# A Compendium of Research on Nonproliferation and Global Security

September 2024

This page is left intetionally blank

# CRDF Global Compendium on Nonproliferation Research: A Brief Overview

## Introduction

CRDF Global, in partnership with and funded by the U.S. Department of State's Export Control and Border Security (EXBS) Program, has executed a grant program to support organizations and individuals in developing research, analysis, and compliance tools related to export controls, sanctions, and other international nonproliferation mechanisms. This initiative is part of a broader effort to address key proliferation challenges, particularly those associated with nation-states that advance Weapons of Mass Destruction (WMDs) or support terrorist activities.

## Project Scope and Focus

The funded projects encompassed a variety of outputs, including research papers, policy papers, compliance protocols, training modules, and analytical tools, all designed to enhance the implementation of nonproliferation measures. Each project provided practical insights and tools that improved stakeholders' ability to mitigate proliferation risks, promote policy reform, and strengthen due diligence and enforcement procedures. Grantees were encouraged to engage in public outreach through events such as workshops, publications, or roundtables to disseminate their findings.

## Funding

The grants supported an eight-month project cycle for each recipient, enabling them to conduct comprehensive research and develop practical tools that contribute to addressing proliferation risks such as unauthorized technology transfers, illicit arms trades, and sanctions evasion.

## Research Highlights

1. Civil Council on Defense and Security (CCDS) - Georgia: CCDS's project supported Georgia's compliance with U.S. and EU sanctions against Russia. The research produced an evidence-based policy report assessing Georgia's adherence to sanctions and included a

workshop for media professionals to enhance understanding of the sanctions' impact

2. Jawaharlal Nehru University (JNU): Dr. Anamika & Dr Varun Gulati: Dr. Anamika and Dr. Gulati's research explored high-risk WMD proliferation scenarios, identifying risks for companies and institutions, and outlining strategies for risk recognition and mitigation. The study involved primary data collection through expert interviews and analysis of government policies on WMDs and dual-use technologies.

3. Observer Research Foundation (ORF): ORF's study focused on identifying nuclear terrorism threats specific to India, ranking them by their potential impact, and exploring countermeasures at both the national and multilateral levels. The resulting policy report provides an overview of India's nuclear security landscape and offers specific recommendations to mitigate identified threats.

## Conclusion

This compendium serves as a valuable resource for policymakers, practitioners, and other stakeholders engaged in nonproliferation efforts. By showcasing the diverse range of research and practical outputs from these projects, CRDF Global and EXBS aim to promote innovative approaches to addressing proliferation risks and strengthening global nonproliferation norms.

## Disclosure

The opinions and perspectives presented in the research outputs are those of the respective researchers and do not necessarily reflect the views of the U.S. Department of State, CRDF Global, or the Strategic Trade Research Institute.

# Table of Contents

International Sanctions on Russia: New Challenges
from the Georgian Perspective.....6

Counterproliferation of Weapons of Mass Destruction:
Strategies against Terrorism through a Questionnaire-Based Study.....32

In Pursuit of Nuclear Security: Reducing India's Risks to
Nuclear Terrorism.....57

# International Sanctions on Russia: New Challenges from the Georgian Perspective

Tamar Pataraia and Ivane Kechakmadze[1]

## Introduction

The imposition of sanctions by the United States and an international coalition of more than 40 allies and partners, including the European Union and G7 nations, in response to Russia's unprovoked invasion of Ukraine in February 2022, marked a significant diplomatic and economic response to Russia's aggression. These sanctions were strategically aimed at limiting Russia's access to capital, technologies, and other resources essential for its aggressive endeavors, specifically targeted critical revenue-generating sectors, financial institutions, the military supply chains, as well as individuals and entities worldwide, defense procurement networks, including international suppliers supporting Russia's military-industrial complex for undermining the peace, security, stability, sovereignty, or territorial integrity of Ukraine. In addition, the U.S. imposed visa restrictions for Russian government officials, their family members, Russian and Belarusian military officials, and others.[2]

Despite Georgia's historical alignment with European Union sanctions in response to Russian annexation of Crimea and Occupation of Eastern Ukrainian territories in 2014, the Georgian government made a deliberate choice not to formally join the coalition in 2022,

1 Dr. Tamara Pataraia is an Associate Professor at the University of Georgia, where she teaches in the Department of Politics and International Relations, her courses focus on global security and nuclear nonproliferation. Mr. Ivane Kechakmadze is an Assistant Professor at Ilia State University since 2020, where he lectures extensively in statistics and SPSS across multiple institutions. He also works atIvane Javakhishvili State University, Caucasus University, and Alma Mater University.

2 United States Department of State, "Ukraine and Russia Sanctions," Last modified July 2, 2024. <https://www.state.gov/ukraine-and-russia-sanctions/>.

citing economic concerns and fears of further Russian aggression. However, subsequent statements by political leaders and high-ranking officials from various agencies, including the Georgian National Bank, demonstrate that despite Georgia not joining the sanctions, it cannot become a country whose customs territory or financial institutions could be used to evade them. Georgia's strategic position and robust transportation infrastructure have rendered it susceptible to Russia's attempts to circumvent sanctions, raising significant security concerns given Georgia's turbulent history of conflict with Russia.

This policy paper examines the multifaceted challenges and threats confronting Georgia following the imposition of sanctions, underscoring the intricate balance the country must strike between its international obligations and its domestic security imperatives.

An analysis of Georgia's foreign trade data reveals a notable increase in trade volumes with specific products to countries emerges, indicating active efforts by Russia to evade sanctions. This study explores emerging challenges for Georgia arising from sanctions policy against Russia and on the basis of the statistical data analysis underscores the urgent need for Georgia to enhance cooperation with coalition members and bolster compliance with sanctions policies.

In conclusion, the paper proposes a series of measures for Georgia to mitigate threats, including the establishment of a comprehensive trade control policy and the enhancement of administrative capacities to assist coalition efforts in weakening Russia's military capabilities. As Georgia navigates the complex geopolitical landscape shaped by ongoing conflicts and sanctions regimes, it is imperative for the country to prioritize its security interests while upholding its commitments to international partners.

## Sanctions against Russia and Russia's Efforts to Re-Establish International Trade with the Help of Third Countries

Immediately after Russia's large-scale, unjust, and unprovoked aggression against Ukraine on February 24, 2022, the United States, United Kingdom, more than 40 members of the European Union, and several G7 and other nations, formed a coalition and introduced sanctions against Russia. This was preceded by the first waves of the EU and U.S. sanctions against Russia in 2014 triggered by the Russian annexation of Crimea and occupation of Eastern Ukrainian territories.[3]

3 United States Department of State. "Ukraine and Russia Sanctions." Last modified July 2, 2024,

During 2022-2023, the U.S. and EU reaffirmed their dedication to imposing sanction measures by introducing several packages of sanctions against Russia aimed to maximize the economic toll on Russia while minimizing adverse effects on the allied states, partners in the coalition and the global economy at large. One of the primary goals for the coalition members is to use innovative and sweeping sanctions and stringent export control measures to deprive Russia of the financial resources required to sustain its invasion and exert power by weakening its military-industrial complex.[4] On February 24, 2023, U.S. Treasury Secretary Janet Yellen affirmed that the sanctions implemented by the U.S., the EU, and their G7 allies had proved effective in both the short-term and long-term. She emphasized that the "actions today show that we will stand with Ukraine for as long as it takes."[5]

It is not surprising that media reports from 2023 show surges in trade for some of Russia's neighbours and allies which are stepped in to provide Russia with many of the products that Western countries tried to cut off as punishment for Moscow's invasion of Ukraine.[6] Besides seeking alternative revenue sources, Russia has remarkably increased its exports to countries such as China, Brazil, India, Turkiye, and others. Some estimates suggest that there are hundreds of instances of individuals from these third countries purchasing vessels to set up new non-Western frameworks of trading with Russia. Such schemes help Russia get around legal restrictions set by the West.[7] In addition to the so called "shadow fleet support," experts suggest that the rise in oil prices by nearly 60% since their March 2023 lows is providing some welcome economic relief to Russia and much needed revenue for the government, thanks to oil and gas taxes.[8]

---

<https://www.state.gov/ukraine-and-russia-sanctions/>; Council of the European Union. "Timeline - EU Sanctions Against Russia," Accessed July 3, 2024. <https://www.consilium.europa.eu/en/policies/sanctions-against-russia/timeline-sanctions-against-russia/>.

4 Adeyemo, Wally, "America's New Sanctions Strategy: How Washington Can Stop the Russian War Machine and Strengthen the International Economic Order," Foreign Affairs, Accessed November 26, 2023, <https://www.foreignaffairs.com/print/node/1129701>.

5 United States Department of State, "Targeting Key Sectors, Evasion Efforts, and Military Supplies, Treasury Expands and Intensifies Sanctions Against Russia," February 24, 2023, https://home.treasury.gov/news/press-releases/jy1296, Accessed 11/26/2023,

6 Swanson, Ana, "Russia Sidesteps Western Punishments, With Help From Friends." The New York Times, January 31, 2023, Accessed November 26, 2023, https://www.nytimes.com/2023/01/31/business/economy/russia-sanctions-trade-china-Turkiye.html?smid=nytcore-ios-share&referringSource=articleShare&fbclid=IwAR1U.S.UzqdePi5q_boUY9s_aVsqZ8UEN_oUBYOIsnAnhgYnpCtO-SHc1xQjE .

7 Swanson, Ana, "Russia Sidesteps Western Punishments, With Help From Friends," The New York Times. January 31, 2023, Accessed November 26, 2023, https://www.nytimes.com/2023/01/31/business/economy/russia-sanctions-trade-china-Turkiye.html?smid=nytcore-ios-share&referringSource=articleShare&fbclid=IwAR1U.S.UzqdePi5q_boUY9s_aVsqZ8UEN_oUBYOIsnAnhgYnpCtO-SHc1xQjE.

8 Briancon, Pierre, "Russian War Economy Is Overheating on a Powder Keg." Reuters. October 25, 2023. https://www.reuters.com/breakingviews/russian-war-economy-is-overheating-powder-keg-2023-10-25.

Consequently, while sanctions and export control restrictions imposed by the United States and the European Union weakened Russia's economy and military industrial complex to a certain extent, they did not render it entirely powerless. In 2022, instead of the previously anticipated double-digit decline, the Russian GDP fell by only about 3%. In October 2023, the International Monetary Fund (IMF) raised its outlook for Russian GDP growth in 2023, this time to 2.2% from the 1.5% growth it was predicting in July.[9] Furthermore, the Russian currency stabilized following an initial slide of 30% since its 2023 January high. Overall, based on the data from 2022 and 2023, observers suggest that Russia managed this with support from third countries that are not coalition members. Another reason for the surprise results is the increased spending of the Russian government following the long tradition of fiscal restraint.[10]

Overall, the efficiency of sanctions imposed by the U.S., the EU, and their allies has been compromised by instances of evasion and circumvention. Multiple sources corroborate that economic operators linked to Russia, as well as entities from third countries, have devised numerous strategies to evade and circumvent sanctions.[11]

As of 2023, the strategic focus for the U.S. and the EU has shifted towards targeting individuals and entities worldwide, registered and operating in third countries, while emphasizing the rigorous enforcement of the established sanctions.

The present study identifies and examines the challenges and threats faced by Georgia following the imposition of sanctions against Russia in February 2022. The analysis emphasizes the significance of these challenges, highlights the complexities Georgia encounters due to its reluctance to join the sanctions coalition while also requiring to adhere fully to the sanctions.

The scrutiny of Georgia's foreign trade data corroborates the hypothesis that the significant surge in trade volumes involving specific products and countries serves as compelling evidence of Russia's active efforts to circumvent sanctions.

---

Accessed November 28, 2023.

9 IMF. Russian Federation At a Glance, https://www.imf.org/en/Countries/RU.S., Accessed November 27, 2023.

10 Briancon, Pierre. "(October 25, 2023) Russian War Economy Is Overheating on a Powder Keg." Reuters. October 25, 2023, https://www.reuters.com/breakingviews/russian-war-economy-is-overheating-powder-keg-2023-10-25, Accessed November 28, 2023.

11 Detecting and Preventing Sanctions Evasion and Circumvention in Trade, Practical Guidance for Economic Operators, Sanctions Team, MFA of Finland, Customs, Control Department, https://vihjeet.tulli.fi/ . Accessed December 04, 2023.

The research methodology employed in this study involves various approaches. It includes a review of academic studies focused on international sanctions, an evaluation of political developments within Georgia, and statistical data analysis. Notably, this analysis integrates data obtained from state agencies specifically solicited for the purpose of this research.

The authors of the paper propose that Georgia's best interests are served by enhancing collaboration with coalition members, particularly with the U.S. and EU, and ensuring robust compliance with sanctions. Moreover, considering the prevailing circumstances, it looks imperative for Georgia to establish a lasting policy framework concerning international trade controls that aligns with the sanctions policies of the U.S. and the EU. Additionally, Georgia needs to prioritize enhancing its administrative capabilities to effectively assist partner states within the international coalition, thereby contributing to the efficient execution of sanctions aimed at further weakening the capabilities of the Russian military in the conflict with Ukraine.

## Georgia's Policies and Challenges Related to Russia Sanctions

Georgia's strategic location, transport potential, and transit infrastructure have made it an appealing hub for Russia's foreign trade. However, Russia represents the most pressing threat to Georgia's stability. Since the early 1990s, Georgia has faced persistent attempts from Russia to occupy its territories. In 2008, Georgia fell victim to Russian aggression, resulting in the occupation of approximately 20% of its territory. This resulted in the establishment of two Russian military bases in Abkhazia and South Ossetia. Since then, Georgia has severed diplomatic ties with Russia, departed from the Russia-led CIS alliance, and rejected participation in the Russia-led Eurasia Economic Union. However, Georgia has continued trade relations with Russia.

To fortify its security as a small post-Soviet state bordering Russia, Georgia has opted to strengthen its democratic foundations, foster a stable political system, enhance security and defence capabilities through closer ties with NATO and the EU, deepen international cooperation, and secure robust support from the U.S. and the EU. These intentions are firmly rooted in Article 78 of the Georgian Constitution which mandates constitutional bodies to exhaust all avenues toward Georgia's complete integration into the EU and NATO.[12]

In this context, Georgia's primary interest is to diminish Russia's military capabilities and

12 Constitution of Georgia. Legislative Herald of Georgia, Accessed July 11, 2024, https://matsne.gov.ge/en/document/view/30346?publication=36.

international influence to safeguard its national security. To achieve this objective, unwavering solidarity with Ukraine is crucial, actively supporting its resistance against Russia's unjust aggression. If Georgia remains committed to all international obligations and aligns itself with the collective efforts led by the U.S., the EU, and other members of the sanctions coalition, it can substantially contribute to implementing stringent measures imposed by them, including actions targeting third party entities supporting Russia's war in Ukraine.

Against this backdrop, following the decision by the U.S. and the EU to impose sanctions against Russia, the Georgian government and prime minister, contrary to all expectations, stated that Georgia was not joining the sanctions, arguing that such a step would become a burden on the country's economy and its citizens. The prime minister stated that as Georgia's economy was heavily dependent on Russia, the government could not deny its citizens the revenues that they received from Russia, which over eight years amounted to U.S.D $12 billion in transfers. Ruling party representatives went further, saying that Georgia's joining the sanctions would damage Georgia-Russia relations and would draw Georgia into the conflict with Russia.[13]

However, later developments and statements by various agencies, such as the Georgian National Bank, the Revenues Service and the Ministry of Finance and Economy demonstrated that in spite of Georgia not joining the sanctions, it could not become a country whose Customs territory and/or financial institutions could be used to evade sanctions.[14] However, abstaining from joining current U.S. and EU sanctions poses additional challenges for Georgia, potentially complicating its aspirations to join the European Union and NATO in the near future. Against the backdrop of the volatile situation stemming from the Ukrainian conflict, Georgia, akin to Ukraine and Moldova, seized an opportune moment and applied for EU membership on March 3, 2022. The European Council decided on granting Georgia the status of EU Membership Candidate on December 14, 2023.

And yet, the Georgian government's decision not to join U.S. and EU sanctions raises the additional risk of Georgia facing potential U.S. secondary sanctions. The analysis presented in the current paper suggests that Russia is expected to escalate tensions in the relationship between Georgia and its partners, capitalizing on Georgia's ambiguous stance and potentially exploiting its territory and economic space to avoid sanctions. Moreover, none of Georgia's neighbouring countries, which share a land border with it, have joined the sanctions against

13 "Georgian PM: Government Imposing Sanctions on Russia would "Destroy our Economy." May 24, 2022, Agenda.ge. https://agenda.ge/en/news/2023/2026, Accessed 12.28.2023.

14 Revenue Service Affirms Adherence to Russia Sanctions," June 26, 2023, https://civil.ge/archives/549672.

Russia, creating the potential for Russia to pose new and diverse future threats.

Georgian media has been extensively monitoring the overall situation. Georgian researchers and analysts believe that under the existing circumstances, Georgia should be prepared to tackle the ever-increasing challenges it faces. Aligning with EU decisions and complying with sanctions is crucial, as the support from its Western strategic partners serves as a significant guarantee for Georgia to protect its sovereignty and territorial integrity. Without this support, Georgia could find itself confronting Russia independently. It is undeniable that Russia will never align with Georgia's state interests, considering it has already occupied part of its territory and continues to use its influence levers in its own favour.

## Emerging Challenges for George Arising from its Ambiguous Sanction Policy against Russia

### *Financial Institutions and Sanctions*

Georgian officials confirm that the Georgian financial sector is a part of the global finance system, meaning that it has the obligation to join international banking sanctions. Shortly after the introduction of sanctions on February 27, 2022, the National Bank of Georgia stated that it would operate in accordance with the standards defined by international resolutions and that it would not and could not contribute to the circumvention of these sanctions as the Georgian banking system was part of the global system and, thus, automatically joined to the sanctions.

The National Bank also stated that as of February 26, 2022, under its instruction, all Georgian financial institutions fully complied with EU and U.S.-introduced financial sanctions. In order to work out a uniform approach to the compliance with the sanctions and introduction of relevant controls, the president of the National Bank issued Decree №208/04 on August 4, 2023, "Procedures of enforcing sanctions regimes by entities under the supervision of the National Bank of Georgia."[15]

Until September 2023, it was believed that the Georgian banking sector unconditionally implemented all sanctions imposed by the U.S. and EU, including strictly controlling money

15 Order of the President of the National Bank of Georgia. "Procedures of enforcing sanctions regimes by entities under the supervision of the National Bank of Georgia," Document # 208/04, August 4, 2023, https://www.matsne.gov.ge/ka/document/view/5888234?publication=0, Accessed 4 December 2023.

transfers by Russian citizens, cutting sanctioned banks off from the SWIFT system, and implementing all restrictions set for the Russian banking system.[16] However, on September 14, 2023, the U.S. Department of Treasury's Office of Foreign Assets Control (OFAC) updated its designation list and named more than 150 new companies and individuals, including many in Turkiye, the United Arab Emirates, and Georgia. This was the first time a Georgian individual and/or entity was included in the list of U.S. sanctioned persons.[17]

The person named on the new list is Georgia's former prosecutor general, the person linked to the ruling party, Otar Partskhaladze, who in 2013 was forced to resign from a brief term as prosecutor general after it transpired that he had been convicted in Germany. (Political opponents of ruling party claim Partskhaladze was convicted of robbery in Germany in 2001. Partskhaladze himself has denied a robbery conviction but said he was convicted in German court following allegations of failing to obey a police officer).[18]

According to information issued by the U.S. Treasury Department in September 2023, Partskhaladze, after his resignation from the post, acquired Russian citizenship with the help of a Russian FSB officer.[19] Partskhaladze, who has reportedly personally profited from his Federal Security Service of the Russian Federation (FSB) connections, has been sanctioned for spreading malicious influence in Georgia for the benefit of Russia.[20] This revelation provoked widespread public concern and criticism, prompting questions about the potential repercussions for Georgia's future relations with the.West.

