also commented on the conditions under which Russia could consider using a CBRN weapon. For example, escalation to CBRN use could occur if Russia were to view US- or NATO-led exercises or training events as a provocation. Such misunderstandings could have grave consequences for Ukraine or neighboring NATO countries. The depletion of Russia's conventional forces could also make it more likely for Russia to consider using nonconventional weapons, especially since reconstituting conventional forces would

Emergency personnel carry a woman out on a stretcher during a re-enactment of a hazardous situation in a subway train in the lower level of the Bay Subway station that is no longer in use in Toronto January 25, 2011. The Canadian Standards Association (CSA) and the Canadian government set up the event to reveal its new standards for emergency services personnel and equipment to respond to chemical, biological, radiological, and nuclear (CBRN) incidents.
REUTERS/Mark Blinch

take significant time. According to one US official, the risk of CBRN weapons use increases the longer the war in Ukraine continues.

However, some respondents questioned Russia's motivations for using a CBRN weapon in Ukraine or Europe now and in the future. Russia has demonstrated its disregard for global norms against the development and use of CBRN weapons through its use of fourth-generation chemical weapons to silence opposition figures; its long-standing support of the Syrian regime, which has used chemical weapons against its citizens since 2012; and its disruptive actions in non-proliferation treaty organizations. However, the international community would swiftly condemn Russia if Russia employed CBRN weapons on a larger scale in Ukraine.[24] At a technical level, it is difficult to control the spread of chemicals once they are released, which could result in Russian troops being sickened or killed as well. This contamination risk could also spread to NATO territory through air, soil, or water, possibly exacerbating the conflict beyond Ukraine.

In the event of Russian CBRN weapons use in Ukraine or in NATO territory, response options are less clear. Interviewees could not offer specific suggestions given the need to protect sensitive information, but several US and European officials identified the need for timely, accurate attribution of any CBRN weapons use to ensure perpetrators are brought to justice. Timely attribution requires forensic detection capabilities to be available in proximity to an attack, but current detection capabilities were considered insufficient. Some respondents also pointed to the role of civilian authorities in the event of a CBRN attack, as NATO or other military forces might not be called upon immediately. First responders and medical professionals might be a more expedient and appropriate choice depending on the location of an attack. Furthermore, there is also a question of when NATO or individual European allies would respond to Russian CBRN use: what is the threshold for response, and what would that response entail? One US official pointed out that Russia had already been accused of using riot control agents in combat, but that has not been enough to warrant a response from Western governments.[25] The threshold question is a topic of ongoing discussion among NATO and US officials.

Existing Cooperation Among Allies Supports US Goals

In Europe, proficiency in CBRN defense has typically resided in a small but active cadre of countries that cooperate in bilateral and multilateral formats and through NATO. The United States is active in NATO CBRN planning, but it also maintains its own relationships with European allies separate from Alliance constructs. Russia's threats of incorporating chemical or nuclear weapons into its tactics in Ukraine have garnered attention from countries such as Germany, Czechia, Poland, the United Kingdom, and others that have been historically more active in CBRN defense.

Additionally, NATO's CBRN Defense Policy was released in 2022—the first update in thirteen years.[26] The new policy provided allied countries with a framework to use to update or create their own national policies and bring them in line with NATO priorities. Several allied military representatives we interviewed referenced this policy, which promotes a coordinated approach based on Alliance-agreed priorities when describing how their national governments think about preparedness against CBRN threats. Given the leading role the United States played in shaping NATO's CBRN Defense Policy, US NATO CBRN personnel are active in operationalizing key tenets of allied and partner involvement in integrated deterrence in Europe.

An important step in enhancing US contributions to European CBRN defense was US involvement in the NATO Framework Nations Concept (FNC) CBRN Defense Cluster. The FNC construct began at NATO in 2014 as a way for European NATO member states to organize capabilities around specialized interest areas to promote interoperability and burden sharing.[27] Germany led the development of the CBRN defense cluster, which included contributions from several member states that participated in exercises and training events. According to a US European Command (USEUCOM) official familiar with the deliberations, incorporation of the United States into the CBRN defense cluster took two years of negotiations, as the FNC was originally intended as a way for European NATO allies to bolster their capabilities without the direct involvement of the United States. However, US integration into the CBRN defense cluster opens greater possibilities for US Government-led training and exercising designed to improve the readiness of NATO CBRN defense elements.

Additionally, the United States is expanding the network of countries it has traditionally worked with to promote CBRN defense-related initiatives in Europe. Part of the expansion strategy includes identifying allies with generally robust capabilities but specific weaknesses, such as the United Kingdom and Norway, which, if improved, could enable these countries to better train other European allies and partners. Two US officials we interviewed spoke to the power of broadening the network of countries with which the United States works closely on CBRN issues to empower regional leaders so that the United States does not have to play a direct role in all facets of cooperation. This type of cooperation deepens strategic integration with highly capable allies, which is an important facet of achiev-

ing integrated deterrence. As a regional leader in CBRN defense, Germany provides training to allies such as the Netherlands and France, and non-NATO countries like Austria, and hosts exercises that include US elements. In this capacity, Germany's efforts further US goals for integrated deterrence against Russia's CBRN threats.

Areas for Improved Cooperation with Allies and Partners

Interviewees identified five key areas for greater cooperation between the United States and Europe that would enhance overall preparedness against Russia's CBRN threats. These areas are described below.

Information and intelligence sharing

Every US official we interviewed mentioned the need to improve information sharing among the United States and its NATO allies, including sensitive intelligence about Russian CBRN threats. Sharing is possible to some extent given common classification standards at NATO but is much more difficult to achieve with non-NATO partners. The challenge is understood: the United States has information about Russian CBRN threats it cannot share. How to overcome this challenge to all allies' satisfaction is less clear, as it is not always possible to downgrade highly protected information. Information sharing has improved since the Ukraine invasion, with both the United States and United Kingdom sharing more within NATO, and the United States and individual allies have made progress on select topics. However, without an institutionalized process to improve intelligence sharing, it is difficult to prove why allies should make greater investments in their CBRN preparedness should the need arise to integrate a transatlantic response.[28]

Awareness of in-theater CBRN assets

CBRN threats require advanced planning to ensure preparedness and proper coordination within the US military and with allies. For example, in the event of an attack, a specialized US Army chemical company will have inadequate time to travel into theater to perform consequence management duties. US forces need to know which countries in Europe can provide such assistance and do so rapidly. One US official we interviewed believed it was imperative for allies to have the capability to collect samples, analyze them, and, if possible, attribute them without having to wait for a US or other European unit to arrive in country to strengthen their resilience.

However, if US forces are in theater during a CBRN attack, allied military commanders we spoke to were unaware what US forces would require of European allies, such as support for mobility or protection for people and equipment. Crisis planning efforts that began after Russia's invasion of Ukraine include CBRN preparedness measures to ensure staging and mobility of assets that might arrive in Europe for a CBRN contingency, which is an important step in ensuring that both US and allied forces understand what to expect from each other in the event of a CBRN attack.