At first, as was expected, the National Bank stated that the Georgian financial sector operated in full compliance with the requirements of the sanctions regimes and restricted Partskhaladze

16 IDFI. "Georgia's Implementation of the international sanctions imposed against Russia". IDFI . November 07, 2022, Accessed: 4 Decmber 2023, tps://idfi.ge/ge/georgias_implementation_of_the_international_sanctions_imposed_against_russia.

17 Office of Foriegn Assets Control, United States Department of Treasury, "Russia-Related Designations, Designations Updates, and Designations Removals; Issuance of Russia-Related General License"s, September 14, 2023, Accessed: 4 December 2023, https://ofac.treasury.gov/recent-actions/20230914?fbclid=IwAR0U7LNWeB2Uym4so-KEbth1ryzDeg4Ggmd5j39Sk3RAmDMIB01xUAQo9u0.

18 Radio Free Europe/Radio Liberty, "Georgia: Fresh Protests Over TV Station Closure," January 10, 2014, https://www.rferl.org/a/georgia/25217011.html; Gvineria, Giorgi, "Georgia's Discredited Chief Prosecutor Resigns, but Anti-UNM Prosecution Cases Multiply," The Jamestown Foundation, https://jamestown.org/program/georgias-discredited-chief-prosecutor-resigns-but-anti-unm-prosecution-cases-multiply/.

19 United States Department of Treasury, "U.S. Department of Treasury With Wide-Ranging New Sanctions, Treasury Targets Russian Military-Linked Elites and Industrial Base," Press Releases, September 14, 2023. Accessed: 4 December 2023.

20 U.S. Department of Treasury With Wide-Ranging New Sanctions, Treasury Targets Russian Military-Linked Elites and Industrial Base, Press Releases, U.S. Department of Treasury, September 14, 2023, Accessed: 4 December 2023.

from accessing his bank assets and conducting financial transactions.[21] However, later, on September 19, the acting president of the National Bank drafted and enforced an amendment which reiterated that the bank fully complied with the sanctions regimes, but the National Bank, guided by the Constitution of Georgia and the presumption of innocence, believed that international sanctions could not be applied to a Georgian citizen unless the individual was found guilty in a court of law. The decision allowed Partskhaladze to sign off all his real estate and movable property to his family members in a day.[22]

Georgian experts and politicians perceive this action as a clear indication that the bank was being influenced by the ruling political party leadership and may violate the principle of supremacy of international law in the future. There is a prevailing belief that this influence is geared towards providing protection to party members from potential future sanctions in the long term.

Later developments demonstrated that the decision was not approved unanimously in the bank, as three of the bank's vice presidents, who also served as members of the Bank Council, resigned the following day. In addition, all main commercial banks, among them the largest TBC and the Bank of Georgia, reaffirmed their commitment to comply with international sanctions initiated by the EU, UK and U.S.

Overall, the state's ambiguous policy put the national financial system at risk of sanctions and undermined the independence of the National Bank of Georgia. The development could have potentially jeopardized the sustainability and reliability of Georgia's financial system if it were not for the decisive actions of key stakeholders, particularly major banks operating in Georgia. By steadfastly upholding their unequivocal position and fulfilling their obligations to fully comply with sanctions imposed against Russia, these major banks have helped safeguard the integrity of Georgia's financial infrastructure.

## Changes in Customs Control Regulations and Dynamics of Foreign Trade

The confusing policy towards sanctions against Russia and the repercussions of the Ukraine

21 Civil.ge, "NBG Blocks Accounts of Sanctioned Partskhaladze," Civil.ge., September 18, 2023. Accessed 4 December 2023, https://civil.ge/archives/559636.

22 Civil.ge, "National Bank Makes U-Turn, Shields Sanctioned Partskaladze." Civil.ge., September 19, 2023, Accessed on December 4, 2023, https://civil.ge/archives/559915.

conflict resulted in increased immigration, escalating prices, and disruptions in the supply caused by the surge in foreign trade volume in Georgia.[23]

Customs officials acknowledge that the administration of the increased flow of imports, exports, transit, and re-export of military and dual-use goods across Georgian borders present heightened challenges.[24] It is important to highlight that Georgia has regulated the trade of strategic goods in accordance with EU regulations since 2013, mandating special permits/ licenses issued under the shared responsibility of the Defence Ministry and the Revenues Service. Following the conflict in Ukraine, the protocols for obtaining these permits have been significantly tightened, subjecting the issuance process to intensified scrutiny and rigorous evaluation. Nevertheless, the European Commission has advised a thorough review of Georgia's existing export control laws and regulatory norms to update and harmonize them with the EU's current legislation.[25] In response, officials state that before relevant changes are made in the law, the Georgian agencies carry out special customs controls over all goods on the list compiled in the U.S. and EU sanctions policies.[26]

One of the primary findings highlighted in the Georgia 2023 Report, prepared by the European Commission in October 2023, reveals that Georgia's export control system (created in 2013) and the control list of military and dual-use goods and strategic products needs to be updated. Georgian authorities acknowledge that the overall system inadequately addresses issues related to technical assistance and brokerage services.[27] Besides, from Georgia's perspective, it is extremely challenging to identify companies registered in Georgia but engaged in business abroad which might seek to bypass sanctions against Russia. This challenge specifically arises because official organizations lack information about the business activities of these entities in foreign countries until they submit documents to acquire authorization for transporting military and dual-purpose cargo across Georgia.[28]

According to the statement made by the finance minister in parliament on March 23,2023, immediately after the sanctions were introduced, the Customs Risk Management Agency operating under the Customs Department of the Revenue Service set up a working group to

23 The Bank of Georgia, Galt and Taggart Research, January 2023.

24 Personal Interviews with anonymous customs officer, CCDS, November 2023.

25 Georgia 2023 Report, Commission Staff Working Document SDW (2023) 697 final Brussels 8.11.2023, Available at: https://neighbourhood-enlargement.ec.europa.eu/system/files/2023-11/SWD_2023_697%20Georgia%20report.pdf,

26 Anonymous official. Private interview with the authors. November 14, 2023.

27 Georgia 2023 Report Brussels 8.11.2023, Commission Staff Working Document SDW (2023) 697 final 2023 Communication on EU Enlargement Policy.

28 Personal Interviews with anonymous customs officer, CCDS, November 2023.

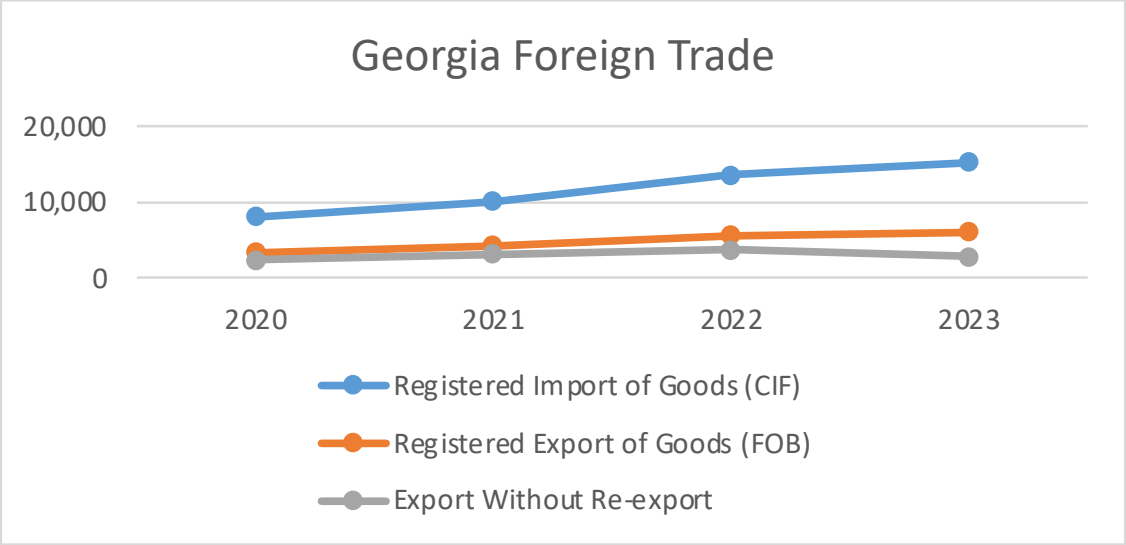
establish centralized control over the enforcement of sanctions. Sixteen risk profiles were created, which would serve as a basis for identifying and controlling the movement, transit, export, or re-export of banned goods on or through Georgian customs territory, when the sender or recipient of the goods is a sanctioned individual or company.[29]

Furthermore, to enforce the sanctions properly, the Finance Ministry of Georgia requested technical assistance from Georgia's strategic partners on multiple occasions. Georgia was given access to the international sanctions training platform DOLFIN; two staff members of the Customs Department acquired a certificate as sanctions enforcement experts. All data concerning Georgia's foreign trade, encompassing both imports and exports, is publicly accessible and routinely published on the official web page. Additionally, this information can be obtained by reaching out to the national Statistics Office of Georgia or the Revenues Service.[30]

Evidence to this is the official data provided by the Revenues Office of the Georgian Finance Ministry and the Georgia Office of Statistics, which, to some extent, reflect Georgia's policies and responses to the sanctions against Russia. These data show that in 2022 Georgia imported the record $13.5 bn dollar-worth goods from abroad, 33 per cent more than during the previous year. Data for the 2023 suggests that this amount is higher in 2023 and reaches about $15.5 bn.

29 Interpressnews,March 23.2023. Accessed: December 4, 2023, Available at: https://www.interpressnews.ge/ka/article/749623-lasha-xucishvili-migebulia-sankcirebuli-sakonlis-ukan-gabrunebis-1020-da-sakonlis-eksportis-an-reeksportis-ganzraxvis-taobaze-piris-momartvaze-uaris-tkmis-600-ze-meti-sabazho-gadacqvetileba/?fbclid=IwAR3W1LukLZm%CB%99g8XoTfQWe67bIrxk03sPW2PUqILTVEq-wWsUPpYXAqzHIb-c.

30 National Statistics Office of Georgia, External Merchandise Trade, Accessed on 07 February 2024, Available at: https://www.geostat.ge/en/modules/categories/765/external-merchandise-trade.




**National Statistics Office of Georgia**[31]

There has been a noticeable and significant increase in trade between Georgia and Russia since 2022, accompanied by a considerable influx of Russian citizens arriving in Georgia and choosing to stay. Migration from Russia boosted real estate market and investments; FDI more than doubled. Along with the growth of imports, the number of Russian companies being registered in Georgia has been rising, which is undoubtedly linked to the Russia-Ukraine war.[32] However, these trends might be reversed amid heightened geopolitical tensions. Data from 2023 indicates such a shift, with the number of immigrants from Russia already declining. Specifically, in the third quarter of 2023, statistics show 14,000 more Russians leaving the country than entering it.[33]

As the international sanctions regime continues to operate against Russia, more time is required to explore the exact impact of Russian aggression against Ukraine on Georgia and, consequently, international sanctions on Georgia's policies, economy, and possible responses. Besides, Georgia's vulnerability and insecurity do not allow it to ignore the importance of compliance with U.S. and EU decisions.

The analysis (provided below) of import, export, re-export, and transit figures across Georgia

31 Ibid.

32 Transparency International Georgia, "Georgia's Economic Dependence on Russia: Impact of the Russia-Ukraine War," Available at: https://transparency.ge/en/post/georgias-economic-dependence-russia-impact-russia-ukraine-war-0.

33 Georgian Ministry of Internal Affairs, Piblic Information, Available at: https://info.police.ge/page?id=757&parent_id=94.

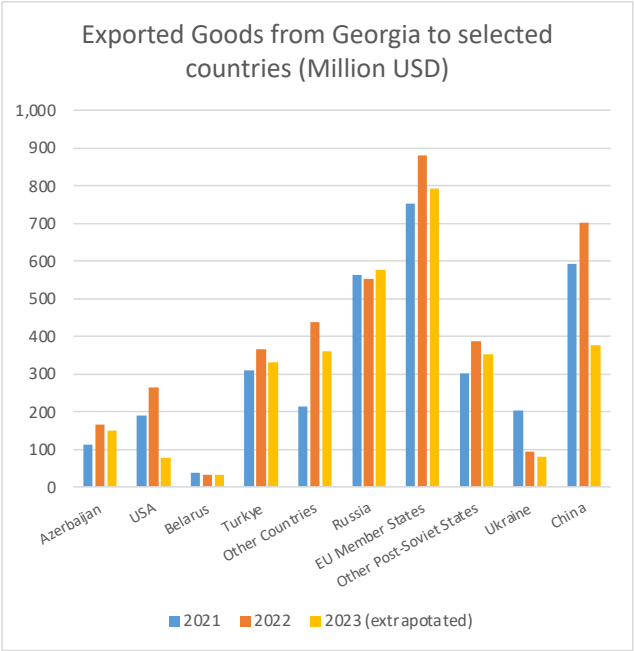
could provide a general understanding whether compliance with international sanctions could help Georgia find more security and achieve economic stability in the future.

## Georgia's Imports and Exports: How Significant is Trade with Russia in Georgia's Foreign Trade?

Based on official data from 2021-2022 and extrapolations for the first eight months of 2023, it is evident that Russia emerged as Georgia's second-largest importer for the period spanning 2022-2023, following Turkey (followed by China).

**Data from the Customs Department of Georgia's Revenues Service, 25.08.2023**

According to data from the Statistics Office, from 2022 to 2023, Georgia saw an increased dependence on Russian imports, primarily in car fuels such as oil and petrol (tripling), fuel gases (doubling), wheat and rye flour (increasing 1.3 times), and coal and coal-based solid fuel (rising 20 times). Despite this, imports from EU countries still constitute the largest share, with volumes significantly surpassing those from Turkey or Russia during the same period.




**Data from the Customs Department of Georgia's Revenues Service, 25.08.2023**

Interestingly, Georgia's total export indicators fell in 2021-2023, with only Russia gaining an upward trend.[34] In the past, EU countries led the list of Georgia's export destinations, followed by China, while Russia and Turkiye jointly occupied the third and fourth positions on that list. Extrapolation of the data for the first eight months of 2023 suggests that Russia will become second largest trade partner for Georgia after the EU. The largest categories of goods exported to Russia are ferroalloys (doubled), natural wines (1.5 more), cars (10 times more), mineral and spring water (1.2 times more), and spirits drinks (doubled).

Examining the trends in car imports and exports is of particular interest to Western partner countries, as they view this indicator as crucial for sanctions implementation. According to the data, significant increases in car imports to Georgia compared to 2021 is evident.[35] The surge is remarkable: imports from Germany have increased ninefold, other EU countries have seen a fivefold rise; the U.S. has quadrupled its imports and Turkiye has doubled its import indicators. These nations remain the principal sources of imports, while imports from China and other countries have decreased since 2022.[36]

All available data support the idea that such a rise in car imports is linked to an increased

34 Statistical data from the Customs Department of the Revenues Service of Georgia was obtained in response to a public information request submitted by the CCDS on August 25, 2023.

35 Ibid.

36 Ibid.

demand for exported cars from Georgia. Perhaps, it was this apparent trend that prompted the Georgian government's decision to ban from August 1, 2023 the export and re-export of cars imported from the U.S. to Russia and Belarus, and those imported from the EU from September 26.[37]

The data indicates that there were no car exports from Georgia to Russia before 2022. However, in the first seven months of 2023, total exports saw a threefold increase compared to 2022 - a significant rise.[38]

The Georgian government's decision to ban car exports to Russia and Belarus has not elicited any comments from Russian authorities and it was implemented without complications. There have been no strong reactions from local operators involved in car exports either. However, it is important to note that Russia and Belarus could potentially secure access to the car market and Western technologies by using transportation channels through neighbouring countries that maintain robust trade relations with Georgia.[39]

## Re-Export

The years 2022 and 2023 were also marked with the growth of car re-exports to other post-Soviet countries. The most substantial increase was observed in car exports to Kazakhstan, with a threefold rise in 2022 compared to 2021 and a similar increase in 2023 compared to 2022. Re-exports of cars to Armenia rose 12 times in 2022, and the volume recorded in 2023 is comparable to that of 2022. Such an increase in car re-exports to countries with which Russia has free trade relations naturally is a cause of concern and raises suspicions that it may enable Russia to avoid sanctions.[40]

The re-export of cars to Russia experienced a 1.8 rise in 2022 compared to 2021. Extrapolating data for the first eight months of 2023 suggests that the increase would have been 1.1 in

37 Georgia bans American car exports to Russia - Georgia's Revenues Service, Business Media, 02.08.2023. Available at: https://bm.ge/news/saqartvelodan-rusetshi-amerikuli-manqanebis-eqsporti-aikrdzala-shemosavlebis-samsakhuri?fbclid=IwAR1oEKSlaqdHRYiwBj5jBLQv0Eo5uOU1IdFrLVxg48qwJtRY-kDX6U.S.nphiY.

38 Statistical data from the Customs Department of the Revenues Service of Georgia was obtained in response to a public information request submitted by the CCDS on August 25, 2023.

39 Georgia 2023 Report, Commission Staff Working Document SDW (2023) 697 final Brussels 8.11.2023. Available at: https://neighbourhood-enlargement.ec.europa.eu/system/files/2023-11/SWD_2023_697%20Georgia%20report.pdf.

40 Statistical data from the Customs Department of the Revenues Service of Georgia was obtained in response to a public information request submitted by the CCDS on August 25, 2023.

2023.[41] However, as stated, in line with the sanctions introduced by the U.S. and EU, the Georgian government banned the re-export and export of cars imported from the U.S. to Russia and Belarus from August 1, 2023.

Likewise, a ban was placed on the re-export and export of cars imported from the EU to Russia and Belarus from September 26, 2023, in line with the provisions envisaged by 11th package of sanctions imposed by the EU on Russia.[42] The government's decision to ban car re-exports to Russia and Belarus appears to be timely. However, Russia can still import cars through other post-Soviet countries with whom it shares a common economic zone. Despite Georgia not being a part of the Eurasia Economic Union, it maintains preferential trade regimes with several CIS countries.

Currently, Georgia is a party to 16 free trade agreements, including with the European Free Trade Association, China, Türkiye and the United Kingdom. In addition, preferential agreements are established with some countries with whom the EU does not have such agreements. These include Armenia, Azerbaijan, the Russian Federation, Turkmenistan, and Uzbekistan.

## Dynamics of Import and Export of Specific Goods

The analysis of Customs Department statistics on goods turnover has revealed emerging trends in foreign trade among regional countries, influenced by the effects of sanctions against Russia. The volume of goods passing through Georgia has been on the rise along with a heightened demand for sanctioned and non-sanctioned goods in post-Soviet countries. However, there is no evidence indicating any movement of sanctioned goods via Georgia to Russia and Belarus.

Nevertheless, the emergence of these new trends suggests that Georgia needs to take effective steps to monitor its foreign trade of goods and align itself with sanctions against Russia. This is particularly important now that stricter sanctions against Russia are anticipated in the coming years. Consequently, Georgia is likely to face persistent challenges for an extended

41 Data retrieved from the National Statistics Office, August 25, 2023.

42 "Georgia Bans American Car Exports to Russia," Georgia's Revenues Service, Business Media, 02.08.2023, Available at: https://bm.ge/news/saqartvelodan-rusetshi-amerikuli-manqanebis-eqsporti-aikrdzala-shemosavlebis-samsakhuri?fbclid=IwAR1oEKSlaqdHRYiwBj5jBLQv0Eo5uOU1IdFrLVxg48qwJtRY-kDX6U.S.nphiY.

period.