Opacity of US Government can hinder closer cooperation

Several NATO allies we interviewed described challenges in understanding the depth and breadth of actors within the US Government that have some role in CBRN cooperation. For smaller countries with fewer resources for CBRN defense, it is easier to work with regional leaders, such as Germany, that are more familiar in both organization and approach than the US military. A better strategy for

Airmen fire M-16 rifles during a combat skills training exercise at Joint Base Andrews, Md., Dec. 2, 2022. The exercise involved a chemical gas simulation in which airmen in full mission-oriented protective posture gear returned fire.
Air Force Airman 1st Class Isabelle Churchill

communicating US CBRN defense and response activities and coordinating outreach to European allies would improve understanding and potentially facilitate easier cooperation.

Expanding education about CBRN threats to a broader community

Knowledge of nuclear deterrence and CBRN weapons capabilities atrophied at the end of the Cold War, leaving a notable gap in the overall US and allied understanding of nuclear threats across the total force. US, European, and NATO officials agreed that awareness of these topics cannot reside within specialized communities in the United States, NATO, or European nations. Ukraine has helped raise the profile of CBRN within NATO, but because the United States and Europe have viewed these issues as a niche capability for so long, it is difficult to compel all allies to pay attention to CBRN threats and take necessary steps to improve their overall posture and capabilities. NATO is trying raise the profile of these issues through its CBRN Defense Policy, but greater action is needed to expand CBRN-focused discussions to broader defense policy and planning committees that emphasize wider threats to the NATO alliance. Additionally, increased training and education in US and allied militaries is required to ensure equal understanding of CBRN threats. With enough time and emphasis from senior leaders, the United States and allied militaries can incorporate these topics into joint exercises and training events.

Improving civil-military cooperation

In many European countries, first responders and civilian authorities might lead the response to a CBRN incident, not the military. Medical professionals and law enforcement personnel might have a better understanding of the effects of chemical exposure, for example. Allied military representatives we interviewed recognized the need to establish more regular cooperation with civilian authorities, including exercises and cooperative planning, to better understand the role of each side in the event of a CBRN incident. NATO officials described some cooperation between NATO and the European Union's European External Action Service, but these discussions

are mainly used to deconflict the aid that the European Union and NATO provide to Ukraine; these discussions could happen more frequently and cover a broader range of topics. Additionally, the Euro-Atlantic Disaster Response Coordination Centre coordinates support among NATO member and partner states, but only for civilian entities.[29] To improve resilience, civil-military coordination is essential because a large-scale CBRN attack could result in military reliance on civilian hospital systems. While efforts are underway to improve connectivity between these two sectors, allied government officials expect progress to be slow.

Mixed Understanding of Integrated Deterrence as a Concept

US, European, and NATO officials broadly agree that knowledge of integrated deterrence is uneven across European allies. Even when non-US officials and experts recognized the term, they were unsure how it differed from existing CBRN cooperation activities either bilaterally with the United States, multilaterally with US and/or other European allies, or within NATO. The term is problematic for some nations, such as France, which has a nuclear-focused view of the term "deterrence"; even though French officials expressed understanding of what the United States is trying to achieve with the concept, their national views of deterrence prevent their support of the semantics.

A USEUCOM official we interviewed expressed difficulties communicating integrated deterrence to key allies because the concept is defined ambiguously and does not comport with how NATO views either conventional or nuclear deterrence, or related terms such as "coherence," "conventional-nuclear integration," or "deterrence by denial." Furthermore, incorporating integrated deterrence into CBRN cooperation was perceived by another US official as "difficult and unnecessary" when doing so interfered with ongoing cooperation activities.

Incorporating integrated deterrence into dialogue with allies could emphasize non-military means of countering Russian CBRN threats by emphasizing the use of all elements of national power. Some allies, such as Romania, already view activities associated with integrated deterrence in terms of a "whole-of-government" approach to cooperation. Such framing could broaden the aperture beyond military-to-military dialogues to include representatives from allied ministries of health, foreign affairs, and interior, and their US counterparts, for example. Security experts we interviewed believed that to communicate integrated deterrence effectively to allies, especially for a technical area like CBRN, US officials need to tailor the messaging to NATO and specific allies depending on the request. The United States should sustain these discussions to promote meaningful action to support US integrated deterrence priorities.

Army basic trainees conduct chemical, biological, radiological and nuclear operations during training at Fort Jackson, S.C., Sept. 1, 2022.
Alexandra Shea, Army

KEY FINDINGS AND RECOMMENDATIONS

These findings and recommendations are based on our research and the insights we uncovered through the scenario-building workshop and expert interviews. Where possible, we include the organization(s) that are the most appropriate to carry out our recommendations.

Finding: Allies and partners already significantly contribute to US approaches to counter Russian CBRN threats in Europe. Future cooperation—bilaterally, multilaterally, and through NATO—should focus on areas of greatest need as mutually identified by the United States and its European allies and partners.

Recommendation: Given the strength of US cooperation with many European countries on CBRN defense, continued US support should focus on areas such as improved information sharing, civil-military coordination, and awareness of Russian CBRN threats beyond the specialist community. Senior leader buy-in is critical to driving these changes, so the Defense Threat Reduction Agency (DTRA) should organize director-level engagements with senior leaders in the Office of the Secretary of Defense (OSD) and within each branch of the services that emphasize the importance of incorporating CBRN considerations in broader planning. US officials should also hold these discussions in parallel with key NATO allies, NATO officials at headquarters, and NATO military commanders at Supreme Headquarters Allied Powers Europe (SHAPE). The US should also discuss with NATO's Allied Command Transformation, which identifies opportunities to innovate and maintain a warfighting edge, how to incorporate CBRN considerations into defense planning and capability development with European allies and partners. Senior US and NATO headquarters-level discussions should also consider how, when, or if to respond to possible Russian CBRN weapons use.

Recommendation: The DoD should sustain its support for joint exercises, training events, and personnel exchanges with European allies and partners and at NATO, as US support contributes to enhanced interoperability and shared understanding of operational concepts. Areas that require increased engagement include intelligence sharing, risk assessments, and cooperative research projects. The DoD should promote specialized knowledge transfer programs to facilitate learning among allies and partners, while investing in joint collaborative research and development initiatives to produce advancements in CBRN protection and consequence management.

Recommendation: To improve information and intelligence sharing, the United States and its European allies should pursue greater collaboration on joint threat assessments related to CBRN weapons and capabilities stemming from Russia. The DoD should closely coordinate with relevant elements of the US intelligence community to increase collaboration with bilateral partners, especially as the Office of the Director of National Intelligence (ODNI) develops the Annual Threat Assessment of the United States.

Recommendation: Joint defense planning and preparedness efforts with respect to CBRN threats offer another opportunity for the United States to build on preexisting cooperation with its European allies. DTRA and the Defense Security Cooperation Agency should regularly coordinate to ensure mutual awareness of CBRN defense capabilities provided to allies and partners to identify possible redundancies and areas for additional support.

Finding: As a concept, integrated deterrence is a useful frame for examining cooperation with European nations to counter Russia's CBRN threats, but the United States should use this framing to identify new opportunities, rather than detract from or encapsulate ongoing cooperation.

Recommendation: Given the mixed understanding among NATO allies of integrated deterrence as it applies to CBRN-related cooperation, OSD Policy should provide clear guidance to USEUCOM, DTRA, and other DoD elements on how to build cooperation strategies in line with integrated deterrence objectives. This guidance should include other parts of the US Government where applicable, including the Department of State and the Centers for Disease Control and Prevention (CDC). Outside the United States, the guidance should include specific requests for European allies and partners that reflect mutual priorities in the region. Enhanced cooperation with allies that have strong CBRN capabilities should also remain a priority for USEUCOM and NATO activities to help establish strong regional leaders.