The compiled statistical data on imports of mobile phones to Georgia from the U.S., Turkiye, EU countries, and China falling under the category of "telephone devices and devices for transmission and reception of sound, image, and other data for wired and wireless communications" is anticipated to increase by 78% by the end of 2023 compared to 2021 figures. This projection is based on data collected over an eight month period in 2023 by authors of the present report. Notably, the import of mobile phones from Armenia increased 15 times compared to 2021, as indicated by extrapolated data from the first eight months of 2023. Interestingly, no exports of mobile devices to Russia and Belarus have taken place in 2023.

In 2021, Georgia imported computers mainly from China, the EU, the U.S., and various other countries. In 2022-2023, imports from Germany increased threefold, while China saw a 28% rise and other EU countries collectively experienced a 12% growth. Other data in this category has not changed significantly. It is worth noting that goods in this category are not exported to Russia or Belarus. However, re-exports to post-Soviet countries increased by 64% in 2022 and are estimated to rise by 73% in 2023.[43]

As regards sanctioned categories, based on data from the Revenues Service, the import of luxury goods, mainly from Turkiye, the EU and China, increased by 21-27 per cent in 2022-2023. The demand for such goods has risen by 48 per cent in post-Soviet countries, and against this background, the export of such goods from Georgia to Russia experienced a growth of 6.8 per cent.[44]

## Cases of Seizing Sanctioned Goods

According to data from the Georgian Statistics Office, the highest-value importers in 2022 were oil-importing companies, as well as those engaged in the import of cars, pharmaceuticals, electronics, and foodstuffs.

During the "Minister's Hour" in Parliament on March 23, 2023, the finance minister reported that in 2022, customs officers prevented the entry of 1020 shipments of sanctioned goods at

43 Statistical data from the Customs Department of the Revenues Service of Georgia was obtained in response to a public information request submitted by the CCDS on August 25, 2023.

44 Interestingly, the Revenues Service refuses to disclose information about importers and exporters (including legal entities) of such goods, citing customs confidentiality

Georgia's customs points. Moreover, more than 600 requests for the export and re-export of goods were turned down in the Customs Clearance Zone.[45]

Later on, the Customs Department of the Revenues Office confirmed that from the start of international sanctions against Russia and Belarus until August 25, 2023, Georgian customs authorities refused entry or registration in over 1450 cases.[46] The Revenues Service has also confirmed that it had prevented attempts to export sanctioned goods, including drones and car parts on July 29, 2022.

In response to media reports concerning ships operating under the Russian flag, the Revenues Service explained that it worked closely with the Maritime Transport Agency to systematically inspect all vessels and their owners. If a vessel or its owner is under sanctions, they are unequivocally prohibited from entering the port and undergoing customs procedures.[47]

Thus, the Georgian government claims that it has identified and documented all suspected cases of sanctions violations during 2022-2023. Nonetheless, given the upward trend of Georgia's foreign trade since the start of the Russia-Ukraine war, it is imperative for state agencies to maintain vigilance in order to effectively manage the increased turnover and ensure that Georgia avoids being listed among third countries in violation of sanctions.

## Statistics on Transit Turnover in Georgia: What Do Figures Suggest?

Georgia's transit potential has been increasingly tapped into over the past years. Since 2019, shipments of certain goods that traditionally went through Russian territory have been redirected through Georgia using the Trans-Caspian International Transport Route (TITR), commonly referred to as the Middle Corridor. The route runs from China through Kazakhstan by rail to the Aktau Port, then crosses the Caspian Sea, and proceeds by rail through Azerbaijan and Georgia to Europe through Türkiye or across the Black Sea before reaching its destination in Europe.

45 Interpressnews 23.03.2023, https://www.interpressnews.ge/ka/article/749623-lasha-xucishvili-migebulia-sankcirebuli-sakonlis-ukan-gabrunebis-1020-da-sakonlis-eksportis-an-reeksportis-ganzraxvis-taobaze-piris-momartvaze-uaris-tkmis-600-ze-meti-sabazho-gadacqvetileba/?fbclid=IwAR3W1LukLZmg8XoTfQWe67bIrxk03sPW2PUqILTVEq-wWsUPpYXAqzHIb-c.

46 Data received from the National Statistics Office, August 25, 2023.

47 Interview.

Following Russia's aggression against Ukraine, sanctions against Russia triggered a shift in cargo flows from traditional to alternative routes. An important step was taken on November 25, 2022 when Kazakhstan, Azerbaijan, Georgia, and Turkiye approved a road map for the development of the Trans-Caspian route. Moreover, in June 2023, Azerbaijan, Georgia, and Kazakhstan reached an agreement to establish a joint logistics operator. [48]

Companies that previously used the Northern route are now facing challenges related to cargo security and uncertainty surrounding insurance coverage. As a result, there has been an increase in demand for alternative routes, including the Middle Corridor which runs through Georgia. The demand is expected to continue rising as geopolitical challenges persist.[49]

**The MC among Trade Corridors Connecting Europe and Asia[50]**

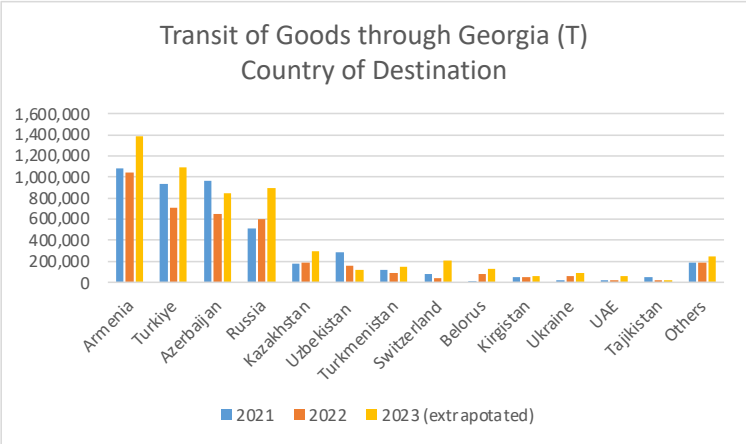
The assessment of transit turnover through Georgia based on data produced by the Customs Department highlights its increased volume. In 2022, Armenia was the leading transit destination (24%) for Georgia, followed by Turkiye (21%) and Azerbaijan (21.4%). Russia's share, which in 2022 stood at 11.35 per cent, increased to approximately 16 per cent in 2023

48 The World Bank, "Middle Trade and Transport Corridor: Policies and Investments to Triple Freight Volumes and Halve Travel Time by 2023, November 2023, Accessed December 4, 2023, https://thedocs.worldbank.org/en/doc/6248f697aed4be0f770d319dcaa4ca52-0080062023/original/Middle-Trade-and-Transport-Corridor-World-Bank-FINAL.pdf.

49 Galt a& Taggart Research, Georgian Economy Key Macro Themes in Focus. January 27, 2023, Accessed 4 December 2023, https://api.galtandtaggart.com/sites/default/files/2023-01/report/georgian-economy_key-macro-themes-in-focus.pdf.

50 The World Bank, "Middle Trade and Transport Corridor: Policies and Investments to Triple Freight Volumes and Halve Travel Time by 2023, November 2023, Accessed December 4, 2023, https://thedocs.worldbank.org/en/doc/6248f697aed4be0f770d319dcaa4ca52-0080062023/original/Middle-Trade-and-Transport-Corridor-World-Bank-FINAL.pdf.

while there were minimal changes in the data for other countries. The volume of transit cargo (in kg) to Belarus also rose 15.5 times. However, this figure may appear substantial because transit to Belarus was insignificant in the past compared to other countries, being 10 or more times less than the volume of transit to Azerbaijan and Turkiye.[51]




**Statistics on Countries of Destination[52]**

Statistics on shipping countries show that transit cargo through Georgia largely originates from Turkiye and Russia. Overall, the volume of transit shipments has increased by 24 per cent, with Russian shipments having a significant share. Transit shipments originating from Russia have increased from 20 per cent in total shipments to 29 per cent of transit volume in 2021 while the share of transit from Turkiye in total transits declined from 32.5 per cent to 28 per cent during the same period.

Based on the data collected for the first eight months of 2023, the increase of transit through Georgia in 2021-2023 is due to the increased transit from the following countries: [53]

- Kazakhstan - increased by 4.3 times, i.e. the growth is 433%
- Ukraine - 1.14 times (growth -114%)
- China - 2.8 times (286%)
- Belarus – 9.1 times (916%)
- U.S. - 2.6 times (263%)

51 Statistical data provided by the Customs Department of the Revenues Service of Georgia, in response to the public information requested by the CCDS, 26 September 2023.

52 Ibid.

53 Ibid.

- Germany – 1.9 times (186%)
- Italy – 1.3 times (132%)
- South Korea – 1.6 times - (156%)

The World Bank report indicates that to some extent the sanctions regime imposed on Russia has impacted or strengthened the region's role not only as a transit route but also as a re-exporter adjacent to/within the EAEU.[54] Georgian media have also extensively reported on the dynamics of intensified shipments along the Middle Corridor.[55]

Experts are currently exploring options to enhance the country's transit capacity, emphasizing that at this stage Georgia's load is insignificant as the country cannot not yet use its potential to the fullest due to its inadequate infrastructure. They note that while the movement of goods has increased 10-15 times, the growth in volume is not significant. In fact, the volume recorded in 2021 only grew by 24% in 2023. Experts attribute this to the lack of transshipment capacity and the failure to fully use the Georgia section of the corridor. Thus, while trade along the Middle Corridor has grown, several administrative, infrastructural, and political challenges must be overcome before it can seriously compete with Eurasia's other major trade routes.
The World Bank document, "The Impact of the War in Ukraine on Global Trade and Investment," is also sceptical about the future prospects of the Middle Corridor. The authors of the document are less optimistic about the Middle Corridor's ability to entirely replace the existing rail route.[56] Nevertheless, the upward trend in shipments through the Middle Corridor suggests that companies have started using this route despite its higher cost, extended duration and potential instability. It is also worth noting that none of the countries along the Middle Corridor route are currently subject to U.S. and EU sanctions.

54 The World Bank, "Middle Trade and Transport Corridor: Policies and Investments to Triple Freight Volumes and Halve Travel Time by 2023, November 2023, Accessed December 4, 2023, https://thedocs.worldbank.org/en/doc/6248f697aed4be0f770d319dcaa4ca52-0080062023/original/Middle-Trade-and-Transport-Corridor-World-Bank-FINAL.pdf.

55 "Shipments to Tajikistan and Uzbekistan on the Up," Rezonansi newspaper, 30.08.2023, Available at: https://www.resonancedaily.com/mobile/index.php?id_rub=3&id_artc=187960.

56 The World Bank. "Middle Trade and Transport Corridor: Policies and Investments to Triple Freight Volumes and Halve Travel Time by 2023," November 2023, Accessed December 4, 2023, https://thedocs.worldbank.org/en/doc/6248f697aed4be0f770d319dcaa4ca52-0080062023/original/Middle-Trade-and-Transport-Corridor-World-Bank-FINAL.pdf.

## Compliance Risks Coming from Occupied Abkhazia

Russia has already taken steps to carry out trade transactions using territories of Georgia's occupied Abkhazia to circumvent sanctions. This is a serious challenge for Georgia. On April 5, 2023, Russian media reported that Russia had started exporting goods through the occupied region of Abkhazia. The de facto Abkhaz customs committee confirmed the information.[57]

This was not an isolated incident. Developments unfolding in the following months revealed Russia's interest in using the occupied territories to avoid international sanctions. On June 16, 2023, Moscow and Sokhumi drew a so-called inter-governmental agreement according to which Sokhumi airport would be leased to a Russian investor. Another operational airport will provide Russia with an additional avenue to bypass sanctions.[58]

Previously, Russia was reluctant to refurbish the airport in question but now, with sanctions tightening even more and no prospect of their withdrawal, Russia needs additional communication routes in so-called grey zones - regions not recognized by the rest of the world. It is anticipated that Russia will attempt to use Abkhazia's port and airport. Shipments will arrive in Sokhumi by rail and air and transported from there by sea.

It is essential for Georgia to protect its vital interests by preventing such transportation operations from occurring on its occupied territories. While the central government lacks access to or control over the processes in the occupied region of Abkhazia and has limited leverage to influence Russia, it remains imperative for it to take all necessary measures to prevent any country from engaging in schemes that violate sanctions or promote illegal trade in Abkhazia.

Georgia cannot deal with this problem on its own and will require support from its Western partners. It is also important for Georgia that the U.S. and the EU reaffirm at every international forum that they: continue to support Georgia's sovereignty and territorial integrity within its internationally recognized borders; consider Sokhumi airport part of Georgia's airspace and demand from Russia to withdraw its forces to the positions before the conflict in accordance with the ceasefire agreement brokered by the EU in 2008.

---

57 "Russia has Started Delivering Cargo to Turkiye through Occupied Abkhazia" Interpressnews (in Georgian), May 4, 2023, Accessed December 4, 2023, https://www.interpressnews.ge/ka/article/751288-rusetma-okupirebuli-apxazetis-gavlit-turketistvis-tvirtis-micodeba-daicqo.

58 Radiotavisupleba RFE/RL, "Where does Abkhazia fly to?" (in Georgian), June 23, 2023, Accessed 4 December 2023.

This also means that Georgia needs to demonstrate strong support to its partners and take a clear and decisive stance on the issue of sanctions against Russia.

## Lifting the Ban on Direct Flights with Russia

The Russian government's decision of May 11, 2023 to lift the ban on flights with Georgia created yet another challenge. Many observers agree that Russia's decision could be linked to its plan to evade sanctions and that the development could put Georgia in a difficult position. This seems especially true as Russian President Vladimir Putin has revealed that the resumption of direct flights to Georgia was his personal idea and decision.[59]

The EU expressed its "regret" at the Georgian government's decision to resume direct flights with Russia and expressed concern that the decision ran counter to the EU determination to isolate and pressure Russia to stop its aggressive war in Ukraine.[60,61]

In response, the Georgian economy minister made explanatory statements, stating that Georgia could not be viewed in the same context as other countries because it was not an EU member. Other officials added that Tbilisi was consulting with countries that have maintained air connections with Russia while abiding by the sanctions.[62]

There is a concern that direct flights between Georgia and Russia may increase the risk of sanctions violations despite the government's assurances that it strives to achieve the highest level of sanctions enforcement, including tightening controls at customs checkpoints and airports.[63] The then U.S. ambassador to Georgia, Kelly Degnan, emphasized the importance of determining whether relevant airlines were sanctioned and evaluating safety risks.[64]

---

59 Civil.ge. "Putin Says Direct Flights with Georgia was his Decision, Georgian Leadership has Repeatedly Raised this Issue". 27 May 2023. Accessed 4 December 2023. https://civil.ge/archives/544713

60 Agenda.ge. Economy Minister: "Direct flights with Russia "can't be viewed in same context" as other countries". 29 May 2023. Accessed December 4, 2023. https://agenda.ge/en/news/2023/2102

61 Reuters. "Georgia to resume flights to Russia this week, drawing EU and Ukrainian criticism." 20 May 2023. Accessed 4 December 2023. https://www.reuters.com/world/europe/georgian-airways-resume-direct-flights-russia-may-20-2023-05-16/

62 "Georgia: Uncertainty Looms as First Carriers Authorized for Russia Flights," Eurasianet, May 16, 2023, Accessed December 4, 2023, https://eurasianet.org/georgia-uncertainty-looms-as-first-carriers-authorized-for-russia-flights.

63 Agenda.ge. "Economy Minister: Direct Flights with Russia "Can't be Viewed in Same Context" as other countries, 29 May 2023, Accessed December 4, 2023, https://agenda.ge/en/news/2023/2102.

64 U.S. Embassy to Georgia, "Ambassador Degnan Remarks at Peace Corps Swearing in Ceremony," May

The U.S. State Department's deputy spokesperson, Vedant Patel, also cautioned about the sanctions risks for companies at Georgian airports if they "service aircraft subject to import and export controls. [65]

Interesting opinions were voiced by James O'Brien, whose candidacy was considered for the position of Assistant Secretary of State for European and Eurasian affairs at a Senate hearing on July 26, 2023.[66] When asked by Senator Jeanne Shaheen about his visit to Georgia and the country's stance towards the Russia sanctions, O'Brien noted that full control was required to monitor movements of cargo by air and land and this goal necessitated continuous work: "… so we want to make sure we know what is going on those planes on the way back to Russia."[67]

Thus, the Georgian authorities will be required to take steps in the near future in response to the current challenges to improve the implementation of sanctions, which will convince Georgia's partner countries, the U.S., the UK, the EU, and its Member States that sanctioned goods do not reach Russia through Georgia.

## Conclusions and Recommendations

Against the backdrop of the United States and EU decisions to tighten measures against sanctions violators, Georgian officials have repeatedly affirmed their commitment to comply with sanctions and have denied there was any potential for violations. However, instances reported in the international media and findings from the studies on foreign trade statistics of Georgia suggest the upward trend of Georgia's foreign international trade since the start of

15, 2023, Accessed 4 December 2023, https://ge.usembassy.gov/ambassador-degnans-remarks-at-peace-corps-swearing-in-ceremony/.

65 "Georgia: Uncertainty Looms as First Carriers Authorized for Russia Flights," Eurasianet, May 16, 2023, Accessed December 4, 2023, https://eurasianet.org/georgia-uncertainty-looms-as-first-carriers-authorized-for-russia-flights.

66 Opening Statement of James C. O'Brien, Nominee for Assistant Secretary of State for European and Eurasian Affairs, Senate Nomination Hearing,Foreign Relations Committee, U.S. Senate, Date: Wednesday, July 26th, 2023, Committee on Foreign Relations, July 26, 2023, Accessed 4 December 2023, https://www.foreign.senate.gov/imo/media/doc/6afd18d1-b8f4-441f-544c-ea148014a01c/072623_O%27Brien_Testimony.pdf ;Georgian media outlets reporting on the hearing on 27-28 July 2023. https://civil.ge/ka/archives/553405 https://www.amerikiskhma.com/a/7199953.html?fbclid=IwAR24gCKoc-RBljf4XwPVu1tDlcBH6R8jEa-hZipULwrBUHr0fMmjuUqU6wQ.

67 Nomination Hearing, Foreign Relations Committee, U.S. Senate, Date: Wednesday, July 26th, 2023. Time: 2:30pm, Location: SD-419.

the Russia-Ukraine war.[68] In addition, continuous detection of attempts to transit sanctioned goods by Georgian agencies throughout 2022-2023 indicates the trend is likely to persist in the future. This is compounded by the fact that none of the countries sharing a land border with Georgia have aligned themselves with the sanctions against Russia.

Currently, Georgia remains highly vulnerable to Russian military threats, requiring a delicate balance between mitigating security risks posed by Russia and potentially aligning with major Western allies. Such a balance can be achieved by reducing risks emanating from economic dependence on Russia and avoiding scenarios in which Russia could exploit economic ties for political advantages. However, analysis of the foreign trade dataset figures suggests that sustained economic rapprochement with Russia does not seem to be an inevitable long-term trend for Georgia. It could be replaceable through trade with other countries, including neighbouring nations.