Recommendation: The United States and its European allies and partners can better integrate the military and private sector to maximize cooperation with industry and expand integrated deterrence. The DoD should enhance partnerships with the private sector, especially in key areas of critical infrastructure that would allow the United States and Europe to counter possible CBRN threats by recognizing and potentially mitigating vulnerabilities while promoting resilience.

Finding: Civil-military cooperation across a variety of sectors is essential to respond to CBRN threats, especially among public health agencies and law enforcement. To fully realize integrated deterrence in the next five to ten years, greater coordination among civilian and military communities—within the United States and among its European allies and partners—is essential to enhancing resilience.

Recommendation: A stronger partnership between the CDC and the European Centre for Disease Prevention and Control could strengthen US and European public health surveillance efforts. The US Government should invest in specialized training programs, capacity building, and information sharing alongside leading research institutions, such as the National Institutes of Health in the United States and the European Union's Framework Programme for Research and Innovation, which could help build integrated resilience strategies against biohazards and other threats.

Recommendation: Given the important role of law enforcement agencies related to CBRN threats, information sharing among the armed forces and law enforcement personnel is crucial. US and European military personnel can more closely collaborate with the appropriate law enforcement agencies to improve mutual awareness of protocols and enhance joint investigative efforts. DTRA can work through appropriate DoD channels to understand US government interagency activities to facilitate this integration. In addition, DTRA can identify opportunities for joint training exercises and tabletop simulations focused on CBRN threat scenarios, emphasizing interoperability and integration of capabilities from both civilian and military sectors.

Finding: Technological advances present significant opportunities and challenges for US cooperation with allies and partners to counter CBRN threats, especially as these threats become more complex. The United States and its European allies should remain vigilant about emerging threats while leveraging new technological developments in detection and attribution systems and emergency response mechanisms to build comprehensive defenses against CBRN threats.

Recommendation: The United States and its European allies and partners should leverage public-private partnerships to invest in new technologies that enhance capabilities to identify and counter Russian CBRN attacks. Supporting research and prioritizing ongoing support for these efforts, including joint research projects and cooperative initiatives to leverage resources, is key.

Recommendation: Through greater understanding of new technologies, the United States and Europe can employ new capabilities to mitigate, detect, and prevent CBRN attacks. The US and its European allies and partners can augment CBRN activation systems, which play a vital role in early detection and CBRN incident responses, with new technologies, such as more efficient sensors and early warning alert systems. In addition, reconnaissance, surveillance, and decontamination efforts can rely on new advancements with autonomous systems. In the long term, advances in biotechnology and medical capabilities could result in more effective countermeasures against biological agents. Additionally, artificial intelligence can analyze huge troves of data to identify patterns, trends, and potential threats related to CBRN attacks and can employ predictive capabilities for response planning and early warning. DTRA should work with the US Joint Program Executive Office for Chemical, Biological, Radiological and Nuclear Defense to understand the latest developments in these technologies to determine where additional investment is required.

Finding: As Russia deploys hybrid warfare tactics to support and conceal potential CBRN escalation, the United States and its European allies must prepare to combat malign influence efforts, such as information influence activities, targeted assassinations, energy sabotage, and economic coercion, related to CBRN use as part of the US strategy of integrated deterrence.

Recommendation: The United States and its European allies should build on pre-existing collaboration, foster knowledge sharing, and invest in fact-checking and debunking strategies to combat Russia's information influence activities related to CBRN weapons. DTRA's Information Resiliency Office, the Department of State's Global Engagement Center, ODNI's Foreign Malign Influence Center, and the US Cybersecurity and Infrastructure Security Agency, among other institutions, can enhance synchronicity and interagency coordination to promote accurate and reliable information related to CBRN issues. US officials must also sustain dialogue with European allies and partners on foreign malign influence efforts related to CBRN threats. Further emphasis on robust and sustained efforts that stress collaboration, education, transparency, resilience, and strategic communication between the United States and Europe is needed to counter Russian malign influence around CBRN weapons and potential false flag scenarios. Specific debunking and counter-response strategies should consider methods to communicate scientific and technical data to non-expert audiences.

Recommendation: To ensure success in this arena, the United States and Europe must strengthen broader societal resilience and safeguard political institutions from malign influence to mitigate the effectiveness of Russian hybrid tactics. Using collaborative and cross-border efforts in strategic communications can counter malign influence efforts that are part of Russia's hybrid warfare.

CONCLUSION

Russia will continue to pose a variety of CBRN risks that will necessitate a robust, coordinated response from the United States and its European allies and partners. The United States can use integrated deterrence as a framework to counter evolving threats by incorporating allies and partners in an effort to stop continued Russian CBRN provocations or, should use of CBRN weapons occur, to prevail against them.

Integrating capabilities across domains between the United States and Europe—including in the military, political, technological, economic, information, and cyber sectors—is critical to dissuade and dispel Russia from considering the use and escalation of CBRN weapons. Integrated deterrence emphasizes and relies on the collective efforts of the United States and its European allies in deterring, detecting, mitigating, and responding to CBRN threats while maintaining resolve and ensuring interoperability among capacities.

Key elements of a successful integrated deterrence approach include intelligence sharing, civil-military integration, joint exercises and rapid response capabilities, strategic communications and counter malign influence efforts, and technological investments. While questions remain about the operationalization of integrated deterrence, the United States and its European allies can enhance collective preparedness and protect shared security interests. Only through a unified, coordinated, and integrated approach can the United States and Europe effectively address potential challenges from Russia posed by CBRN weapons.

APPENDIX A. INTERVIEW PARTICIPANTS

We interviewed thirteen individuals for this report. The interviews were conducted in person in Washington, DC and Brussels, Belgium, and virtually when necessary. We selected interviewees based on their familiarity with concepts relevant to the research questions, including integrated deterrence, NATO CBRN defense capabilities, and bilateral and multilateral US-European cooperation to counter Russian CBRN threats. The organizations whose personnel we interviewed are provided in the table below. Most individuals declined to be named to protect their identity.

Interview Participant Affiliation
Anonymous
Office of the Under Secretary of Defense for Policy (2)
US Mission to NATO
USEUCOM
NATO International Staff
Federal Ministry of Defense of Germany
Ministry of Defense of the United Kingdom
Ministry of Foreign Affairs of Romania
Ministry of Foreign Affairs of the Republic of Lithuania
Ministry of Defense of the Republic of Latvia
Embassy of France to the United States
Center for a New American Security

APPENDIX B. SCENARIO WORKSHOP METHODOLOGY AND DETAILED RESULTS

Scenario Workshop Methodology

The Atlantic Council convened a group of experts and officials from the United States and Europe in December 2022 to participate in a scenario planning exercise to conceptualize integrated deterrence with respect to Russia's potential use of CBRN weapons use in Europe. Using strategic foresight scenario planning methodology, which involves a structured exploration of multiple plausible futures to inform present decision-making, the workshop identified four possible futures in which Russia could use CBRN weapons in Europe over ten years for which the transatlantic community will have to prepare.

The core questions that the workshop answered included the following:

- Under what conditions might Russia use CBRN weapons in Europe in the next ten years?
- What drivers might compel Russia to threaten or use CBRN weapons in Europe?
- How would transatlantic cooperation, both military and non-military, among the United States and its European allies look like in each scenario?

Scenario-building workshops are a classic strategic foresight technique used by the public and private sectors to consider alternative paths.[30] For this workshop, the scenario mapping methodology sought to reduce human bias by methodically exploring alternative futures and the factors that might cause them, so that decision-makers can better forecast global shifts and respond should they materialize. These exercises often use a 2x2 matrix technique to build the relevant scenarios. This matrix is built around a two-axis diagram that isolates two impactful and uncertain forces of change, where the ends of each axis correspond to one variation of each force, with the opposite end of the axis corresponding to the opposite version of the respective force. The axes designate four quadrants that correspond to four alternative worlds defined by the interaction of the two driving factors. Because the matrix structure is intentionally limiting, participants are required to concentrate their efforts on the most impactful, uncertain, and relevant factors that will drive developments over the coming years.

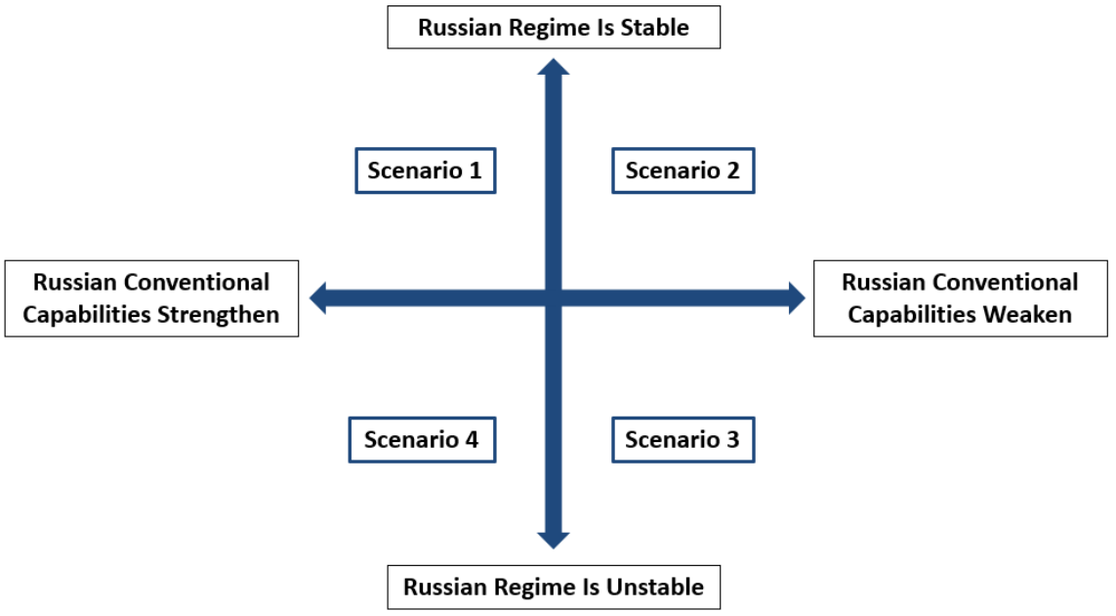
Before the workshop, the Atlantic Council completed a "trend analysis," or "driver mapping" process, which explored the fundamental political, economic, social, technological, legal/policy, and environmental (PESTLE) forces of change at work in Russia's circumstances. As part of the background research, the project team conducted significant background research on CBRN weapon development, Russia's conventional capabilities, and Russia's regime stability. After examining the forces of change and conducting background research, the project team identified two key driving factors that provided the analytic foundation for this exercise especially related to Russia's potential use of CBRN weapons: Russia's regime stability and the strength of Russia's conventional capabilities.

The workshop intended for participants to think creatively about possible future scenarios with respect to Russia's decision-making around the use of CBRN weapons and the consequent impact on the security landscape in Europe. Using the 2x2 matrix technique and methodology outlined above, workshop participants created four possible versions of the year 2032 based on the interaction of the two chosen factors specified above. The discussion developed narratives for possible futures in the next ten years that focused on the potential for CBRN escalation from Russia, scenarios for deterrence of Russian CBRN threats, and the transatlantic response to Russia in each scenario.

For this exercise, the resulting matrix (Figure 1) created by these two axes consists of four quadrants, each defined by the interaction of the key driving factors. The upper-left quadrant displays a case in which Russia's regime grows more stable at home while conventional capabilities strengthen. The lower-right quadrant displays the opposite scenario in which the Russian regime becomes more fragile as its conventional capabilities weaken, raising the specter of overall instability in Eurasia. The other two quadrants represent in-between worlds: The lower-left quadrant is one in which Russia's regime becomes more unstable while its conventional capabilities grow stronger, and the upper-right quadrant depicts a world where Russia's conventional capabilities weaken while the regime enjoys greater stability.

Thirty participants joined the workshop. In the first part of the exercise, the Atlantic Council divided participants into four groups (one per quadrant), and asked attendees to define the likelihood of Russia using CBRN weapons in the year 2032 using the parameters outlined in each of the four scenarios based on the interaction of the two factors. Following the breakout discussions, the Atlantic

Figure 1: Scenario-Building Workshop Matrix



Council reconvened everyone to discuss each of the four scenarios and the conditions under which Russia may use CBRN weapons.

In the second part of the exercise, the Atlantic Council outlined the US concept of integrated deterrence as defined in the 2022 U.S National Defense Strategy. Participants were then divided again into groups to identify opportunities for US-European cooperation through integrated deterrence strategies and methods to respond to scenarios in which Russia would escalate the use of CBRN weapons in Europe. The Atlantic Council reconvened everyone to share lessons learned from each of the four scenarios and the conditions under which the United States could better support integrated deterrence.

Part I: Understanding the Effect of Russia's Conventional Warfare Capabilities and Regime Stability on CBRN Escalation

For the first part of the workshop, participants were asked to consider characteristics regarding the strengths and/or weaknesses of the Russian regime and Russia's conventional capabilities assigned to their scenario, and how those characteristics could affect Russian decision-making around CBRN use and the consequent impact on the security landscape in Europe. The conditions of each scenario, as well as the key perspectives from participants and lessons learned, are included in detail below.

Scenario 1: High Regime Stability and Strong Conventional Warfare Capabilities

The Russian threat is acute due to Russia's strong military capabilities and a stable regime, which enjoys significant support at home. These characteristics could make the use of CBRN weapons more attractive to Russia, especially as a method to complement its conventional military strength. These factors could make it more appealing for Russia to pursue hybrid warfare tactics, including with CBRN weapons, especially in instances in which Russia seeks to safeguard its regime stability from political opposition and exiled activists. Russia may also use CBRN weapons in times of conflict outside of Europe to maintain conventional balance and multipolarity with the West. Russia may rely on heightened and escalatory rhetoric on potential use of CBRN agents, circulating foreign malign influence efforts and propaganda to support its agenda. Russia may employ technological advances, such as bioengineering, artificial intelligence, machine learning, and additive manufacturing, alongside strong conventional warfare capabilities to increase its CBRN capabilities, especially with respect to tactical nuclear weapons and bioengineered weapons. In this scenario, Russia may also use CBRN weapons to demonstrate strength. If the Russian regime is strong, it might also use CBRN weapons to expend fewer conventional forces in times of conflict.