Besides, the years 2022 and 2023 witnessed a surge in Georgian re-exports to other post-Soviet nations. Notably, significant growth was observed in exports to Kazakhstan, Kyrgyzstan, Uzbekistan, and Armenia. This suggests that Russia could still acquire goods through other post-Soviet countries with whom it maintains a shared economic zone. Consequently, the current challenge for Georgia lies in devising effective strategies to address this issue and proactively prevent potential sanctions evasion by Russia through intensifying collaboration with the U.S., EU, United Kingdom, G7, and the Euro-Atlantic community.

Regarding the amplified volume of re-exports involving dual-use goods that are explicitly sanctioned by both the EU and U.S., Georgia should prioritize scrutinizing the reliability of end-user certificates. Ensuring that goods are not transported without the necessary documentation is crucial.

Overall, it is crucial for state agencies to uphold vigilance and allocate ample administrative resources to manage the escalated trade volume diligently. This proactive approach is essential to prevent Georgia from being listed amomg third countries in violation of sanctions. Strengthening cooperation with international partners like the U.S., the European Union, Great Britain, the G7, and the Euro-Atlantic Community members is instrumental in achieving this objective. Collaborative efforts can effectively identify potential red flags denoting sanctions evasion and violations of export controls. This collective vigilance and collaborative approach will play a vital role in safeguarding compliance and deterring any attempts to circumvent sanctions.

68 National Statistics Office of Georgia, External Merchandise Trade, Accessed on 07 February 2024, Available at: https://www.geostat.ge/en/modules/categories/765/external-merchandise-trade.

The following recommendations could help Georgia navigate the complexities of its geopolitical landscape and safeguard its security interests :

1. Reduce Economic Dependence on Russia: Georgia should prioritize diversifying its economic partnerships to reduce reliance on Russia. This entails fostering trade relations with other countries, particularly those outside the post-Soviet region. By expanding its trade network, Georgia can mitigate the risk of economic manipulation by Russia for political gain.

2. Enhance Collaboration with Western Allies: Given the vulnerability to Russian military threats, Georgia should strengthen its cooperation with major Western allies, members of the Euro-Atlantic community. Closer collaboration will bolster Georgia's security posture and deter potential aggression from Russia. Collective vigilance and a collaborative approach will also facilitate the early detection of potential sanctions evasion and bolster compliance with export controls.

3. Address Re-export Challenges: Georgia must address the surge in re-exports, particularly of dual-use products subject to sanctions by the EU and the U.S.. Prioritizing the verification of end-user certificates and ensuring strict adherence to documentation requirements will mitigate the risk of unwittingly facilitating sanctions evasion.

4. Allocate Administrative Resources: State agencies in Georgia must allocate adequate administrative resources to manage the heightened trade volume diligently. Vigilance is paramount to prevent inadvertent violations of sanctions and to avoid being listed among third countries in breach of international sanctions regimes.

# Counterproliferation of Weapons of Mass Destruction: Strategies against Terrorism through a Questionnaire-Based Study

Anamika, Varun Gulati*

**Keywords:** Weapons of Mass Destruction, proliferation, questionnaire, strategies, risk management

## Abstract

*The study was conducted with an aim to address the critical issue of preventing the spread and misuse of Weapons of Mass Destruction (WMD) in the context of the threat of terrorist attacks involving nuclear, biological, and chemical weapons, their delivery systems and related materials. The study utilized a questionnaire-based research methodology to gather insights from subject matter experts and the scientific community, providing a comprehensive understanding of the motivations, capabilities, resources, and potential consequences of WMD proliferation.*

*The study results highlighted the multifaceted motivations of potential proliferators, including deterrence, prestige, financial gain, and offensive purposes, necessitating a*

* Dr. Anamika is Assistant Professor at the Center for Studies in Science Policy, School of Social Sciences, Jawaharlal Nehru University, New Delhi, and Convener and Innovation Ambassador of Institute's Innovation Council and Coordinator, National Innovation Startup Policy, Ministry of Education's Innovation Cell. Dr. Varun Gulati is a distinguished academic with 18 years of teaching experience in the Department of English at the Arts Faculty, North Campus, University of Delhi. Funding: The research has been funded by U.S. CRDF Global.

*nuanced assessment of the risks associated with WMD proliferation. It also underscores the significance of understanding the capabilities and resources available to potential proliferators, such as scientific, technological, and industrial capabilities, as well as financial and human resources. Additionally, the study focused on the potential consequences of WMD proliferation, including its impact on regional and global security, the economy, and society, and underscoring the need for robust measures to prevent and counter its proliferation.*

*The study also highlighted the importance of nonproliferation strategies, including diplomatic, economic, and military measures, and emphasizes the costs and benefits of different strategies. It underscores the necessity for organizations to establish due diligence processes, policies, procedures, and training programs, and to collaborate with other stakeholders to address WMD proliferation challenges effectively. Additionally, it acknowledges the potential for technology or expertise to be misused for WMD development and emphasizes the importance of sharing experiences and best practices to raise awareness and improve risk management.*

*In conclusion, the study provided valuable insights into the risks of WMD proliferation for companies and institutions, highlighting the need for proactive risk management strategies, collaboration with stakeholders, and a deep understanding of the potential consequences and implications of WMD proliferation. It underscores the importance of addressing these risks through a comprehensive and collaborative approach, proactive risk management strategies, and a deep understanding of the potential consequences and implications of WMD proliferation.*

## Introduction

As part of efforts by the International communities to prevent the spread of Weapons of Mass Destruction (WMD), increasing attention is being directed towards preventing the proliferation and misuse of dual-use technologies. This is deemed essential globally in light of the threat of use by terrorist and other non-State groups involving nuclear, biological, and chemical weapons. The United Nations recognizes the potential dangers posed by such weapons, including nuclear devices, radioactive material, biological pathogens, and chemical substances and canvassed these as a global issues.[2] Preventing the use of WMDs and the spread of their delivery systems requires a comprehensive approach involving arms control, disarmament, and nonproliferation.[3]

1 United Nations, Disarmament, 2024, https://www.un.org/en/global-issues/disarmament.

2 NATO, 2023, Weapons of Mass Destruction. NATO, https://www.nato.int/cps/en/natohq/topics_50325.htm.

It is crucial that the scientific community in concerned countries understands the risks associated with their interactions with groups and organizations in suspected WMD-producing nations. These institutions must realize that proliferation-related procurement can occur not only through direct transactions but also through agents, front organizations, and other indirect means. Terrorists may use indirect methods to conceal their true objectives, and therefore vigilance is necessary.[4]

Dual-use and arms export controls cover a wide range of physical items as well as software and technology, including conventional arms, delivery systems for WMDs, and parts and components related to WMDs. They are applied to different categories of technology, for instance, the "specially designed" or "necessary" technology for "development, production, or use" of items with nuclear capabilities. Technology and software in these frameworks are considered as part and parcel of the interventions.[5]

Some types of software and technologies can be covered by various export control regimes, e.g., Australia Group (AG; focuses on biological and chemical weapons), the Missile Technology Control Regime (MTCR; focuses on delivery system), the Nuclear Suppliers Group (NSG; focuses on nuclear weapons), the Wassenaar Arrangement (focuses on conventional weapons such as small arms and rockets), and country-specific or regional arms export control frameworks. License agreements accompanying technology and software are avenues through which technology and software are transferred, such as in the commercial sale of restricted software or technology or products carrying these items.[6]

An additional challenge undermining the proliferation networks or the non-state actors producing WMDs is the method or medium of delivery of these weapons.[7] In many cases, weapons are ineffective because they are unable to be deployed since they lack the means of

4 Kassenova, T. (2020), The Exploitation of the Global Financial Systems for Weapons of Mass Destruction (WMD) Proliferation. Carnegie Endowment for International Peace. https://carnegieendowment.org/2020/03/04/exploitation-of-global-financial-systems-for-weapons-of-mass-destruction-wmd-proliferation-pub-81221; Ouagrham-Gormley, S. B. (2012). Barriers to Bioweapons: Intangible Obstacles to Proliferation. International Security, 36(4), 80–114, https://doi.org/10.1162/ISEC_a_00077.

5 Bromley, M., & Maletta, G. (2018). The challenge of software and technology transfers to nonproliferation efforts: Implementing and complying with export controls. https://www.nonproliferation.eu/wp-content/uploads/2019/11/sipri1804_itt_software_bromley_et_al.pdf.

6 de Bruin, E. (2022). Export Control Regimes—Present-Day Challenges and Opportunities. In R. Beeres, R. Bertrand, J. Klomp, J. Timmermans, & J. Voetelink (Eds.), NL ARMS Netherlands Annual Review of Military Studies 2021 (pp. 31–53). T.M.C. Asser Press. https://doi.org/10.1007/978-94-6265-471-6_3.

7 Mcisaac, J. (2011). (P1-24) Future Weapons of Mass Destruction: Preparing For Emerging Threats. Prehospital and Disaster Medicine, 26(S1), s106–s107. https://doi.org/10.1017/S1049023X11003566; Salama, S., & Hansell, L. (2005). Does Intent Equal Future Capability? AI-Qaeda and Weapons of Mass Destruction. https://www.aclu.org/wp-content/uploads/legal-documents/ACLURM002136.pdf.

delivering themselves, through the use of ballistic missiles, cruise missiles, or UAVs. Some proliferating states to the question of concern have not yet reached the desired technological level to create these means. But, it is alarming to know that some countries, which are technologically able to do so, are willing to sell the technology or offer it as technical support.[8] Despite the existence of various relevant treaties (MTCR, AG, NSG, Wassenaar Arrangement), there are state seeking to obtain WMDs, their delivery systems and related materials, often motivated by a perceived power imbalance in their region. Historically, these countries have been overt in their attempts to procure goods and knowledge from Europe and other countries with high technology.[9] However, after the Gulf War against Iraq in 1990-1991, it was discovered that Iraqi government institutions had not only procured dual-use goods from Western countries but also that Iraqi technicians and scientists had received training in Western Europe and North America. The companies and scientific institutions involved were generally unaware of their contribution to the Iraqi WMD program.[10]

Governments have become more aware of possible procurement activities and export control mechanisms have been refined to the point where overt procurement of proliferation-sensitive goods and knowledge is difficult. As a result, countries of concern are increasingly attempting to conceal their procurement activities, for example by using transshipment hubs, employing false end-user documentation, engaging in document fraud, and using scientific exchange through students, involvement of concerning entities, matching denied

8 Ackerman, G., & Jacome, M. (2018). WMD Terrorism: The Once and Future Threat - ProQuest. Prism : A Journal of the Center for Complex Operations; Washington, Vol 7(Issue 3), 22–36; Gosden, C., & Gardener, D. (2005). Weapons of mass destruction—Threats and responses. BMJ : British Medical Journal, 331(7513), 397–400; Maitre, E. (2022). Arms Control and Delivery Vehicles: Challenges and Ways Forward. Journal for Peace and Nuclear Disarmament, 5(1), 123–147. https://doi.org/10.1080/25751654.2022.2047360; Moltz, J. C., Monterey Institute of International Studies, & Mountbatten Centre for International Studies (University of Southampton) (Eds.). (2003). New challenges in missile proliferation, missile defense, and space security [Electronic resource]. Monterey Institute of International Studies, Center for Nonproliferation Studies ; University of Southampton, Mountbatten Centre for International Studies. http://cns.miis.edu/pubs/opapers/op12/index.htm.

9 Reynolds, C. (2019). Global Health Security and Weapons of Mass Destruction Chapter. Global Health Security, 187–207. https://doi.org/10.1007/978-3-030-23491-1_9.

10 Ali, J. (2001). Chemical weapons and the Iran-Iraq war: A case study in noncompliance. The Nonproliferation Review, 8(1), 43–58. https://doi.org/10.1080/10736700108436837; Baxter, P., Hastings, J. V., Kim, P., & Yim, M. (2023). Assessing Intangible Technology Transfer in North Korea's Nuclear International Collaboration Networks. Strategic Trade Review, 9(10), 51–78; Halliday, F. (1994). The Gulf War 1990-1991 and the Study of International Relations. Review of International Studies, 20(2), 109–130; Kim, H. (2023). Intangible Transfer of Technology (ITT): Open-source Information Analysis for the Implementation of Sanctions on North Korea - 38 North: Informed Analysis of North Korea, 38 North, https://www.38north.org/2023/03/intangible-transfer-of-technology-itt-open-source-information-analysis-for-the-implementation-of-sanctions-on-north-korea/; Salisbury, D., & Dolzikova, D. (2023). Profiting from Proliferation? North Korea's Exports of Missile and Nuclear Technology, https://static.rusi.org/onward-proliferation-dprk-occasional-paper-dec-2023.pdf.

persons lists, inconsistent business profiles, freight forwarding as final destination, orders from mismatched locations, technical incompatibility, complex ownership structures and misleading documentation, or advanced technologies that can be used in new or novel ways to enhance adversaries' military capabilities or support mass surveillance programs that enable human rights abuses.[11] There is no reason to believe that terrorists will not use the same strategies.

This questionnaire-based research aimed to identify the possible risks for companies and institutions with respect to proliferation of WMDs, their delivery systems and related materials and how these risks can be identified as well as the methods terrorist groups use to obtain knowledge and goods for their WMD projects and the strategies to overcome the identified risks of proliferation.

## Research Methodology

The study was carried out by means of interviews with subject matter experts and scientific community possessing domain expertise in the areas of technology transfer and national security through the questionnaire. The experts were contacted through the institutional email IDs from the respective institute websites. These experts were from various National as well as International organisations including research Universities, research institutes and think tanks like Observer Research Foundation (ORF), Stockholm International Peace Research Institute (SIPRI), Center for Strategic and International Studies (CSIS), National Institution for Transforming India (NITI) Aayog, Centre for Air Power Studies, etc. However, few of the respondents refused to disclose their work institute.

## Participant Confidentiality

The participation of the experts in the study was voluntary and the questionnaire responses was stored in a secure electronic database. Only authorized researchers had the access to this

11 FinCEN and the U.S. Department of Commerce's Bureau of Industry and Security Announce New Reporting Key Term and Highlight Red Flags Relating to Global Evasion of U.S. Export Controls. (2023, November 6). https://www.bis.gov/press-release/fincen-and-us-department-commerces-bureau-industry-and-security-announce-new; Jack, L. (2024, April 23). Counterproliferation Finance Detection and Deterrence—What Can Financial Institutions Do? Institute for Financial Integrity. https://finintegrity.org/counterproliferation-finance-detection-and-deterrence-what-can-financial-institutions-do/.

data. The authors of this research article affirm that any personal information collected from participants during the study has been treated with the utmost confidentiality. All data collected has been anonymized in a secure manner to protect participant privacy. Any identifying details that could potentially disclose the identity of participants have been removed. The findings presented in this article are based on aggregated and anonymized data. The authors respect the rights and privacy of the participants involved and are committed to maintaining the confidentiality of their information.

## Study Questionnaire

The following questionnaire was employed to engage the scientific/subject experts to obtain their expert opinions on the potential risks for companies/organisations and institutions with respect to the WMD proliferation. In addition, viewpoints were also acquired on how these risks can be identified and also the methods terrorist groups use to obtain knowledge and goods for their WMD projects and provide the strategies to overcome the identified risks of proliferation.

The intricately constructed questionnaire is outlined below:

- What is your primary industry or area of expertise? (e.g., pharmaceuticals, chemicals, biologicals, technology, finance, research, etc.)
- Dual-Use Technologies: Do you develop, manufacture, or export any products or technologies that could have dual-use applications (civilian and military)? If so, please specify.
- Why did the actor acquire a WMD program? Or What are the motivations of the potential proliferators?
- Are they seeking to acquire WMDs for deterrence, prestige, or offensive purposes? Understanding the motivations of potential proliferators can help decision-makers to assess the risk of proliferation and to develop appropriate countermeasures.
- What are the capabilities of the potential proliferators?
- Do they have the scientific, technological, and industrial capabilities to develop and produce WMDs? Assessing the capabilities of potential proliferators can help decision-makers to identify the most pressing proliferation threats.
- What are the resources available to the potential proliferators?
- Do they have the financial and human resources necessary to develop and produce WMDs?

Assessing the resources available to potential proliferators can help decision-makers to gauge the likelihood of proliferation.

- Does simple acquisition present a threat that necessitates a response?
- What is the desired effect the actor wishes to achieve (kill people, gain publicity, retaliation, etc.)?
- What is the vital interest threatened by the actor's use of WMD? Is it national survival, territory, military forces, population, economic interests, etc.?
- Is there any defensive protection in existence or is offensive protection the only viable means of deterring WMD use?
- What type(s) of technology has the actor acquired or developed?
- What are the centers of gravity of this actor, and are they vulnerable?
- What is the international context?
- Are there regional conflicts or tensions that could motivate countries to acquire WMDs? Are there international norms and institutions that can help to prevent proliferation? Assessing the international context can help decision-makers to identify the factors that are driving or restraining proliferation.
- What are the potential consequences of WMD proliferation?
- How would WMD proliferation affect regional and global security? What would be the impact of WMD proliferation on the economy and society?
- What are the options for preventing WMD proliferation?
- What diplomatic, economic, and military measures can be used to deter and counter proliferation?
- What are the costs and benefits of different nonproliferation strategies?
- How can decision-makers weigh the risks and benefits of different strategies to choose the best course of action?
- Are you aware of the potential risks of WMD proliferation for companies and institutions like yours?
- Have you conducted any formal assessments to identify potential WMD proliferation risks within your organization?
- Do you have any policies, procedures, or training programs in place to mitigate these risks? If so, please elaborate.
- Do you conduct due diligence on potential partners, suppliers, or customers to assess their involvement in WMD proliferation activities?
- Do you have a system for reporting suspicious activities or potential violations of WMD

proliferation regulations?

- How concerned are you about the financial risks associated with WMD proliferation, such as sanctions or reputational damage?
- How concerned are you about the operational risks, such as disruption of supply chains or damage to facilities, that could result from WMD proliferation?
- How concerned are you about the potential for your technology or expertise to be misused for WMD development or proliferation?
- How concerned are you about the potential for legal liability if your organization is inadvertently involved in WMD proliferation activities?
- What additional steps do you think companies and institutions should take to mitigate the risks associated with WMD proliferation?
- How open would your organization be to collaborating with other stakeholders (governments, industry associations, NGOs) to address WMD proliferation challenges?
- Would you be interested in sharing your experiences and best practices with others in your sector to raise awareness and improve risk management?

## Results

The investigation achieved a total response rate of 19 experts who consented to complete the questionnaire and provide their subject matter expertise on WMD proliferation-related matters. These outcomes indicate that the survey was filled out by diverse stakeholders from educational, governmental, and research sectors, all potentially involved in areas pertinent to WMD proliferation concerns and among the respondents, research was the major focus area (Figure 1).