Scenario 2: High Regime Stability and Weak Conventional Warfare Capabilities

The Russian regime maintains control over political and social life, potentially drawing from continued authoritarianism and political repression. However, with weakened conventional power, Russia may turn to drastic measures to achieve its goals, including employing CBRN weapons. In this scenario, Russia seeks to exert as much control as possible—including through heightened rhetoric of nationalism and Russian exceptionalism—as key sources of its regime's legitimacy. Russian messaging strategies, both at home and abroad, are positioned to counter the West and offer an alternative to the United States and Europe. To offset weak conventional capabilities, Russia may consider using CBRN weapons in targeted instances—such as political assassinations or direct attacks on critical infrastructure—with greater incentives to create unconventional weapons not governed by international norms. Russia may look to augment its nuclear capabilities to prop up its military power. Russia could refuse to relinquish control of its nuclear weapons arsenal or agree to future arms control treaties as a last means to maintain global legitimacy and offset the global posture of the United States. Russia might also utilize hybrid warfare in which CBRN weapons are augmented by malign influence. To expand the economy and boost conventional capabilities, Russia might search for additional meth-

ods to enhance military capacity, such as investing in the bioeconomy—the use of renewable biological resources to produce food, materials, and energy—or developing dual-use technologies and materials—that could translate into greater military capabilities.

Scenario 3: Low Regime Stability and Weak Conventional Warfare Capabilities

Russia's regime becomes more fragile as its conventional capabilities weaken, raising the specter of instability in Eurasia. These factors leave fewer options for Russian decision-makers to achieve their geopolitical goals and as such, Russia may employ CBRN weapons in both targeted assassinations and on the battlefield to achieve its geopolitical agenda. Because the Russian regime is weak and lacks a strong central authority, there is greater potential for instability in secessionist regions of Russia. The Russian regime scrambles to identify ways to improve its regime stability and compensate for lacking conventional capabilities, all while struggling to achieve its geopolitical agenda. Russia may place greater emphasis on its existing nuclear capabilities as a deterrent, consider isolated use of chemical and biological weapons to target political opponents, or employ tactical nuclear weapons against key targets to compensate for conventional weakness. In addition, criminal organizations and non-state actors may emerge as contenders to exercise power and cause societal disruption. Due to a weakened regime, Russian authorities may not effectively regulate the information environment or mitigate strong political opposition. With an unstable regime and weak conventional capabilities, Russia could lose its position as a world power, setting it on a course toward isolationism and instability. Its participation in and support for multilateral institutions, including key arms control regimes and disarmament treaties that monitor compliance regarding CBRN weapons, are in question.

Scenario 4: Low Regime Stability and Strong Conventional Warfare Capabilities

The Russian regime is vulnerable to both the Russian public and the international community, which could cause Russian decision-makers to rely on all available means to restore power and legitimacy, including through Russia's strong conventional warfare and existing CBRN capabilities. In this scenario, the military maintains strong capacity and remains well organized. With its great conventional warfare capabilities, Russia can inflict severe damage on military targets using unmanned aerial systems, targeted strikes, and missile attacks while increasing its technological sophistication, including in artificial intelligence. Russia may direct more resources into developing CBRN weapons that are harder to trace and identify, allowing the limited use of CBRN attacks. As Russia's central authority weakens, illegal markets may surface where organized crime groups and terrorist organizations transport and transfer CBRN weapons, materials, and technology to malign actors, thus broadening the possibility of CBRN escalation and conflict beyond Russia. To reestablish or defend its regime stability from further erosion, Russia will seek to suppress democratic movements and growing support for opposition candidates. As a solution, Russia may turn to targeted CBRN attacks using chemical agents to neutralize opponents and further deter efforts that would challenge the Russian regime. Russia may use methods that can complement its conventional warfare capabilities to inflict damage, including through hybrid warfare.

Part II: Conceptualizing Integrated Deterrence Among the United States and Its European Allies to Address CBRN Weapons Use

For the second part of the workshop, the project team asked participants to consider how the United States could use integrated deterrence to better incorporate European allies and partners into US strategy to respond to a scenario in which Russia would consider the use of CBRN weapons in Europe. The conditions of each scenario, as well as the key perspectives and lessons learned, are described below.

Scenario 1: High Regime Stability and Strong Conventional Warfare Capabilities

Russia could integrate CBRN weapons into its strong conventional capabilities. The United States and its European allies and partners would need comprehensive counter-responses to this threat, especially given Russia's regime stability in this scenario. As Russia relies on strong support for its political regime, including among the Russian public, the regime may turn to its strong conventional capabilities, augmented with CBRN weapons, to project its influence. When Russia's conventional warfare capabilities are strong, it is more difficult for NATO to take a hardline stance to deter both conventional and hybrid warfare tactics. Greater coordination among allies is crucial, especially for detection and attribution of the use of CBRN weapons below NATO's Article 5 threshold, above which NATO allies will come to one another's aid. Allies must look beyond specific military preparations to incorporate civilian preparedness with respect to readiness related to potential CBRN attacks. These efforts would include strategic communication efforts to push back on escalatory rhetoric and maintain cohesion among allies.

Scenario 2: High Regime Stability and Weak Conventional Warfare Capabilities

Russia will likely pursue development of unconventional weapons to offset its weakened conventional warfare capabilities, including enhanced CBRN weapons not governed by international conventions. The United States and its European allies and partners would need to identify effective methods to counteract Russia's potential use of CBRN weapons to achieve geopolitical goals. Participants shared that the United States and its European allies and partners should maintain a consistent focus on combating CBRN warfare with a greater emphasis on implementing specialized training exercises. With Russia's weaker conventional capabilities, NATO allies must also implement preparedness efforts to identify and discern accidental CBRN launches. The United States and its European allies should consider prioritizing greater integration of civil-military relations on critical security infrastructure, such as power grids, public health systems, cyber infrastructure, and other domains, to reinforce defenses against potential attacks with CBRN weapons. The transatlantic community must monitor new frontiers of CBRN development, including bioweapons and chemical agents, and should prioritize joint investigative mechanisms. To combat CBRN-related threats at all levels, cooperation among the United States and its European allies and partners needs to extend beyond strategic-level decision-making. The United States could better coordinate and integrate operational and tactical planning in bilateral settings with its European allies as well as in multilateral platforms, such as NATO.

Scenario 3: Low Regime Stability and Weak Conventional Warfare Capabilities

In this scenario, Russia is the most unpredictable in its behavior given its weakened conventional warfare capabilities and dwindled regime stability. This scenario would prompt the United States and its European allies and partners to prepare for any possible scenario in which Russia uses CBRN weapons. Because this scenario might serve as a launch pad for criminal proxies, non-state actors, and paramilitary groups to emerge and inflict damage on civil-military infrastructure, the United States and its European allies and partners must consider how a destabilized Russia could influence potential CBRN warfare in the region. The United States and its European allies must identify and implement methods to strengthen and defend critical infrastructure from targeted attacks using CBRN weapons, both from state and non-state actors. The United States and its European allies and partners must prepare forces to fight through a contaminated environment to ensure complete and comprehensive readiness against CBRN threats. Multilateral bodies, such as NATO, can serve as a central authority to preserve resolve around key priorities, including with respect to CBRN weapons use.

Scenario 4: Low Regime Stability and Strong Conventional Warfare Capabilities

In this scenario, Russia maintains strong conventional capabilities, but lacks centralized political control. The United States and its European allies and partners should prepare for potential scenarios in which the Russian military looks to use CBRN weapons to reassert political control. To prepare for any possible situation, allies must find ways to strengthen detection, warning, and attribution capabilities while training to mitigate CBRN attacks. In addition, allies should not silo readiness plans within national resilience strategies alone and should enshrine a higher level of cooperation in bilateral and multilateral settings. There is a greater need to develop a holistic response following a CBRN-event, including the design of decontamination, protection, and evacuation procedures. Specific safeguards can protect against and deter CBRN attacks, such as increased border security, intelligence capabilities, and investigative mandates. False flags in this scenario are especially likely, as Russia may instigate situations in which it may rely on its strong conventional warfare capabilities to achieve its geopolitical agenda. The United States and its European allies and partners must identify additional methods to suppress and counter hybrid warfare and Russian malign influence. It is critical for the United States and its European allies and partners to prioritize strong counter-messaging strategies that debunk and proactively share truthful information before false flag scenarios can materialize and escalate to prevent Russia from turning to CBRN weapons.

AUTHOR BIOGRAPHIES

Natasha Lander is a nonresident senior fellow with the Scowcroft Center's Transatlantic Security Initiative. She previously worked as a senior policy analyst at the RAND Corporation, where she led research on a range of issues, including chemical, biological, and nuclear policy; counterterrorism; European security; and military and civilian workforce policy. Lander has also served as an advisor within the Office of the Under Secretary of Defense for Policy. In this capacity, she aided the development of policy guidance influencing diplomatic, operational, and technical aspects of the international mission to remove and destroy Syria's declared chemical weapons. During her assignment at the Pentagon, Lander was also the principal advisor for NATO's Committee on Proliferation in the Defense Format, where she fostered implementation of policies to protect NATO allies against threats posed by weapons of mass destruction and strengthen NATO's chemical, biological, radiological, and nuclear preparedness. For her efforts, Lander was twice awarded the Office of the Secretary of Defense Medal for Exceptional Public Service. Prior to joining RAND, she was a senior analyst and deputy program manager at BAE Systems, where she authored a variety of analytic products for US Government policymakers.

Lander holds a master of science degree with distinction in psychology and the neuroscience of mental health from King's College London, a master of public policy degree from George Mason University, and a bachelor's degree in journalism with a dual major in political science from Bowling Green State University. Her analysis has been published in the *Cipher Brief, National Interest, Real Clear Defense*, and *US News and World Report*.

Ryan Arick is an assistant director with the Transatlantic Security Initiative at the Atlantic Council's Scowcroft Center for Strategy and Security. In this capacity, he supports the Transatlantic Security Initiative's work to strengthen the transatlantic alliance against emerging security threats from around the world. His research interests include NATO defense policy and transatlantic security; arms control, disarmament, and nonproliferation; democratic resilience from foreign malign influence; and state fragility and conflict prevention.

Previously, he served as an assistant program officer with the International Forum for Democratic Studies at the National Endowment for Democracy (NED), where he supported NED's transnational kleptocracy and democratic resilience portfolios. Prior to joining the International Forum for Democratic Studies, he worked with the National Democratic Institute's Central and Eastern Europe division, where he supported democracy programs in the Western Balkans as well as cross-regional grants to promote pluralism and good governance. He graduated from Indiana University with a bachelor of science in public affairs.

Christopher Skaluba is the director of the Transatlantic Security Initiative in the Atlantic Council's Scowcroft Center for Strategy and Security, where he and his team direct a broad portfolio of programming related to NATO and transatlantic security as well as manage a vast network of expert fellows.

Before joining the Atlantic Council, Skaluba served as a career civil servant in the Office of the Secretary of Defense, rising from presidential management fellow to the senior executive service. Among his roles in the Pentagon, Skaluba served as the principal director for strategy and force development, where he was responsible for assessing the future of international security and crafting the Defense Department's strategies to develop a prepared, capable, and effective US military. He also served a lengthy tenure as the principal director for European & NATO Policy, where he formulated and implemented US defense policy for Europe and conducted defense relationships with thirty-one European nations. In this capacity, he helped inaugurate the European Deterrence Initiative in the aftermath of Russia's 2014 invasion of Crimea. In other roles, Skaluba served as the acting deputy assistant secretary of defense for Middle East policy and in the Pentagon's Policy Planning office, working primarily on long-term competitive strategy development. His private sector experience includes completion of the Walt Disney Company's management development program.

Skaluba is a graduate of the Maxwell School of Citizenship and Public Affairs at Syracuse University where he earned a master of arts in international relations and where he intermittently serves as an adjunct Professor of Practice in international relations. He also holds a master of arts in English from Syracuse, teaching numerous classes in writing and rhetoric while pursuing his degrees. He holds a bachelor's degree in English and history from Penn State University. His writing and commentary are widely solicited and have appeared in the New York Times, the Washington Post, NPR, The Economist, USA Today, and War on the Rocks, and on various Atlantic Council platforms. He was the editor-in-chief of the seminal Atlantic Council essay series NATO 20/2020: Twenty Bold Ideas to Reimagine the Alliance after the 2020 US Election, where he was also a contributing author.

Acknowledgements

The research team thanks the US Defense Threat Reduction Agency's Strategic Trends Research Initiative (STRI) for sponsoring this work and for the guidance and support provided throughout the course of the project. Special thanks go to the wide range of experts and stakeholders, inside and outside of the US and European governments, who took part in the scenario-building exercise, contributed their perspectives during the interview process, spoke during roundtable discussions, and participated in other contexts to enrich the analysis.

We would also like to acknowledge Hans Binnendijk and Dr. Matthew Kroenig who offered strategic direction and key perspectives throughout the project. Within the Atlantic Council's Transatlantic Security Initiative team, we recognize our colleagues Leah Scheunemann, Anca Ioana Agachi, Zelma Sergejeva, Viltautė Zarembaitė, and Alvina Ahmed for their project management, peer review, and research support. We would also like to thank the Atlantic Council's Gretchen Ehle, Nicholas O'Connell, Ursula Murdoch, and Caroline Simpson, whose support for this project was invaluable.

This report is intended to live up to General Brent Scowcroft's standard for rigorous, relevant, and nonpartisan analysis on national security issues. The Atlantic Council's Scowcroft Center for Strategy and Security works to continue his nonpartisan commitment to the cause of security, support for US leadership in cooperation with allies and partners, and dedication to the mentorship of the next generation of leaders.

The views expressed herein are those of the author(s) and do not necessarily reflect the official policy or position of the Defense Threat Reduction Agency, the US Department of Defense, or the United States Government.