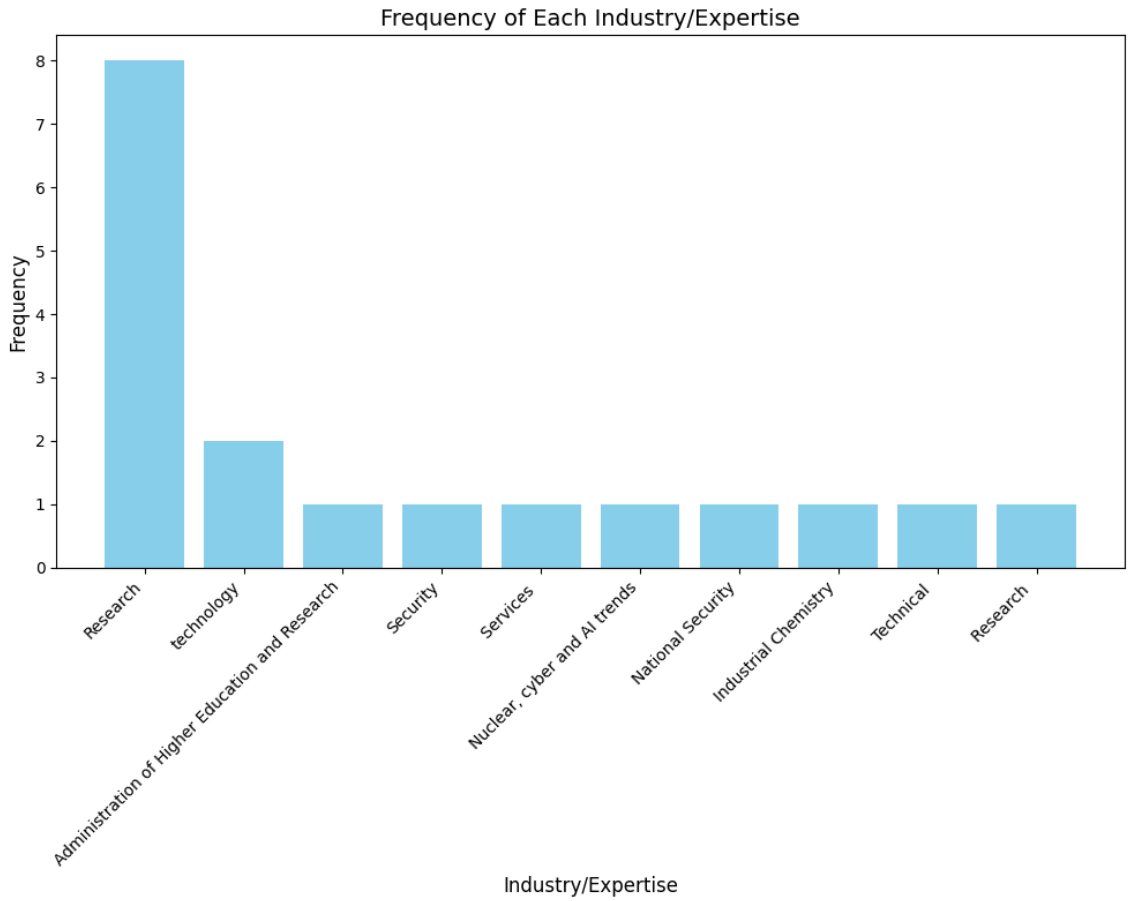



**Figure 1: Type of Industry/Expertise**

**a. Why did the actor acquire a WMD program? Or What are the motivations of the potential proliferators?**

The motivations of potential proliferators in acquiring WMD vary. Some seek WMDs for deterrence, prestige, or offensive purposes. These motivations can help decision-makers assess the risk of proliferation and develop appropriate countermeasures. Additionally, few experts believe that potential proliferators are primarily motivated by financial gain. However, it is important to note that the motivations for acquiring WMDs are complex and multifaceted, encompassing a range of factors such as geopolitical advantage, status, and national security. Understanding these motivations is crucial for assessing the likelihood of proliferation and developing effective strategies to prevent it.

**b. What are the capabilities of the potential proliferators? Do they have the scientific, technological, and industrial capabilities to develop and produce WMDs? Assessing the**

**capabilities of potential proliferators can help decision-makers to identify the most pressing proliferation threats.**

The ability of potential proliferators to develop and produce WMDs depends on a complex interplay of scientific, technological, industrial, financial, and international factors. While some countries or entities (state or non-state actors) may possess the full spectrum of capabilities required for independent WMD development, others may rely on external support or illicit networks to acquire the necessary materials and technologies. International efforts to prevent proliferation focus on disrupting these capabilities and denying potential proliferators the resources they need to succeed. Especially the non-state actors have high-tech human resources and sufficient liquid funds, enabling them to acquire or develop WMDs. Additionally, they have the financial and human resources necessary for WMD development. It is noted that technological and scientific capabilities are often outsourced, and industrial capabilities are considered vital. Furthermore, it is emphasized that the capabilities of potential proliferators are dependent on the actor and that they are continually in the process of acquiring or improving resources. Understanding these capabilities is crucial for decision-makers to identify and address the most pressing proliferation threats.

c. **What are the resources available to the potential proliferators? Do they have the financial and human resources necessary to develop and produce WMDs? Assessing the resources available to potential proliferators can help decision-makers to gauge the likelihood of proliferation.**

Potential proliferators often possess or acquire the financial and human resources necessary to develop and produce WMDs. Many potential proliferators are state actors with significant government budgets (e.g., North Korea, Iran, etc.). These states can allocate substantial funds to WMD programs, often disguised within defense or research budgets to avoid detection. Non-state actors and states under sanctions often engage in illicit activities such as smuggling, trafficking, and other forms of organized crime to generate the necessary funds, establishing legitimate-looking businesses to channel funds and acquire materials without attracting suspicion or using offshore financial centers to obscure financial transactions and maintain anonymity.

Countries with advanced educational systems and research institutions train and retain a highly skilled workforce of scientists, engineers, and technicians with expertise in nuclear, chemical, biological, and missile technologies who in turn are capable of developing WMDs. Also, the non-state actors recruit foreign experts through legal or illegal means, including

enticing them with financial incentives or coercion and utilize diaspora networks to bring in expertise from abroad. Further, non-state actors expand by investing in domestic education and training programs to develop the necessary technical skills and sending students and professionals abroad to study in fields relevant to WMD development.

To add, experts view was that the technology is not static and cannot be confined. It bound to proliferate and grow. In this age of capitalism, globalization and ideological rivalry, technology proliferation happens for profit making, ideology promotion, etc. So proliferation motive is not handicapped by technology unavailability, or scientific-industrial incapability. Anybody can procure and spread it in this age of IT revolution and mad rush for profit making. More than scientific or technological capabilities, a potential proliferator has is industrial capabilities; technological and scientific capabilities are now outsourced. The clear comprehension of the main enablers of proliferation and their capabilities allow decision makers to define dissemination chances and create relevant countermeasures accordingly.

**d. Does simple acquisition of WMDs present a threat that necessitates a response?**

The question of whether simple acquisition of WMD or mere acquisition of such weapons presents a threat that necessitates a response is not straightforward. Nevertheless, based on the received information shared by the experts, this mere acquisition doesnot necessarily present a threat directly that necessitate a response, however, if a country develops or acquires (for example) long-range missile technologies, then that allows them to expand their deterrent and presence of WMDs in any part of the world is a threat to every part of the world.

The responses from the experts also indicate that the potential threat posed by the acquisition varies depending on the specific actor and their unique motivations. Some actors may seek to increase national power or gain publicity through acquisition, while others may view it as a means of deterrence. Additionally, these experts suggests that diplomatic channels may be required to indirectly respond to simple acquisition, rather than a direct military or economic response. Therefore, the assessment of whether simple acquisition necessitates a response is contingent on the specific circumstances and the actor involved.

**e. What is the desired effect the actor wishes to achieve (kill people, gain publicity, retaliation, etc.)? And what is the vital interest threatened by the actor's use of WMD? Is it national survival, territory, military forces, population, economic interests, etc.?**

The desired effect the non-state actor wishes to achieve varies and can include gaining publicity, retaliation, deterrence of the target state, and potentially killing people. Additionally, the desire for status, violence, and retribution are also identified as potential motivations for the acquisition of WMDs. It is important to note that the specific desired effect may depend on the individual actor and their unique motivations. Understanding these desired effects is crucial for assessing the potential risks and implications of WMD proliferation and for developing appropriate strategies to address them.

The vital interest threatened by the state actor's use of WMD can vary depending on the context and the actor's motivations. However, the expert suggests that national survival is often at the core of these threats. National survival encompasses a range of elements including the government, military, population, and territory. These elements are considered the basis of a state's survival and can be targeted by WMD use. Additionally, economic interests are also identified as threatened by the actor's use of WMDs. The responses indicates that the use of WMDs can lead to significant destruction and loss of life in the country where such weapons have been used, which in turn can affect the country's economic stability and overall security. Therefore, the use of WMDs poses a direct threat to national survival and economic interests.

**f. Is there any defensive protection[12] in existence or is offensive protection[13] the only viable means of deterring WMD use?**

To this, the experts suggests that defensive protection against the spread of WMDs is limited, and international collaboration is crucial in this regard. The responses indicate that offensive protection is considered the primary means of deterring WMD use. It is emphasized that major powers have the capability to prevent the proliferation of WMDs, and offensive action is seen as the most viable means of deterring their use. Additionally, the responding experts highlights that the best defence against WMD use is the capability to carry an unacceptable second strike, along with other protective measures such as ballistic missile defence and anti-drone measures. Therefore, the prevailing view is that offensive protection is the most effective means of deterring WMD use.

12 Defensive protection strategies focus on mitigating the effects of WMDs in case of their use such as missile defence system, civil defence measures, Biological and Chemical Defence, and medical countermeasures.

13 Offensive protection strategies are aimed at disrupting or preventing the proliferation and use of WMDs by adversaries including export controls, counterproliferation operations, Diplomatic Efforts, and cyber operations.

**g. What type(s) of technology has the actor acquired or developed?**

The actor has acquired or developed various types of technology, including Electronic Measures and Electronic Counter Measures, aerospace technology, and nuclear weapon technology of different yields, cruise and ballistic missiles capable of being launched from ground, air, sea and undersea, industrial aviation technology. Additionally, the experts suggests that terror groups may seek to miniaturize chemical and biological weapons to enable drones or UAVs to carry out WMD attacks. The technology that an actor has acquired or developed is further dependent upon the actor. If looking at China, its development of hypersonic boost glide systems, and expansion of its missile silos expand its ability to penetrate missile defences thereby strengthening its deterrent.

It is also noted that the there is a significant shift in the technological and scientific landscape for WMD development indicating that likely a state or non-state actors has transitioned from relying solely on internal technological and scientific capabilities to seeking external sources, partnerships or acquisitions for these capabilities.[14] Further, these actor recognizes the critical role of industrial infrastructure and expertise in advancing their WMD programs.

**h. What are the centers of gravity of this actor, and are they vulnerable?**

The centers of gravity[15] of the state-actor are primarily related to political leadership and scientific cadre. These centers of gravity are considered vulnerable, particularly in the context of weak political leadership and governance. Additionally, the experts suggests that the vulnerability of these centers of gravity varies depending on the actor, and that political leadership is a key focus. For non-state actors, the various key focus points include leadership, financial resources, communication networks, logistics and supply chains, support base, ideological foundation, safe havens, and availability of human resources. Understanding the vulnerability of these centers of gravity is crucial for assessing the potential risks and implications of WMD proliferation and for developing appropriate strategies to address them.

14 Rajagopalan, R. P., & Patil, S. (2024). Future Warfare and Critical Technologies: Evolving Tactics and Strategies, https://www.orfonline.org/public/uploads/posts/pdf/20240212113627.pdf.

15 "Centers of gravity" is a concept often used in strategic planning, military operations, and organizational analysis to identify critical elements that are essential for the functioning and effectiveness of an entity, such as a state, organization, or actor. These elements are focal points or sources of strength that, if targeted or compromised, could significantly impact the entity's ability to operate effectively.

**i. What is the international context? Are there regional conflicts or tensions that could motivate countries (state actors) to acquire WMDs? Are there international norms and institutions that can help to prevent proliferation? Assessing the international context can help decision-makers to identify the factors that are driving or restraining proliferation.**

The international context surrounding the proliferation of WMDs is complex and multifaceted. There are regional conflicts and tensions that could potentially motivate countries to acquire WMDs, with factors such as geopolitical rivalries, territorial disputes, and national security concerns contributing to this motivation. Further, as per the experts, that international norms and institutions play a crucial role in preventing proliferation. Diplomatic, economic, and military measures, as well as international cooperation and dialogue, are highlighted as key strategies to deter and counter WMD proliferation. Understanding the international context is essential for decision-makers to identify the driving forces and constraints related to WMD proliferation and to develop effective strategies to address these challenges.

**j. What are the potential consequences of WMD proliferation? How would WMD proliferation affect regional and global security? What would be the impact of WMD proliferation on the economy and society?**

The potential consequences of WMD proliferation are significant and far-reaching. They pose a grave threat to regional and global security, potentially leading to a destabilizing impact on the international order. WMD proliferation can result in heightened tensions, increased risk of conflict, and the potential for catastrophic consequences, including mass casualties and widespread destruction. Additionally, the proliferation of WMDs can have a profound impact on the economy, leading to disruptions in trade, investment, and overall economic stability. Furthermore, the societal impact of WMD proliferation is substantial, as it can create fear, insecurity, and social unrest, affecting the well-being and safety of populations. Overall, WMD proliferation has the potential to cause severe and widespread harm, necessitating robust measures to prevent and counter its proliferation.[16]

As per the responding experts, the potential consequence of WMD proliferation is financial

16 Kassenova, T. (2020). The Exploitation of the Global Financial Systems for Weapons of Mass Destruction (WMD) Proliferation. Carnegie Endowment for International Peace. https://carnegieendowment.org/2020/03/04/exploitation-of-global-financial-systems-for-weapons-of-mass-destruction-wmd-proliferation-pub-81221; Reynolds, C. (2019). Global Health Security and Weapons of Mass Destruction Chapter. Global Health Security, 187–207. https://doi.org/10.1007/978-3-030-23491-1_9.

gains by the proliferators at the cost of death and destruction and focus would be more on vertical than horizontal proliferation, given current trends. For example, China's vertical expansion of its own arsenal does change the security and deterrence calculus of countries like the United States. Further, they shared that WMD proliferation brings home the idea of doomsday. The entire humanity is at stake, not just economy or society; it affects the regional security in short and medium time frame. But in larger interest, WMD proliferation is dangerous for global security. Strategic stability can be disturbed by regional/international geopolitical scenario and can have a cascading influence. China modernising its nuclear forces and increasing the number of warheads will create more asymmetry for India, with a possible fallout for Pakistan. North Korean nuclear capability is creating a rethink in South Korea and Japan. This will translate into a cascading impact on security, economy and society.

**k. What are the options for preventing WMD proliferation? What diplomatic, economic, and military measures can be used to deter and counter proliferation?**

The options for preventing WMD proliferation encompass a range of diplomatic, economic, and military measures. Diplomatically, negotiations and treaties through international cooperation and collaboration, along with the use of diplomatic channels for sanctions, incentives, export controls, and confidence-building measures, are essential for deterring and countering proliferation. Economic measures, such as sanctions, political isolation, International financial measures and support for alternative energy[17] can also play a significant role in preventing WMD proliferation. Additionally, military measures such as conventional deterrence[18], developing and deploying missile defense systems, conducting military operations to disrupt or destroy WMD programs, and enhancing intelligence capabilities and sharing information with allies to monitor and counter proliferation activities are utilized to deter and counter proliferation, with major powers having the capability to prevent the spread of WMDs. It's important to note that these measures need to be pursued simultaneously, and a comprehensive approach involving international norms and institutions is crucial in preventing WMD proliferation.

**l. What are the costs and benefits of different nonproliferation strategies? How can decision-makers weigh the risks and benefits of different strategies to choose the best course of action?**

17 Providing economic and technical support for the development of peaceful nuclear energy programs as an alternative to nuclear weapons programs.

18 Maintaining a strong conventional military posture to deter potential proliferators from believing that WMDs are necessary for their security.

The costs and benefits of different nonproliferation strategies are multifaceted and require careful consideration by decision-makers. Economic measures are often deemed most effective, but they can involve high costs and may not always be cost-effective, particularly when diplomatic relations are at stake.[19] Decision-makers must weigh the financial gains against the high costs involved, as well as the risks of conflict escalation and collateral damage. Additionally, understanding the potential risks of WMD proliferation for companies and institutions is crucial, as it can impact financial and operational aspects, such as technology disruption and reputational damage. In assessing nonproliferation strategies, decision-makers should consider the associated costs, operational risks, and potential for disruption, and take steps to mitigate these risks. It's essential to conduct formal assessments to identify potential WMD proliferation risks and collaborate with other stakeholders to address these challenges effectively.

**m. Are you aware of the potential risks of WMD proliferation for companies and institutions like yours?**

Few of the responding experts asserted their awareness of the potential risks of WMD proliferation for companies and institutions. The risks associated with WMD proliferation include the potential for disruption of supply chains, technology expertise being misused, reputational damage, and economic instability. Additionally, the spread of WMDs can create a threatening environment, disrupt regional stability, and have a significant impact on global security. Understanding these risks is crucial for companies and institutions to assess the potential implications and develop appropriate strategies to mitigate the threats posed by WMD proliferation.

As per the expert's opinion, International collaboration, regimes, national commitments and strict action against proliferators, and time-bound disarmament is the way forward through diplomatic measures, military measures, along with economic sanctions, technology and market access denial regime.

19 Donkervoort, I., & Onderco, M. (2022). The WMD Nonproliferation Clause in EU Trade Agreements. European Foreign Affairs Review, 27(Issue 2), 223–240. https://doi.org/10.54648/EERR2022020;
Grip, L. (2013). The European Parliament and WMD Nonproliferation: Policy-Making Processes and Decision-Making Outcomes. European Foreign Affairs Review, 18(Special Issue), 563–583. https://doi.org/10.54648/EERR2013041.

**n. Have you conducted any formal assessments to identify potential WMD proliferation risks within your organization?**

An organization would typically conduct risk assessments in the following ways: evaluating the security of materials and information that could be used in WMD development; reviewing the background and activities of personnel to prevent insider threats; ensuring compliance with national and international regulations on the handling of sensitive materials and technologies; implementing measures to monitor and control access to sensitive areas and information; establishing protocols for reporting and responding to suspicious activities or security breaches, and international collaboration for information-sharing initiatives. Conducting such assessments helps an organization ensure it is not inadvertently contributing to the global threat posed by WMD proliferation and that it is compliant with legal and ethical standards.

Based on the information provided, it appears that the organizations including the research organisations, universities, and the government agencies has not conducted any formal assessments to identify potential WMD proliferation risks. An expert from NITI Aayog, however, shared that these type of assessment do happen in their institute but most of these assessments are informal in nature. From the responses received, it was noted that the practices highlighted above have not been followed in ensuring the risk assessment for the controlling the WMD proliferation. Further, there has been a lack of due diligence on potential partners, suppliers, or customers to assess their involvement in WMD proliferation activities. Additionally, there is no system for reporting suspicious activities or potential violations of WMD proliferation regulations. It is crucial for organizations to conduct formal assessments to identify potential WMD proliferation risks and develop appropriate strategies to mitigate these threats.

**o. Do you have any policies, procedures, or training programs in place to mitigate these risks? If so, please elaborate.**

Based on the extracted information, it appears that the organization does not have any policies, procedures, or training programs in place to mitigate the risks associated with WMD proliferation. The responses indicate a lack of due diligence on potential partners, suppliers, or customers to assess their involvement in WMD proliferation activities, as well as a lack of a system for reporting suspicious activities or potential violations of WMD proliferation regulations. Additionally, there is no formal assessment conducted to identify potential WMD proliferation risks within the organization. Therefore, it is essential for the organization to

develop comprehensive policies, procedures, and training programs to mitigate these risks and ensure compliance with nonproliferation regulations.

In addition to the mitigation process, due diligence process on potential partners, suppliers, or customers to assess their involvement in WMD proliferation activities was also queried through the questionnaire. Conducting due diligence on potential partners, suppliers, or customers to assess their involvement in WMD proliferation activities is a critical step for companies to ensure compliance with national and international regulations, protect their reputation, and avoid legal and financial risks. According to the information provided, the organization does not conduct due diligence on potential partners, suppliers, or customers to assess their involvement in WMD proliferation activities, except for the expert from Centre for Strategic and International Studies. Most of the responders stated that such type of deligence is not applicable to their respective organisations (mostly educational institutes). This lack of due diligence could pose significant risks to the organization, as it may inadvertently engage with entities involved in WMD proliferation. Due diligence is crucial to ensure compliance with nonproliferation regulations and to mitigate the potential risks associated with WMD proliferation. Therefore, it is imperative for the organization to establish robust due diligence processes to assess the involvement of partners, suppliers, and customers in WMD proliferation activities.