Endnotes

1. "Russia, the Skripal Poisoning, and US Sanctions," Congressional Research Service, August 14, 2019, https://crsreports.congress.gov/product/pdf/IF/IF10962.
2. "Russian Noncompliance with and Invalid Suspension of the New START Treaty," US Department of State, Office of the Spokesperson, March 15, 2023, https://www.state.gov/russian-noncompliance-with-and-invalid-suspension-of-the-new-start-treaty/.
3. "The Kremlin's Never-Ending Attempt to Spread Disinformation about Biological Weapons," US Department of State, Global Engagement Center, March 14, 2023, https://www.state.gov/the-kremlins-never-ending-attempt-to-spread-disinformation-about-biological-weapons/; "Many Speakers Voice Concern over Increase in Dangerous Nuclear Weapons Rhetoric amidst Ongoing War against Ukraine, as Disarmament Commission Opens Session," United Nations, Meetings Coverage and Press Releases, April 3, 2023, https://press.un.org/en/2023/dc3847.doc.htm.
4. *The 2022 National Defense Strategy of the United States of America*, US Department of Defense, 2022, https://media.defense.gov/2022/Oct/27/2003103845/-1/-1/1/2022-NATIONAL-DEFENSE-STRATEGY-NPR-MDR.PDF.
5. For more, see Alberto Behar and Sandile Hlatshwayo, "How to Implement Strategic Foresight (and Why)," International Monetary Fund, February 2021, https://www.imf.org/en/Publications/analytical-notes/Issues/2021/12/22/Strategic-Foresight-at-the-International-Monetary-Fund-463660.
6. See "Tools for Futures Thinking and Foresight across UK Government," UK Government Office for Science, November 2017, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/674209/futures-toolkit-edition-1.pdf; or Alun Rhydderch, "Scenario-Building: The 2x2 Matrix Technique," *Prospective and Strategic Foresight Toolbox*, June 2017, https://www.researchgate.net/publication/331564544_Scenario_Building_The_2x2_Matrix_Technique.
7. The project team conducted extensive background research related to the outlined drivers of change that formed the basis of the scenario exercise. On regime stability, see Robert Person, "Putin's Big Gamble," *Journal of Democracy*, September 2022, https://www.journalofdemocracy.org/putins-big-gamble/; Tatiana Stanovaya, "Russia's Elites Are Starting to Admit the Possibility of Defeat," Carnegie Politika, October 3, 2022, https://carnegieendowment.org/politika/88072; Richard D. Hooker, Jr., "Climbing the Ladder: How the West Can Manage Escalation in Ukraine and Beyond," Atlantic Council, April 21, 2022, https://www.atlanticcouncil.org/in-depth-research-reports/report/managing-escalation-in-ukraine/; F. Joseph Dresen, "Putin's Russia Today: Sources of Stability and Emerging Challenges," Wilson Center, https://www.wilsoncenter.org/publication/putins-russia-today-sources-stability-and-emerging-challenges. On Russia's conventional capabilities, see Scott Boston and Dara Massicot, "The Russian War of Warfare: A Primer," RAND Corporation, 2017, https://www.rand.org/pubs/perspectives/PE231.html; "Russia's Armed Forces: More Capable by Far, but for How Long?" International Institute for Strategic Studies, October 9, 2020, https://www.iiss.org/online-analysis//military-balance/2020/10/russia-armed-forces; Michael Kofman and Rob Lee, "Not Built for Purpose: The Russian Military's Ill-Fated Force Design," War on the Rocks, June 2, 2022, https://warontherocks.com/2022/06/not-built-for-purpose-the-russian-militarys-ill-fated-force-design/; John E. Herbst, Anders Åslund, David J. Kramer, Alexander Vershbow, and Brian Whitmore, Global Strategy 2022: *Thwarting Kremlin Aggression Today for Constructive Relations Tomorrow*, Atlantic Council, February 8, 2022, https://www.atlanticcouncil.org/content-series/atlantic-council-strategy-paper-series/thwarting-kremlin-aggression-today-for-constructive-relations-tomorrow/.
8. The Visual Journalism Team, "Putin Threats: How Many Nuclear Weapons Does Russia Have?" BBC News, October 7, 2022, https://www.bbc.com/news/world-europe-60564123.
9. See Robert Peterson, "Fear and Loathing in Moscow: The Russian Biological Weapons Program in 2022," *Bulletin of Atomic Scientists,* October 5, 2022, https://thebulletin.org/2022/10/the-russian-biological-weapons-program-in-2022/.
10. For background on hybrid warfare, see Christopher Chivvis, "Understanding Russian 'Hybrid Warfare,'" RAND Corporation, May 11, 2017, https://www.rand.org/pubs/testimonies/CT468.html; Alice R. Chen, Andrew Thvedt, Gregory F. Treverton, Kathy Lee, and Madeline McCue, "Addressing Hybrid Threats," Hybrid Center of Excellence, May 9, 2018, https://www.hybridcoe.fi/publications/addressing-hybrid-threats/.
11. For one explanation of Russia's hybrid warfare tactics, see Simon Tisdall, "Unseen and Underhand: Putin's Hidden Hybrid War Is Trying to Break Europe's Heart," *The Guardian,* October 23, 2022, https://www.theguardian.com/commentisfree/2022/oct/23/unseen-and-underhand-putins-hidden-hybrid-war-is-trying-to-break-europes-heart.
12. Patrick Reevell, "Before Navalny, a Long History of Russian Poisonings," ABC News, August 26, 2020, https://abcnews.go.com/International/navalny-long-history-russian-poisonings/story?id=72579648.
13. On biological weapons-related disinformation, see "The Kremlin's Never-Ending Attempt to Spread Disinformation about Biological Weapons," US Department of State. On chemical weapons related disinformation, see "The Kremlin's Chemical Weapons Disinformation Campaigns," US Department of State, Global Engagement Center, May 1, 2022, https://www.state.gov/wp-content/uploads/2022/05/The-Kremlins-Chemical-Weapons-Disinformation-Campaigns_edit.pdf.