**p. Do you have a system for reporting suspicious activities or potential violations of WMD proliferation regulations?**

Organizations such as National Regulatory Agencies, Law Enforcement and Intelligence Agencies, Military and Defense Departments, International Atomic Energy Agency (IAEA), Organisation for the Prohibition of Chemical Weapons (OPCW), United Nations (UN), International NGOs, Industry and Trade Associations, etc., play crucial roles in the global effort to monitor, report, and mitigate the risks associated with WMD proliferation. Their reporting systems are essential for ensuring compliance with national and international regulations, facilitating intelligence sharing, and enabling coordinated responses to potential threats.

Based on the information received from the experts, the organization does not have a system for reporting suspicious activities or potential violations of WMD proliferation regulations to their governmental authorities. This lack of a reporting system could pose significant risks, as it may hinder the organization's ability to identify and address potential proliferation activities. It is crucial for the organization to establish a formal reporting mechanism to ensure

compliance with nonproliferation regulations and to mitigate the potential risks associated with WMD proliferation.

**q. How concerned are you about the financial risks associated with WMD proliferation, such as sanctions or reputational damage?**

Based on the information provided, the expert highlights the significant financial risks associated with WMD proliferation, including potential sanctions and reputational damage. The financial risks associated with WMD proliferation for companies that export goods and technology are substantial and multifaceted. They include increased compliance and operational costs, potential legal penalties, reputational damage, restricted market access, higher insurance premiums, decreased investor confidence, and loss of business opportunities. Additionally, the responses emphasizes the importance of understanding the potential severe and wide-ranging consequences of WMD proliferation that affect national security and economic stability, regional peace and cooperation, and the broader international order including nuclear brinkmanship, global sanctions, increased defense spending which in turn cause economic and trade disruptions, undermining International treaties and Global governance challenges which in turn affects the International order. Further, mass casualty potential and displacement and refugee crises cause humanitarian consequences of proliferation and development of WMD programs.

In response to the question, the concerns about the financial risks associated with WMD proliferation are substantial. The potential for sanctions, reputational damage, and economic disruption poses significant challenges for companies and institutions. It is crucial for decision-makers to assess and address these risks to mitigate the potential impact of WMD proliferation on financial and operational aspects. Understanding and addressing these concerns is essential for developing effective strategies to prevent and counter WMD proliferation.

**r. How concerned are you about the operational risks, such as disruption of supply chains or damage to facilities, that could result from WMD proliferation?**

Responding experts have highlighted the significant operational risks associated with WMD proliferation, including potential disruption of supply chains and damage to facilities. Experts who have responded to this matter have expressed warning stating that in operating the WMD proliferation tremendous operational risks showing that there are several critical areas that would be most affected. Needs to be cited Supply chain disruptions can be seen as one of the significant concerns due to their deep impact on the possibility of receiving goods and materials. For instance, the measures and limitations applied owing to occurrence or threat

of the usage of WMDs may affect movement and delivery of essential commodities, thereby leading to a slow or hindered delivery process. Pharmaceuticals and medical equipment to food and consumables are among the many sectors that can be disrupted hence leading to disruption of normal business and economic activities in societies.

Similarly, they also stresses on damage to facilities, in this case, the likely to be damaged highly, either as a primary consequence of the use of WMD or as an outcome of related security measures. That hurt could entail the physical erosion of production facilities, research and development facilities, storage depots and distribution centers. It is imperative to note that the consequences of such damage are numerous more than merely the physical loss; they include the possible loss of data and value assets, sites' contamination, and the need for the numerous wipe out and reconstruction. In terms of expenses, especially when many infrastructures are damaged, or the business ceases to function for some time, the expenses for repair or replacement of damaged structures can at times be very high.

These risks can have far-reaching consequences for companies and institutions, impacting their operational capabilities and potentially leading to economic instability and reputational damage. The responses also emphasizes the importance of understanding and addressing these concerns to develop effective strategies to prevent and counter WMD proliferation. Therefore, it is crucial for decision-makers to be highly concerned about these operational risks and to take appropriate measures to mitigate the potential impact of WMD proliferation on their operations.

**s. How concerned are you about the potential for your technology or expertise to be misused for WMD development or proliferation?**

Based on the information provided by the experts, the potential for technology or expertise to be misused for WMD development or proliferation is a significant concern. The experts share that the risks associated with WMD proliferation, including the potential for disruption of supply chains, damage to facilities, and reputational harm for companies and institutions. Additionally, the experts emphasize the importance of understanding and addressing these concerns to develop effective strategies to prevent and counter WMD proliferation. Therefore, decision-makers should be highly concerned about the potential misuse of technology or expertise for WMD development or proliferation and take appropriate measures to mitigate these risks.

**t. How concerned are you about the potential for legal liability if your organization is**

**inadvertently involved in WMD proliferation activities?**

In the context of concerns about potential legal liability related to WMD proliferation activities, it is essential for organizations to have robust compliance measures, risk assessment protocols, and clear policies to prevent inadvertent involvement in such activities. This includes strict adherence to international nonproliferation treaties and regulations, as well as internal controls to prevent the misuse of scientific research for illicit purposes. To address concerns about legal liability, organizations should ensure compliance with international nonproliferation regulations, implement robust ethical oversight mechanisms and provide comprehensive training and awareness programs for researchers, staff, and collaborators to educate them about the risks associated with WMD proliferation and the importance of ethical conduct in scientific research. Conducting thorough risk assessments and due diligence processes to identify and mitigate potential risks associated with research activities, collaborations, and technology transfers is another way of mitigating the risks of any legal liability within any organisation.

Based on the information provided by the experts, the organization does not have policies, procedures, or training programs in place to mitigate the risks associated with WMD proliferation. However, it is important for organizations to take proactive measures to prevent inadvertent involvement in WMD proliferation activities and to demonstrate a strong commitment to ethical conduct and compliance with international regulations. By implementing robust compliance measures and ethical oversight, organizations can mitigate the risk of legal liability and contribute to global efforts to prevent the proliferation of WMDs.

**u. What additional steps do you think companies and institutions should take to mitigate the risks associated with WMD proliferation?**

Companies and institutions should take several additional steps to mitigate the risks associated with WMD proliferation. These steps include:

1. Establishing Robust Due Diligence Processes: Implementing thorough due diligence on potential partners, suppliers, and customers to assess their involvement in WMD proliferation activities is crucial. This can help identify and mitigate potential proliferation risks.
2. Developing Policies, Procedures, and Training Programs: Creating comprehensive policies, procedures, and training programs to mitigate the risks associated with WMD proliferation

is essential. This includes implementing measures to prevent inadvertent involvement in proliferation activities and ensuring compliance with nonproliferation regulations.

3. Implementing Reporting Mechanisms: Establishing a system for reporting suspicious activities or potential violations of WMD proliferation regulations is vital. This allows for the timely identification and addressing of potential proliferation threats.
4. Collaborating with Stakeholders: Engaging in collaboration with other stakeholders, including governments, international organizations, and industry partners, to share best practices and coordinate efforts to prevent and counter WMD proliferation.
5. Assessing Capabilities and Resources: Continuously assessing the capabilities and resources of potential proliferators can help in identifying the most pressing proliferation threats and developing targeted mitigation strategies.
6. Implementing Defensive Protection Measures: Investing in defensive protection measures, such as international collaboration against the spread of WMDs, can help mitigate the risks associated with WMD proliferation.

By taking these additional steps, companies and institutions can enhance their ability to mitigate the risks associated with WMD proliferation and contribute to global efforts to prevent the spread of these dangerous weapons.

**v. How open would your organization be to collaborating with other stakeholders (governments, industry associations, NGOs) to address WMD proliferation challenges? Would you be interested in sharing your experiences and best practices with others in your sector to raise awareness and improve risk management?**

There is no due diligence conducted on potential partners, suppliers, or customers to assess their involvement in WMD proliferation activities, and there is no system for reporting suspicious activities or potential violations of WMD proliferation regulations. Therefore, the organization may not be open to collaborating with other stakeholders to address WMD proliferation challenges or sharing experiences and best practices to improve risk management at this time.

However, it is crucial for organizations to consider collaborating with governments, industry associations, and NGOs to address WMD proliferation challenges. Sharing experiences and best practices with others in the sector can raise awareness and improve risk management. By engaging in collaborative efforts, organizations can contribute to global nonproliferation initiatives and enhance their own capabilities to mitigate the risks associated with WMD proliferation. Therefore, it would be beneficial for the organization to consider being open to

such collaborations in the future to address WMD proliferation challenges effectively.

## Discussion and Conclusions

Experts have highlighted various aspects related to the risks of WMDs, their delivery systems and related materials proliferation for companies and institutions. The risks cover lack of policies, procedures, or training programs to mitigate these risks, the absence of due diligence on potential partners, suppliers, or customers involved in WMD proliferation activities, and the lack of a system for reporting suspicious activities or potential violations of WMD, their delivery systems and related materials proliferation regulations. Moreover, these regulations deals with the issues related to the monetary and the operational risks, possible legal liability, cooperation with stakeholders, and the repercussions of WMD diffusion.

Partnership with governments, industry associations, and NGOs would considerably augment the endeavours to fight and prevent WMD diffusion. Sharing practices and co-operation with other organizations in controlling the WMD, their delivery systems and related materials proliferation is one of the best ways to raise an awareness and improve risk management. Additionally, decision makers need to evaluate the capacities and means of possible proliferators, and predict the results of WMD their delivery systems and related materials proliferation, so they can explore diplomatic, economic and military options to prevent and face this proliferation.[1]

It is also important to consider the societal and global security implications of WMD their delivery systems and related materials proliferation, as well as the potential threats to national survival and economic interests. Decision-makers should weigh the risks and benefits of different nonproliferation strategies and be aware of the potential legal and reputational risks associated with inadvertent involvement in WMD proliferation activities.[2]

Overall, addressing the risks of WMD proliferation requires a comprehensive and collaborative

1 Annawitt, P., & Finaud, M. (2011). Reinforcing Disarmament: Combating Illicit Trade in Weapons and Materials. https://www.sipri.org/sites/default/files/research/disarmament/dualuse/pdf-archive-att/pdfs/un-reinforcing-disarmement-combating-illicit-trade-in-weapons-and-materials.pdf; S. Fisher, C. (1999). Reformation and Resistance: Nongovernmental Organisations and the Future of Nuclear Weapons. The Henry L. Stimson Center. https://stimson.org/wp-content/files/file-attachments/ReformationandResistance_1.pdf.

2 Eilstrup-Sangiovanni, M. (2023). The instability of the nuclear nonproliferation regime complex. Review of International Political Economy, 30(6), 2094–2121. https://doi.org/10.1080/09692290.2023.2238732

approach, proactive risk management strategies, and a deep understanding of the potential consequences and implications for companies and institutions.

Our survey participants do not have a common primary industry either they are researchers, technology professionals, security personnel, or administrators. They do this by providing information that can hint whether the peculiar application of the products or the technologies in a country exist, the motivations for WMD proliferation, the capabilities and resources of potential proliferators, as well as nature of threats postulating the acquisition of WMD, their delivery systems and related materials.

The data set continuation as observed further in the aspect of different objectives of actors involved in WMD programs like deterrence, attrition, or financial gains and the core interests concerned, that most likely to be threatened being national survival or economic interests. Cognizance goes even deeper in current security and counter-attack in the scheme of WMD offence and defence use, the type of weapons bought by actors and their vulnerabilities, and the international circumstances which is fair for proliferation.

The author also analyzed the due diligence performance controlling partnerships to prevent WMD activities involvement, systems for suspicious activities reporting and the hazard of financial, operational, reputational, and legal risks WMD, their delivery systems and related materials spreading. Ultimately, it addressed the concerns on further mitigating risks, readiness to engage with partners, and any other comments or worries related to the risks of WMDs for the companies and the institutions.

Overall, the study proved to be very important as it provided the evidence for WMD proliferation risks for companies and institutions and must be considered by identifying effective risk management strategies, engaging contacts with stakeholders, and acquiring deep knowledge about the range of consequences and likelihood of WMD proliferation. It emphasizes the cruciality of this issue with a holistic and collaborative effort, as such, proactive hazard management strategies, in-depth appreciation of the complexities, and implications of WMD proliferation.

**Acknowledgements**

*We would like to express our sincere gratitude to U.S. CRDF (Grant no. 71022) that supported this research project. Without their generous financial support, this research would not have been possible. We would further like to extend our heartfelt appreciation to all the study respondents who generously dedicated their time and shared their valuable insights. Their willingness to participate was crucial in carrying out this research. We are grateful for their contribution, which has greatly enhanced the quality and impact of this study.*

# In Pursuit of Nuclear Security: Reducing India's Risks to Nuclear Terrorism

Rajeswari Pillai Rajagopalan, Sameer Patil, Shravishtha Ajaykumar, and Prateek Tripathi[1]

## Introduction

Nuclear security concerns have intensified since the end of the Cold War, but these became particularly acute after the 9/11 terrorist attacks on the United States, as Washington grew concerned about the ability of terrorist groups to obtain nuclear and other radioactive materials. Indeed, the nuclear threat is no longer mere fodder for fiction. According to the International Atomic Energy Agency (IAEA), between 1993 and 2023, there were 4,243 incidents of illegal or unauthorised activities involving nuclear and radioactive materials.

Yet, while the world regarded the nuclear threat more seriously in the context of terrorism only after 9/11, India has had such awareness for far longer. For India, the spectre of nuclear terrorism is magnified by Pakistan's nuclear arsenal. This report identifies and evaluates nuclear terrorism threats based on India's counterterrorism experience in the past three decades.

The India-Pakistan relationship is complex and carries enormous historical baggage, fuelling a volatile regional security environment. For India, its nuclear threat perception encompasses a number of plausible scenarios: Pakistan's direct involvement in nuclear terrorism; internal security breaches; and the theft of nuclear materials. While the likelihood of domestic violent non-state actors acquiring nuclear weapons is low, the risks of "dirty bombs" or cyberattacks

1 Rajeswari (Raji) Pillai Rajagopalan is Resident Senior Fellow, Australian Strategic Policy Institute, Australia and former Director, Centre for Security, Strategy & Technology (CSST), Observer Research Foundation (ORF); Sameer Patil is Director, CSST, ORF; Shravishtha Ajaykumar is Associate Fellow, CSST, ORF; Prateek Tripathi is Research Assistant, CSST, ORF.

on nuclear facilities are significant.

Given India's unstable neighbourhood, including beyond Pakistan to the larger South Asian region, India has had to remain vigilant to multiple threats to its nuclear infrastructure. Based on the IAEA's broad principles on nuclear security, India has adopted a risk-reduction strategy involving legal, intelligence, diplomatic, and operational measures. Given the evolving nature of threats, however, this report recommends additional safeguards, such as advanced threat detection, robust security audits, comprehensive trainings, and advanced cybersecurity measures.

Nuclear security became a worrying issue in the early 1990s after the end of the Cold War. That the erstwhile Soviet Union was in possession of thousands of nuclear weapons and a large stockpile of weapons-usable fissile material and was home to a sizeable number of nuclear experts provoked concern. The United States feared that, upon the Soviet Union's fall, its tight internal policing system around its nuclear assets would collapse. This event would then put those weapons, radioactive material, and expertise into the world, including in a nuclear black market where malign actors, whether states or terrorists, could be scouting to purchase them. Compounding the fear was the idea that scientists from the erstwhile Soviet Union themselves could steal nuclear materials and transfer their technical expertise elsewhere. These concerns heightened after the 9/11 terrorist attacks in the U.S., with Washington worrying that terrorist groups could get their hands on such materials.

As per the International Atomic Energy Agency's (IAEA) Incident and Trafficking Database (ITDB), there have been 4,243 incidents of illegal or unauthorised activities involving nuclear and other radioactive material between 1993 and 2023. In 2023 alone, there were 168 incidents based on information provided by IAEA member states. Given large quantities of nuclear materials available worldwide—nearly 2,000 metric tonnes of weapons-usable nuclear material available in 24 countries and in more than 100 facilities—the issue of securing nuclear materials and ensuring that they do not fall into the wrong hands is real. There are also concerns about the more easily accessible but potentially dangerous radiological sources such as Cesium-137, Cobalt-60 and Iridium-192 because of their common applications in areas such as medicine, agriculture, and industry.

The 9/11 terrorist attacks were a watershed event, ushering in a new sense of urgency as the threat of nuclear terrorism emerged. That the al-Qaeda leader Osama Bin Laden made a proclamation stating that the procurement and use of weapons of mass destruction (WMDs) was his "Islamic duty" exacerbated the situation. Many nations perceived the acquisition of nuclear devices by terrorist organisations and other violent non-state actors to be the single greatest threat to humanity's existence.

The threat persists, even as the return of great-power politics is beginning to mask the danger

from terrorism, overall, and nuclear terrorism, in particular. Indeed, in the aftermath of U.S. withdrawal from Afghanistan in 2021 and the growth of extremism in West Asia, the threat of nuclear terrorism is growing. The implications of this growing threat are yet to be fully recognised.

For India, the threat of nuclear terrorism raised concerns, especially with its rising prominence in South Asia, and given nuclear-armed Pakistan's deep linkages with pan-Islamic terrorist organisations and the anti-India terrorist groups in particular. While India has experienced the threat of cross-border terrorist attacks from Pakistan-based terrorist organisations for decades, the nuclear tests of 1998 added a new dimension to the threat. Faced with much superior Indian conventional military capabilities and the fears of nuclear escalation, Pakistan amplified the low-intensity conflict against India by utilising terrorist organisations like the Lashkar-e-Tayyaba (LeT) and Jaish-e-Mohammed (JeM). American scholar Christine Fair describes this Pakistani policy as "jihad under the nuclear umbrella." The spate of terrorist attacks by these organisations against Indian government, military, and civilian targets in the late 1990s and early 2000s demonstrated Pakistan's use of this tactic. In 2008, the violence would culminate in the Mumbai terrorist attacks which targeted multiple locations and killed 174 people.

The close linkages of these terrorist organisations with the Pakistani military establishment led to speculations and concerns over nuclear terrorism wherein India could face five distinct nuclear terrorism threat scenarios, outlined in the following points:

- Pakistan providing nuclear weapons to terrorist groups as a matter of state policy (authorised transfer)

- Sections of the Pakistani establishment or rogue elements within engaging in the transfer of technology and/or radiological materials in contravention of formal state policy or without necessary approvals from the highest political authorities (unauthorised transfer

- Terrorists stealing nuclear materials without any support from state actors (theft)

- Pakistani state/rogue actors' support for terrorist actions against Indian facilities that could include nuclear power plants and other nuclear establishments, including through cyberattacks against power plants and other parts of nuclear establishment, causing disruption, chaos, or even deaths.

- Attempts to acquire nuclear materials in India, including intelligence support and other

types of support from Pakistan to keep its own role hidden

- Furthermore, two closed-door discussions conducted by the authors of this report with Indian stakeholders[2] suggested two additional threat scenarios:
- Use of nuclear and radiological materials by other state actors who have inimical interests towards India
- Domestic terrorism by Indian insurgents, including Naxalites or left-wing extremists

This report aims to identify and evaluate the nuclear terrorism threats that confront India. While there is literature on terrorism in India, and South Asia in general, it fails to effectively evaluate the elements of the nuclear terrorism threat.

This report thus identifies nuclear terrorism threats that can arise from India's neighbourhood as well as from within the country and ranks them in terms of the degree of likelihood.[3] The report will first examine Indian nuclear security in general, then gauge specific kinds of nuclear terrorism-related threats faced by India, while ranking them according to the relative danger they pose. Subsequently, the report will outline steps India has taken to counter these threats and conclude with specific, targeted measures that India can take to mitigate them.

This report benefitted from two closed-door focused group discussions convened by the Observer Research Foundation (ORF) with representatives of India's national security establishment, the Department of Atomic Energy (DAE), and members of academia, civil society, and the Indian strategic community. In an effort to rank nuclear terrorism threats, the authors of this report also conducted an online survey among the relevant stakeholders. The survey questionnaire aimed to yield more objective insights on the subject, but the ranking is done not merely on the basis of the survey results but also extensive discussions with the Indian atomic energy and security officials. The survey and its findings are appended to this report.

## India's Nuclear Security Posture Review

Situated between two nuclear neighbours—Pakistan and China—nuclear security has been a priority for India, especially as it has not had an easy and peaceful relationship with these two

2 These discussions were held in hybrid format on February 26, 2024 and June 6, 2024.

3 Nuclear terrorism threats were identified following extensive discussions with security and atomic energy officials, including through two closed-door focused group discussions held earlier in the year.

neighbours. Of the two, India perceives a distinct threat from Pakistan because of the existence of terrorist organisations like the LeT and JeM and the Pakistani Army's deep links with pan-Islamic terrorist organisations like al-Qaeda. China, meanwhile, exacerbates Indian concerns regarding the competing influence in this strategic region. Moreover, China's pivotal role in bolstering Pakistani nuclear capabilities and propping up north-eastern insurgent groups[4] in the past have had profound implications for regional stability. Despite its international commitments to nuclear nonproliferation, China has provided extensive nuclear assistance to Pakistan, including technology transfers and material support, enabling the rapid expansion of its nuclear arsenal.

This assistance, coupled with Pakistan's strategic focus on tactical nuclear weapons, poses challenges for India and upends regional stability. New Delhi views with concern the growing economic and military partnership between China and Pakistan, particularly amid initiatives like the China-Pakistan Economic Corridor. This close cooperation between Islamabad and Beijing has also shaped India's threat perception.

Through the 1998 Pokhran nuclear tests, known as Operation Shakti, India demonstrated its nuclear capabilities and sought to deter potential nuclear threats, particularly from Pakistan and China. Following the tests, India developed and formalised its nuclear doctrine, which adhered to a "No First Use" policy and emphasised a "credible minimum deterrence posture" while underscoring the country's commitment to massive retaliation if any WMD, including tactical nuclear weapons, are used against it.

Pakistan responded with its own round of nuclear tests in the same year, beginning the nuclearisation of South Asia. This escalation elevated the importance of nuclear weapons and their potential threats for India, including in terms of crisis management. The 1998 nuclear tests by both India and Pakistan marked a turning point in the overall security dynamics in the region. For India, it meant there was a need to develop a more nuanced and sophisticated approach to nuclear threat assessment and balancing.

India has continued to view nuclear weapons as a deterrent tool; yet, the possibility of use still exists. Nevertheless, recognising the unparalleled negative consequences of nuclear use, India has behaved in a responsible manner. It has improved its nuclear material safety and security at both national and global levels, tightened national legal architecture, and participated in global efforts such as the Nuclear Security Summits. It is also signatory to a number

4 China has previously supported groups such as the Naga National Council and Mizo National Front. See: Obja Borah Hazarika and Chandan Kumar Sarma, "The "China Factor" in the Northeast Component of India's Act East Policy: Implications for Security, Connectivity, Commerce," *International Journal of China Studies* 13, no. 1 (2022), https://ics.um.edu.my/img/files/IJCSV13N1/IJCS%20V13N1-03-Obja-Chandan.pdf.

of international instruments that address global nuclear proliferation and nuclear security governance. One such agreement is the International Convention for the Suppression of Acts of Nuclear Terrorism (Convention on Nuclear Terrorism or CNT), adopted by the United Nations General Assembly on 13 April 2005. The convention declares nuclear terrorism as a crime under international law. Further, India is party to the United Nations Security Council Resolution 1540, that disallows state support to non-state actors in building, stockpiling, or trading weaponisable material, including radioactive materials; it exhorts member states to establishes stringent national regulations aimed at preventing the proliferation of these weapons and their delivery systems, especially in the context of nuclear terrorism.

Pakistan, meanwhile, has continued to use non-state actors and terrorist groups to further its political objectives vis-à-vis India. Just a few months after both countries went nuclear, Pakistan initiated the Kargil war in May 1999. This limited war was accompanied by veiled threats on the use of nuclear weapons against India and underscored the need for India to respond to Pakistan's provocations while ensuring that its actions did not contribute to nuclear escalation. Further, the 2008 Mumbai terrorist attacks, carried out by ten LeT members, along with other terrorist attacks,[5] forced India to review its threat assessment. The concern was that terrorist groups, especially those based in Pakistan, with support from its military establishment, could attempt to strike nuclear facilities and/or acquire nuclear and radioactive materials.

The worry was not unfounded. The Mumbai terrorist attacks in November 2008, for example, left the Indian nuclear establishment untouched but has been found to have been executed with the involvement of Pakistan's intelligence services, the ISI. Police interrogation reports, cited by the media, revealed the key role played by ISI in engaging figures like David Coleman Headley[6] in plotting the Mumbai attacks. Similarly, the India head of the terrorist group Indian Mujahideen, Ahmad Zarar Siddibappa alias Yasin Bhatkal, in 2013 claimed that he was "planning to set off a nuclear bomb in Surat." During the National Investigative Agency (NIA) investigation, Yasin Bhatkal reportedly said that he had asked his superior, Riyaz Bhatkal, who was Pakistan-based, whether he "could arrange a small 'nuclear bomb'." Riyaz reportedly responded, "Anything can be arranged in Pakistan."

Further, Bhatkal was arrested in Nepal in August 2013, which indicates the pervasiveness of

5 In the 2000s, LeT carried out a series of serial blasts in various India cities including the October 2005 pre-Diwali blasts in Delhi and the July 2006 Mumbai suburban train bombings. See: Arun Vishwanathan and Sameer Patil, "Lashkar-e-Taiba (LeT)," in *Handbook of Terrorist and Insurgent Groups: A Global Survey of Threats, Tactics, and Characteristics*, ed. Scott N. Romaniuk, Animesh Roul, Amparo Pamela Fabe, János Besenyő (Boca Raton: CRC Press, Forthcoming).

6 American terrorist who worked for the LeT.

and linkages of terrorism across South Asia. Even though his plans did not fructify, Bhatkal's confession is revealing of the interest and inclination of these terrorist groups and the linkages within Pakistan. Each of these terrorist attacks have shaped India's threat perception in the context of nuclear security, which in turn have framed New Delhi's overall approach to broader nuclear strategy and nuclear security in particular.

According to the IAEA, the quantity of nuclear material required to build a nuclear bomb is 8 kg for plutonium and 25 kg for Highly Enriched Uranium (HEU). Only 22 countries possess such weapons-grade nuclear materials, and India is one of them. As of 2023, India is estimated to possess about 164 nuclear weapons. Additionally, it has 22 nuclear reactors currently in operation, which produce large amounts of radioactive nuclear waste (spent fuel), with some even producing weapons-grade nuclear material. India is among only five countries employing a plutonium fuel cycle in its nuclear reactors. There are more than 7,000 "radiation facilities" in the country, including institutions using radiation sources or radiation-generating equipment for industrial, research, medical, consumer products, and scanning facilities. These radioactive materials require security.

## Nuclear Terrorism and India: A Threat Analysis

Mike Mullen, former chairman of the joint chiefs of staff of the U.S., once described the LeT as Pakistan's "proxy". LeT, JeM, and other organisations have received extensive support from the Pakistani security establishment in executing terrorist attacks against India. These attacks have also brought both countries to the verge of direct military conflict. American scholar Daniel Markey has stated that if there was any single terrorist organisation in Pakistan most likely to provoke an all-out war with India, it is the LeT.

It has not helped that Pakistan has historically resisted international counterterrorism efforts, especially with respect to the UN's attempts to address the issue of terrorism emanating from Pakistan's borders. Pakistan has also found an ally in China to support its agenda as far as non-cooperation on terrorist groups is concerned. China has repeatedly prevented the United Nations from acting against terrorists sheltered in Pakistan. In addition to Pakistan's close links to terrorist groups, the current domestic troubles fermenting political, economic, and social instability are particular cause for concern.

### Threat Actors

It is in this context that the threat of nuclear terrorism has come to the forefront for India, wherein the security establishment is concerned that there are various scenarios of how the threat of nuclear terrorism may turn out. This may manifest in the form of rogue elements in

states like Pakistan, which have historically harboured terrorist groups, providing technical know-how, radiological materials and other forms of support.

As far as India is concerned, there are two additional scenarios. The first is the possibility of terrorists acquiring or crafting a nuclear bomb and detonating it in a major city. This is potentially the most catastrophic scenario. In the past, terrorists have considered carrying out terrorist attacks in India by detonating nuclear bombs. For instance, in 2013, as mentioned earlier, Yasin Bhatkal attempted to procure a nuclear bomb from Pakistan through an associate of his based in Pakistan, which then he disclosed to Indian interrogators that he intended to detonate a nuclear bomb. The Pakistani associate had confirmed that "Anything can be arranged in Pakistan". While this threat did not materialise, these are examples of attempts made by and intentions of terrorist groups to acquire nuclear material to carry out a terrorist attack with a nuclear device .

The second is the employment of a 'dirty bomb' or Radiological Dispersal Device (RDD), which, though not as destructive as a nuclear bomb, is still capable of causing massive damage; it is also easier to acquire, assemble, and possibly even deploy. The Indian security establishment considers both scenarios plausible.

The threat of nuclear terrorism, therefore, arises from two types of actors: external and internal.

## External Threats

External threats include those emanating from outside India, mainly from terrorist organisations that could infiltrate the country's nuclear systems (or those of its neighbours) and execute a nuclear/radiological attack on Indian soil. As discussed earlier in this report, India's geographical proximity to Pakistan, with whom it has a strained political relationship, has long put it at constant risk of terrorist activity. Among the terrorist groups, al-Qaeda, Islamic State, Tehreek-e-Taliban-e-Pakistan (TTP), LeT and JeM stand out with the greatest potential to harness nuclear capabilities. Understanding the nature of these threats is imperative for crafting effective counter-strategies to safeguard India's nuclear facilities and broader security.

The TTP, a militant organisation operating in the volatile regions of Pakistan and Afghanistan, is not necessarily an anti-India terror outfit, but the TTP's potential access to nuclear materials in Pakistan could pose a threat to South Asia and possibly escalate tensions in the region and beyond. However, a much more serious threat emanates from the LeT and JeM, which have consistently carried out attacks against Indian targets—military, government, and civilian. Both organisations have a well-documented anti-India agenda and possess sophisticated operational capabilities, making them alarming adversaries.

LeT, founded by Hafiz Saeed, is one of the most dangerous terrorist organisations operating in the region. LeT is responsible for numerous high-profile attacks in India, including the 2008 Mumbai attacks. LeT's operations are characterised by meticulous planning, coordinated execution, and the use of well-trained militants. The group's objectives include the "liberation" of Kashmir from Indian control and the establishment of an Islamic state in the region governed by Sharia law. LeT has also demonstrated the capability to strike at strategic locations, underscoring the gravity of the threat it poses to national security.

JeM was founded by Masood Azhar with the explicit aim of fighting against Indian interests. It, too, has been involved in numerous attacks against Indian military and civilian targets. Notably, the group claimed responsibility for the 2001 attack on the Indian Parliament, which brought India and Pakistan to the brink of war. More recently, in 2019, JeM orchestrated the Pulwama attack, in which a suicide bomber targeted a convoy carrying Indian paramilitary personnel and killed 40 of them near Lethpora on the Jammu–Srinagar National Highway, leading to an escalation in India-Pakistan tensions. JeM's sophisticated operational tactics, including the use of suicide bombings and armed assaults, pose a severe threat to India's security. The group focuses on high-impact targets to demonstrate its offensive capabilities that have the potential to destabilise regional security.

Both groups have had extensive support from the Pakistani establishment for its anti-India activities. Both LeT and JeM benefit from a support network that includes financial resources, training camps, and logistical assistance. This support is often traced back to elements within Pakistan, adding a layer of complexity to India's counterterrorism efforts.

## Internal Threats

While external threats pose a significant risk for India, there is also an internal dimension for India that includes Left Wing Extremists (LWE), north-eastern insurgent groups, and radicalised individuals indoctrinated by extremist propaganda—what Indian law enforcement agencies call "lone wolves".

The LWE represents a different category of internal threat rooted in Maoist insurgency and rural discontent. They focus on socio-economic grievances and armed struggle against the Indian state. However, the Naxalites'[7] propensity for violence, along with their anti-nuclear stance, cannot be overlooked in the context of nuclear security risks. Interviews with senior police officials in Jodhpur, Rajasthan, in April 2014,[8] indicated that there are some indications

7 Referring to the Maoist motivated militant insurgency groups.

8 Interviews with senior police officials by one of the authors on nuclear security in India as part of an earlier study on the same subject, Jodhpur, Rajasthan, April 14, 2014. The information was further corroborated

of Naxalites showing interest in attacking Indian nuclear installations, but these claims could not be corroborated. The same interviews indicated that it was possible that Naxals could join hands with jihadists under an anti-India platform, but this too has not fructified. However, given the severity of any nuclear or radiological incident, the threat from left-wing extremism is treated with a certain seriousness.

The north-eastern insurgent groups are also part of the internal threat matrix. While the insurgency has largely been on the decline, except for the recent unrest in Manipur, it does figure in the Indian threat calculus, given China's past linkages with these groups. Though Beijing has not employed these insurgent groups against India for a while, it has kept its options open and has several instruments available.

Similarly, India appears to be "immune" to the "lone wolves" phenomenon. In recent years, however, Indian law enforcement agencies have made several arrests of lone wolves who branch from radicalised civilian groups. These are individuals who have been radicalised through online social media platforms, encrypted chat rooms on the darknet, and propaganda on instant messaging apps. While it is hard to get hold of definite information on such activities, these radicalised individuals still pose a threat to the security of India's nuclear infrastructure. This can be particularly true in the case of insider threats, where such radicalised individuals can engage in acts of sabotage. There also exists the possibility of an insider (a lone wolf)-outsider joining hands in a sabotage or other nuclear incident. While not directly related to the lone wolves phenomenon, the Kaiga incident in 2009 demonstrates the potential of such acts. In this instance, a disgruntled employee at the Kaiga Atomic Power Station in Karnataka was reportedly responsible for contaminating the drinking water supply with heavy water from the plant, which led to 45 employees being poisoned. Given such instances, security managers have to examine all potential scenarios when it comes to safeguarding the nuclear plants. These dynamics pose a challenge to nuclear security.

At the closed-door focused group discussion organised by ORF, there was broad consensus that terrorist organisations in India do not seem to possess the technical competence to engage in nuclear terrorism. Historically, they have not been technically proficient or employed anything beyond "simple" explosives. As against this view, some other participants argued that terrorist organisations do indeed have the capacity to engage in nuclear terrorism. They pointed out that the use of drones by terrorist organisations like Hezbollah and Houthi rebels proves that recent technological advances have a lower entry barrier, and therefore non-state

---

most recently in July 2024 and there is still no confirmation of Naxalites' interest in nuclear weapons. In fact, given that the left-wing violence has gone down significantly in recent years, it is unlikely that the Naxals will resort to nuclear weapons.

actors could gain such technical proficiency easily. This has the potential to pose severe challenges to national security establishments worldwide in the future. Aerial and cyber threats to nuclear facilities are within the realm of possibility in terms of incidents because both these technologies are easily accessible and there are no foolproof countermeasures against them.

Table 1: Threats and Plausible Outcomes

| Threat | Risk of Manifestation |
|---|---|
| **External Threats** | |
| **Terrorist Organisations** | **- Nuclear/Radiological Attack:** These organisations could infiltrate India's or its neighbours' nuclear systems and execute attacks.<br>**- LeT & JeM:** Consistently targets India, carrying out high-profile attacks like the 2008 Mumbai attacks and the 2019 Pulwama attack. These groups possess sophisticated operational capabilities.<br>**- State-Sponsored Terrorism:** Support from elements within Pakistan enhances their threat to Indian security. |
| **Regional Geopolitical Tensions** | **- Escalation Risk:** Proximity to Pakistan and strained political relations increase the risk of conflict, with potential involvement of nuclear materials.<br>**- State-Sponsored Supply:** Historical reporting of suspicious actors in Pakistan might sell nuclear materials to terrorists due to internal conflict, posing a direct threat. |
| **Nuclear Smuggling** | **-Trafficking during Transportation:** There is a high likelihood of nuclear/radiological materials being intercepted during transport, leading to smuggling or terrorist acquisition. |

| | |
|---|---|
| **Cyber Threats** | **-Cyberattacks on Nuclear Facilities:** Non-state actors could use cyberattacks to disrupt nuclear operations, steal sensitive data, or sabotage systems, as seen in the 2019 Kudankulam incident.<br>**- AI-Enabled Attacks:** State-sponsored actors could target India's nuclear infrastructure through advanced cyber means. |
| **Coastal Security Threats** | **- Infiltration via Sea:** Nuclear facilities along the coast are vulnerable to attacks from small boats or drones, as demonstrated by the 2008 Mumbai attacks. |
| **Internal Threats** | |
| **Left Wing Extremists (LWE)** | **- Anti-Nuclear Stance:** Potential interest in attacking nuclear installations as part of their broader anti-state agenda.<br>**- Potential Alliances:** Cooperation with jihadist groups is possible under an anti-India platform, although this remains unconfirmed. |
| **North-Eastern Insurgent Groups** | **- Historical Links with China:** Though insurgency is declining, past linkages with China pose a potential threat.<br>**- Vulnerability during Unrest:** Any resurgence in unrest, like the recent events in Manipur, could exacerbate this threat. |
| **Lone Wolves** | **- Insider Sabotage:** Radicalized individuals could infiltrate nuclear facilities and engage in sabotage.<br>**-Collaboration with Outsiders:** There is potential for insider-outsider collaboration in attacks, similar to the 2009 Kaiga incident, in which a disgruntled employee poisoned water at a nuclear facility. |
| **Orphaned Radioactive Sources** | **- Sabotage & Accidents:** Mishandling or deliberate use of orphaned sources, as seen in the 2010 Mayapuri incident, could lead to radiological incidents. |

| | |
|---|---|
| **Fear Mongering with Misinformation** | **-Mass Panic:** Terrorist organisations might detonate conventional explosives and falsely claim it was a nuclear device, causing widespread panic and chaos. |

## Current Regional Dynamics and Threat Scenarios

India appears to be in a "sweet spot", with no mass-casualty attacks on Indian soil since Pulwama in 2019. This is in contrast to a decade ago, when terrorist incidents within the country were commonplace across a variety of targets. However, as indicated by the recent spike in terrorist violence in the Jammu region, this should not result in complacency. Additionally, the October 2023 Hamas raid on Israel is proof that scenarios that were earlier considered improbable could materialise. The likelihood of the resurgence of a terrorist organisation is increasing daily. In addition, the possible activation of sleeper cells within India cannot be ignored. The same argument applies to nuclear terrorism.