14. For more, see Sarah Jacobs Gamberini, "Social Media Weaponization: The Biohazard of Russian Disinformation Campaigns," *Joint Force Quarterly 99*, November 19, 2020, https://wmdcenter.ndu.edu/Publications/Publication-View/Article/2422660/social-media-weaponization-the-biohazard-of-russian-disinformation-campaigns/; Abigail Stowe Thurston, "Russia's Non-proliferation Disinformation Campaign," *Bulletin of the Atomic Scientists*, March 22, 2022, https://thebulletin.org/2022/03/russias-non-proliferation-disinformation-campaign/.
15. See "Collective Defence and Article 5," NATO, updated April 14, 2023, https://www.nato.int/cps/en/natohq/topics_110496.htm.
16. For example, see Austin Wright, "Dual-Use Goods Are Fueling Russia's War on Ukraine," *Foreign Policy*, November 8, 2022, https://foreignpolicy.com/2022/11/08/dual-use-goods-are-fueling-russias-war-on-ukraine/.
17. Raymond A. Zilinskas, "The Soviet Biological Weapons Program and Its Legacy in Today's Russia," Weapons of Mass Destruction (WMD) Case Study, the Center for the Study of Weapons of Mass Destruction (CSWMD) at the National Defense University, July 18, 2016, https://inss.ndu.edu/Media/News/Article/848285/the-soviet-biological-weapons-program-and-its-legacy-in-todays-russia/.
18. J. Kenneth Wickiser, Kevin J. O'Donovan, Michael Washington, et. al., "Engineered Pathogens and Unnatural Biological Weapons: The Future Threat of Synthetic Biology," Combating Terrorism Center Sentinel at West Point, August 2020, https://ctc.westpoint.edu/engineered-pathogens-and-unnatural-biological-weapons-the-future-threat-of-synthetic-biology/.
19. Lois M. Davis and Jeanne S. Ringel, "Public Health Preparedness for Chemical, Biological, Radiological, and Nuclear Weapons," originally published in *WMD Terrorism: Science and Policy Choices*, RAND Corporation, 2009, https://www.rand.org/pubs/reprints/RP1415.html.
20. For more, see "Critical Infrastructure Sectors," US Cybersecurity and Infrastructure Security Agency, n.d., https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors, accessed May 2023.
21. For more on the impact of emerging technologies related to WMD, see *Future Implications of Emerging Disruptive Technologies on Weapons of Mass Destruction*, Arizona State University Threatcasting Lab, September 2022, https://cyber.army.mil/Portals/3/Documents/Threatcasting/wmds/Threatcasting_WMDs.pdf.
22. "Disinformation Roulette: The Kremlin's Year of Lies to Justify an Unjustifiable War," US Department of State, Global Engagement Center, February 23, 2023, https://www.state.gov/disarming-disinformation/disinformation-roulette-the-kremlins-year-of-lies-to-justify-an-unjustifiable-war/.
23. Davey Alba, "Russia Has Been Laying Groundwork Online for a 'False Flag' Operation, Misinformation Researchers Say," *New York Times,* February 19, 2022, https://www.nytimes.com/2022/02/19/business/russia-has-been-laying-groundwork-online-for-a-false-flag-operation-misinformation-researchers-say.html.
24. For more, see *Washington Post* Editorial Board, "How Russia Turned America's Helping Hand to Ukraine into a Vast Lie," *Washington Post*, March 29, 2023, https://www.washingtonpost.com/opinions/2023/03/29/russia-disinformation-ukraine-bio-labs/; Kenneth D. Ward, "Syria, Russia, and the Global Chemical Weapons Crisis," Arms Control Association, September 2021, https://www.armscontrol.org/act/2021-09/features/syria-russia-global-chemical-weapons-crisis; Filippa Lentzos and Jez Littlewood, "How Russia Worked to Undermine UN Bioweapons Investigations," *Bulletin of the Atomic Scientists*, December 11, 2020, https://thebulletin.org/2020/12/how-russia-worked-to-undermine-un-bioweapons-investigations/.
25. "Statement by Ms. Dr. Kateryna Bila—Representative of Ukraine to the 27th Session of the Conference of States Parties to the Chemical Weapons Convention," Organization for the Prohibition of Chemical Weapons, 2022, https://www.opcw.org/sites/default/files/documents/2022/11/National%20Statement_Ukraine_Agenda%20item%209%28d%29-rev%20pdf.pdf.
26. NATO's Chemical, Biological, Radiological, and Nuclear (CBRN) Defense Policy, NATO, last updated July 2022, https://www.nato.int/cps/en/natohq/official_texts_197768.htm.
27. Diego Ruiz Palmer, "The Framework Nations Concept and NATO: Game-Changer for a New Strategic Era or Missing Opportunity," NATO Defense College, July 2016, https://www.ndc.nato.int/news/news.php?icode=965.
28. AVM Sean Corbett, CB MBE and James Danoy, "Beyond NOFORN: Solutions for Increased Intelligence Sharing among Allies," Atlantic Council, October 31, 2022, https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/beyond-noforn-solutions-for-increased-intelligence-sharing-among-allies/.
29. "Euro-Atlantic Disaster Response Coordination Centre," NATO, September 2021, https://www.nato.int/cps/en/natohq/topics_52057.htm.
30. For more on strategic foresight methodology, see "Tools for Futures Thinking and Foresight across UK Government," UK Government Office for Science; or Rhydderch, "Scenario-Building: The 2x2 Matrix Technique."

Atlantic Council

Board of Directors

CHAIRMAN
*John F.W. Rogers

EXECUTIVE CHAIRMAN EMERITUS
*James L. Jones

PRESIDENT AND CEO
*Frederick Kempe

EXECUTIVE VICE CHAIRS
*Adrienne Arsht
*Stephen J. Hadley

VICE CHAIRS
*Robert J. Abernethy
*Alexander V. Mirtchev

TREASURER
*George Lund

DIRECTORS
Stephen Achilles
Gina F. Adams
Timothy D. Adams
*Michael Andersson
Barbara Barrett
Colleen Bell
Sarah E. Beshar
Stephen Biegun
Linden P. Blue
Adam Boehler
John Bonsell
Philip M. Breedlove
Richard R. Burt
*Teresa Carlson
*James E. Cartwright
John E. Chapoton
Ahmed Charai
Melanie Chen
Michael Chertoff
*George Chopivsky
Wesley K. Clark
*Helima Croft
*Ankit N. Desai
Dario Deste
Lawrence Di Rita
*Paula J. Dobriansky
Joseph F. Dunford, Jr.
Richard Edelman
Thomas J. Egan, Jr.
Stuart E. Eizenstat
Mark T. Esper
*Michael Fisch
Alan H. Fleischmann
Jendayi E. Frazer
Meg Gentle
Thomas H. Glocer
John B. Goodman
*Sherri W. Goodman
Marcel Grisnigt
Jarosław Grzesiak
Murathan Günal
Michael V. Hayden
Tim Holt
*Karl V. Hopkins
Kay Bailey Hutchison
Ian Ihnatowycz
Mark Isakowitz
Wolfgang F. Ischinger
Deborah Lee James
*Joia M. Johnson
*Safi Kalo
Andre Kelleners
Brian L. Kelly
Henry A. Kissinger
John E. Klein
*C. Jeffrey Knittel
Joseph Konzelmann
Keith Krach
Franklin D. Kramer
Laura Lane
Almar Latour
Yann Le Pallec
Jan M. Lodal
Douglas Lute
Jane Holl Lute
William J. Lynn
Mark Machin
Marco Margheri
Michael Margolis
Chris Marlin
William Marron
Gerardo Mato
Erin McGrain
John M. McHugh
*Judith A. Miller
Dariusz Mioduski
*Richard Morningstar
Georgette Mosbacher
Majida Mourad
Virginia A. Mulberger
Mary Claire Murphy
Julia Nesheiwat
Edward J. Newberry
Franco Nuschese
Joseph S. Nye
Ahmet M. Ören
Sally A. Painter
Ana I. Palacio
*Kostas Pantazopoulos
Alan Pellegrini
David H. Petraeus
*Lisa Pollina
Daniel B. Poneman
*Dina H. Powell McCormick
Michael Punke
Ashraf Qazi
Thomas J. Ridge
Gary Rieschel
Michael J. Rogers
Charles O. Rossotti
Harry Sachinis
C. Michael Scaparrotti
Ivan A. Schlager
Rajiv Shah
Gregg Sherrill
Jeff Shockey
Ali Jehangir Siddiqui
Kris Singh
Varun Sivaram
Walter Slocombe
Christopher Smith
Clifford M. Sobel
Michael S. Steele
Richard J.A. Steele
Mary Streett
Nader Tavakoli
*Gil Tenzer
*Frances F. Townsend
Clyde C. Tuggle
Melanne Verveer
Charles F. Wald
Michael F. Walsh
Ronald Weiser
*Al Williams
Ben Wilson
Maciej Witucki
Neal S. Wolin
*Jenny Wood
Guang Yang
Mary C. Yates
Dov S. Zakheim

HONORARY DIRECTORS
James A. Baker, III
Robert M. Gates
James N. Mattis
Michael G. Mullen
Leon E. Panetta
William J. Perry
Condoleezza Rice
Horst Teltschik
William H. Webster

**Executive Committee Members*

List as of July 5, 2023

The Atlantic Council is a nonpartisan organization that promotes constructive US leadership and engagement in international affairs based on the central role of the Atlantic community in meeting today's global challenges.

Atlantic Council

1030 15th Street, NW, 12th Floor,
Washington, DC 20005

(202) 463-7226, www.AtlanticCouncil.org