In the focused group discussion organised by ORF, there was discussion around the possible state-sponsored supply of nuclear material to terrorist groups. With Pakistan embroiled in internal conflict, personnel working at nuclear establishments may sell nuclear and/or radiological material to terrorist organisations. In contrast, in India, where nuclear installations are heavily guarded, the likelihood of a breach is relatively low.[9] Additionally, Indian installations have robust and multifaceted accounting mechanisms. The surveillance and technologies that are employed in case of an intrusion enable even less than one microgram of nuclear material can now be tracked. However, the radicalisation of insider elements remains the obvious challenge.

Indian nuclear weapons are stored in a de-mated form, with different components, like the delivery system and nuclear warhead, stored separately at various locations. This makes their assembly especially difficult. Therefore, even if a terrorist organisation acquires one or more of these components, they would not be usable in isolation. Additionally, the detonation technique for nuclear weapons is highly sophisticated, and there is no evidence that even

9 This is a sharp context because of many vulnerabilities and failures that analysts attribute to Pakistan's security establishment. For instance, Shaun Gregory in a report said, "the vulnerabilities within Pakistan's nuclear safety and security arrangements mean that the risks of terrorist groups gaining access to nuclear materials are real. Moreover, militants have recently attacked a number of Pakistan's nuclear facilities, including an August 21, 2008 incident at the Wah cantonment, widely understood to be one of Pakistan's main nuclear weapons assembly sites." For details, see Shaun Gregory, "The Terrorist Threat to Pakistan's Nuclear Weapons," CTC Sentinel, Vol 2 Issue 7, July 2009, https://ctc.westpoint.edu/the-terrorist-threat-to-pakistans-nuclear-weapons/

organisations like al-Qaeda possess the necessary technical prowess.

Sabotage is much more feasible during the transportation of nuclear material. Radiological material, which is transported for uses in the agriculture and pharmaceutical industry, presents an added threat. The possibility of these materials being intercepted by traffickers during transportation is high. This has given rise to fears of nuclear smuggling. There were 168 incidents of illegal and unauthorised activities involving nuclear and radioactive materials in 2023 alone, six of which were related to trafficking or malicious use of radioactive material. About 52 percent of all these incidents over the period of 1993-2023 occurred during the authorised transport of these materials. In the past decade, this figure rose to 65 percent. This makes nuclear material transport a key challenge in the context of nuclear security.

Nuclear smuggling has been a persistent issue for decades. Terrorist organisations and other non-state actors may seek to exploit existing smuggling networks or to establish their own networks to acquire fissile material or other nuclear-related items. Nuclear smuggling incidents, such as the case of the Nuclear Wal-Mart network led by Pakistani nuclear scientist A.Q. Khan, underscore the persistent threat posed by illicit trafficking networks.

An additional scenario that needs attention is the threat posed by orphaned sources, which can be utilised for sabotage or can cause a radiation incident. The Mayapuri incident in New Delhi in 2010[10] exemplifies how mishandling orphaned sources like Cobalt-60 could have severe consequences. This challenge is not unique to India, though. Globally, there have been several incidents involving orphaned sources. Therefore, it would be beneficial to develop improved technology for the minor or trace detection of radioactive materials.

Another possible scenario that was debated in the focused group discussion was the bluff of a "nuclear bomb". A terrorist organisation could detonate a regular explosive and claim that it was a nuclear device. Though this tactic has not been employed so far, it is the simplest to execute since it does not require an actual nuclear weapon or RDD but could create mass hysteria and panic. RDDs also do not create a nuclear explosion but spread radioactive material over a wide area upon detonation, causing fear, contamination, and potentially long-term health and environmental consequences. Extremist groups may view RDDs as more accessible alternatives to nuclear weapons, as they require less sophisticated technology and materials while causing significant psychological impact and disruption.

Another dimension of the nuclear threat is the vulnerability of nuclear facilities installed along the Indian coast, which could be potentially infiltrated using small boats or drones carrying

10 In this incident, eight people were injured and one died after they were exposed to high radiation due to mistakes in handling radioactive material. The material in question - a research irradiator, belonged to the Delhi University and was sold to a scrap-metal dealer. He dismantled it, unaware of the hazard, causing radiation.

explosives or RDDs. The incursion by sea that was executed by LeT terrorists during the 2008 Mumbai terrorist attacks underlined the importance of coastal security. Therefore, there is a need for a greater degree of vigilance around coastal areas.

Another concerning area in recent years is cybersecurity in nuclear installations. The cyberattack on India's largest nuclear reactor in Kudankulam in September 2019 exemplifies the danger posed by the lack of a robust cybersecurity infrastructure. Although the breach affected administrative systems and did not penetrate classified systems that controlled the operations of the nuclear plant, it demonstrated the vulnerability of the nuclear infrastructure to cyberattacks.

The Russia-Ukraine War has also highlighted the threat posed by AI-enabled cyberattacks. State-sponsored non-state actors with advanced cyber capabilities could target India's nuclear infrastructure to disrupt operations, compromise sensitive data, or gain unauthorised access to critical systems. Non-state actors, including terrorist organisations and hacker groups, also pose cyber threats. These groups may lack the extensive resources of state actors, but they do not require large resources to execute sophisticated cyberattacks.

Attackers might employ advanced persistent threats to establish long-term presence within targeted systems to conduct surveillance and extract data. Phishing, social engineering, and exploiting software vulnerabilities are common tactics used to gain initial access. Once inside, attackers can deploy malware that is designed to disrupt Industrial Control Systems or Supervisory Control and Data Acquisition (SCADA) systems that manage nuclear operations. Cyberattacks can also provide another avenue for blackmailing or radicalising employees within nuclear installations.

Based on the above overview, this study identifies three kinds of threat scenarios as likely vis-à-vis nuclear terrorism: insider threat, cyberattacks, and use of orphaned sources. All of these scenarios could be utilised by terrorist organisations and other violent non-state actors to sabotage and engage in nuclear terrorism targeting India. In addition, even if the terrorist organisations are unable to engage in violence by utilising the above scenarios, they could detonate explosive devices and claim it was a nuclear device to create mass hysteria and panic.

Due to the easy and affordable access to cyber warfare, the authors rank this as having the highest probability of threat to nuclear security. A close second is insider threats, which can arise from cybersecurity breaches or through radicalisation. Orphaned sources are ranked third.

## Countermeasures Implemented by India

Addressing the nuclear threat posed by terrorist organisations requires a multifaceted and robust nuclear security approach that includes legal measures, intelligence sharing, counterterrorism operations, diplomatic collaborations, and global commitments. Furthermore, strengthening nuclear security measures, including securing fissile materials, enhancing export controls, securing physical borders, and bolstering safeguards against illicit trafficking, are necessary steps to prevent terrorist organisations and other violent non-state actors from acquiring nuclear capabilities. This requires close collaboration among different stakeholders within the government establishment, international organisations, and other stakeholders such as industries and civil society.

Table 2: An Overview of Countermeasures deployed by India

| | **Description** |
|---|---|
| **Risk Reduction Approach** | India employs a multi-layered risk reduction strategy that draws from the IAEA's suggestions and includes deterrence, robust security protocols, and continuous risk assessments to minimise the likelihood of nuclear or radiological incidents. The approach involves a combination of effective governance, national legal frameworks, and the establishment of appropriate institutions, all while adhering to international legal obligations to ensure comprehensive nuclear security. |
| **Regulatory Tools** | India has comprehensive laws governing nuclear safety and security, as summarised in Table 3. These laws provide the legal basis for controlling nuclear materials and ensuring safe practices in nuclear operations. This framework includes regulatory and oversight institutions like the Atomic Energy Regulatory Board (AERB), which enforces safety standards across different nuclear facilities and streamlines licensing processes through a digital platform called eLora (e-Licensing of Radiation Applications). |

| | |
|---|---|
| **Security and Intelligence** | India's nuclear facilities are protected by a combination of military units, such as the Central Industrial Security Force (CISF), and intelligence agencies like the Research and Analysis Wing (RAW), ensuring a high level of security. |
| **Nuclear Facilities with Secure Designs** | India's nuclear installations are designed with multiple safety and security layers, including physical barriers and access controls that protect against sabotage and unauthorised access. |
| **Emergency Response Systems** | India has developed comprehensive emergency response protocols that involve coordination between local, state, and national agencies, including specialised units for rapid response to nuclear or radiological emergencies. |
| **Technological Innovations** | India invests in advanced technologies such as radiation detection systems, surveillance technologies, and AI-enabled cybersecurity measures to enhance the protection and monitoring of nuclear facilities and materials. |
| **Insider Threat Detection** | India's nuclear sector employs stringent vetting processes, continuous monitoring, and psychological assessments to detect and mitigate insider threats, with particular attention to the potential radicalisation of personnel. |
| **Monitoring of Other Radiological Sources** | Beyond nuclear facilities, India monitors other radiological sources, such as those used in medical, industrial, and research settings, to prevent their misuse or accidental release, ensuring a comprehensive approach to radiological safety. |
| **Public Awareness** | Public education campaigns and community engagement are part of India's approach to increasing awareness of nuclear safety, emergency preparedness, and the risks associated with radiological materials. |

| | |
|---|---|
| **International Perceptions** | India actively engages with international bodies such as the IAEA. It adheres to global nonproliferation norms to maintain and enhance its reputation as a responsible nuclear state, aiding diplomatic and security efforts. |

## Risk-Reduction Approach

India has adopted a 'risk reduction' approach to nuclear security, whereby attempts are made to bring the risks down to an acceptable level. The IAEA's "risk informed approach to nuclear security measures" has influenced this three-tier strategy:

1. The first tier involves physical protection measures for nuclear and radioactive materials, in addition to material accountability, which is provided in all nuclear facilities, including during their transport, in all life-cycle phases. Technology, especially surveillance and databasing tools, plays an essential role in this. India has invested in and developed these technologies indigenously. For instance, India can account for sensitive and strategic materials like plutonium and uranium up to an accuracy of almost a milligram.[11] There are also other technologies and access control mechanisms, both physical, such as spike strips and cement/steel barriers, as well as technology-aided, such as biometric systems, that have been implemented to help delay access to the core of a facility in case of a security breach.[12] Such measures and technologies provide security personnel in a facility some lead time to take control of a situation while calling for external assistance.

2. The second tier involves the detection of any material that has left regulatory control. Extending from the first tier of physical protections, the access and control systems help Indian authorities detect any material that is unaccounted for. Additionally, to be able to detect such material, inter-agency cooperation is important, and such preparedness requires the involvement of security forces.

3. The third tier uses security forces to respond to a potential emergency. The Central Industrial

11 Information confirmed by former Indian Department of Atomic Energy officials at the Focused Group Discussions held on June 6, 2024.

12 Based on interviews with senior police officers posted in nuclear establishments in Maharashtra, February 18, 2014. These have been further corroborated with senior Indian Police officials during interactions in Delhi in July 2024.

Security Force (CISF) is one such organisation, which holds regular drills to prepare for emergencies on material loss and detection as well as potential disasters, including the appropriate steps to be taken in case any such material enters the public domain accidentally or through intentional attacks.

## Legislative Framework

The three-tier approach is implemented through effective governance, national legal frameworks, and the establishment of appropriate institutions, alongside adhering to international legal obligations. The Atomic Energy Act of 1962 serves as the umbrella legislation and provides the legal framework for all aspects of developing nuclear and radiation technologies, including their security. Rules and guidelines issued under this Act form the backbone of India's framework for governing nuclear activities. The legislation also authorises the central government to establish rules and regulations and release periodic notifications to execute the provisions of this Act.

Since its implementation, the Act has undergone amendments to strengthen the legal basis for India's nuclear security measures. Legislation concerning environmental issues—among others—has also been critical in determining the location and operation of nuclear power plants. These include the Environment (Protection) Act, 1986; the Atomic Energy (Factories) Rules, 1996; and the Electricity Act, 2003. The DAE also formulated the Guidelines for Nuclear Transfers (Exports) in 2006. Key legislation introduced under the Atomic Energy Act include the Atomic Energy (Radiation Protection) Rules 1971 (further revised in 2004); the Atomic Energy (Working of the Mines, Minerals and Handling of Prescribed Substances) Rules 1984; and the Atomic Energy (Safe Disposal of Radioactive Wastes) Rules 1987.

The Atomic Energy (Radiation Protection) Rules sanction activities for nuclear fuel cycle facilities and radiation use in industry, medicine and research. After its revision in 2004, the Rules are more comprehensive and clearly set out the roles and responsibilities of different parties, including employers and Radiological Safety Officers, in protecting against radiation. The rules also clearly identify the powers and roles of the Atomic Energy Regulatory Board (AERB), detailing requirements in areas such as safety, health surveillance of workers, radiation surveillance and records, directives, inspections, and enforcement actions. The Radiological Safety Division of the AERB is mandated to ensure compliance with the 2004 Radiation Protection Rules and the 1987 Atomic Energy (Safe Disposal of Radioactive Wastes) Rules and institute parameters for the decommissioning and disposal of radioactive waste. The provisions in the 1987 Rules lay out the responsibility on the AERB in ensuring that the licensees comply with their responsibilities regarding the safe disposal of radioactive waste. The Atomic Energy (Working of the Mines, Minerals and Handling of Prescribed

Substances) Rules, 1984, are responsible for regulating the mining, processing, and handling of prescribed substances.

Other legal instruments have been formulated or augmented with amendments to strengthen nuclear security policy. For example, the Unlawful Activities (Prevention) Act 1967, amended in 2012 now includes terrorist activities already defined under several treaties, including the Convention on the Physical Protection of Nuclear Material (CPPNM) and the International Convention for Suppression of Acts of Nuclear Terrorism (2005). The Act also incorporates U.S.C Resolution 1373, which obliges countries to immediately freeze the assets of any person or persons accused of terrorist activities. Currently, it has listed 42 terrorist organisations and 56 individual terrorists. All acts of terrorism involving WMDs are punishable offences under the Act. India also established the National Investigation Agency in 2008, which serves as the central counter-terrorism law enforcement agency in India.

In addition, recognising the need for enhanced domestic nuclear regulatory frameworks, India introduced the Nuclear Safety Regulatory Authority (NSRA) Bill in September 2011. This proposed legislation aimed to replace the AERB with a more independent NSRA, modelled after regulatory bodies in advanced nuclear states like France, the UK, and the U.S.. However, the Bill faced criticism regarding the lack of clarity and autonomy of the proposed regulatory authority. Since 2014, attempts have been made to reintroduce an improved NSRA Bill that focuses on ensuring robust nuclear regulatory oversight aligned with international best practices, but the Indian Parliament is yet to conduct a debate on the Bill.

Table 3: Indian Approach to Nuclear Security and Safety

| Governing Tool | Description |
|---|---|
| **Atomic Energy Act, 1962** | The foundational legislation for India's nuclear activities covers all aspects of developing and securing nuclear and radiation technologies. It authorises the central government to establish rules, regulations, and notifications. |
| **Environmental and Operational Legislation** | This includes critical laws like the Environment (Protection) Act of 1986, Atomic Energy (Factories) Rules of 1996, and the Electricity Act of 2003, which influence the location and operation of nuclear power plants and related activities. |

| | |
|---|---|
| **Guidelines for Nuclear Transfers (Exports), 2006** | Established by the Department of Atomic Energy (DAE) to govern the export of nuclear materials. |
| **Atomic Energy (Radiation Protection) Rules, 1971** | Rules that regulate radiation protection in nuclear fuel cycle facilities and other radiation-related industries. |
| **Atomic Energy (Safe Disposal of Radioactive Wastes) Rules, 1987** | Mandates the AERB to ensure licensees follow guidelines for the safe disposal of radioactive waste, including decommissioning procedures, to prevent environmental contamination. |
| **Atomic Energy (Working of Mines, Minerals and Handling of Prescribed Substances) Rules, 1984** | Governs the mining, processing, and handling of nuclear materials, ensuring safe and secure operations throughout these activities. |
| **Unlawful Activities (Prevention) Act, 1967** | The Act allows for freezing assets related to terrorist activities and lists organisations and individuals as terrorists. |
| **National Investigation Agency (NIA), 2008** | The NIA plays a crucial role in investigating and prosecuting crimes related to nuclear security and terrorism. |
| **Nuclear Safety Regulatory Authority (NSRA) Bill, 2011** | A proposed legislative measure to replace the AERB with an independent NSRA, modelled after regulatory bodies in advanced nuclear states. |
| **Convention on the Physical Protection of Nuclear Material (CPPNM)** | India is a signatory to the CPPNM, which mandates that nuclear materials are protected during international transport and sets out guidelines for the physical protection of nuclear facilities and materials domestically. |

| | |
|---|---|
| **International Convention for Suppression of Acts of Nuclear Terrorism, 2005** | India is committed to preventing nuclear terrorism by adhering to this international treaty, which criminalises the unlawful possession and use of nuclear materials and obliges countries to cooperate in addressing nuclear terrorism. |
| **United Nations Security Council Resolution 1373** | India has incorporated UNSC Resolution 1373 into its domestic legislation, thus mandating the freezing of assets linked to terrorist activities and requiring international cooperation in combating terrorism, including nuclear terrorism. |

## Regulatory Institutions

India also has several autonomous bodies that oversee and govern nuclear security and safety. One of the primary institutions is the Atomic Energy Commission (AEC), set up in 1948 initially under the Department of Scientific Research. Subsequently, following a government resolution in 1958, the AEC was established in the Department of Atomic Energy (DAE) to function as an autonomous body with financial and executive powers. The AEC functions as an overarching body in nuclear security and safety. The members of the AEC are chosen by the Prime Minister based on the Secretary, DAE's recommendations. The AEC is primarily responsible for creating DAE policies and budgets, with execution assigned to the DAE. In 1954, the DAE was assigned the task of developing nuclear power technology and applications of radiation technologies in various fields, including agriculture, industry and scientific research. The DAE is also responsible for the design to operation of nuclear power and research reactors.

The AERB, established in 1983, is India's nuclear regulator and operates independently of nuclear power operators in the country. This independence is essential to ensure its ability to regulate all activities related to the safety and security of nuclear and radioactive materials, particularly in terms of facilities and transport. The AERB has several committees under its umbrella to discharge its duties, including the Safety Review Committee for Operating Plants (SARCOP) and the Safety Review Committee for Applications of Radiation (SARCAR), which are responsible for safety review. SARCOP, established in 1988, assesses and enforces nuclear, radiological, and industrial safety in all operating plants under the DAE. SARCAR is responsible for streamlining the implementation of Radiation Protection Rules in all its

processes and institutions that use radioisotopes and radiation materials in medical, industrial, and research institutes.

Each of these agencies plays a key role in enhancing nuclear security through better coordination as well as periodic review of existing measures, which augment the overall readiness of the nuclear establishment to deal with any contingency, including nuclear terrorism.

### Licensing

Licensing is strictly subject to the operator submitting, to the AERB's satisfaction, that the emergency and security plans for installation and safe storage for sources are available within their premises. In the case of transport of radioactive material, ranging from Category 1 to Category 3 sources, the regulatory process involves online package tracking and an online real-time monitoring and reporting system called eLORA (e-Licensing of Radiation Applications), which is also used to report loss or theft to the police and the AERB within 24 hours. The AERB is responsible for all licensing, including tech transfer at universities as well as the import and export of materials. These are also enforced through India's export control mechanisms, including the Nuclear Suppliers Group, which are reviewed and updated in line with India's commitments under the global nonproliferation regime.

## Security Institutions in the Context of Nuclear Security

Besides the regulatory bodies in the nuclear sector, national security institutions also play an important role in maintaining nuclear security. These include intelligence agencies, the CISF, state-level police forces, the military, and the National Disaster Management Agency (NDMA) and National Disaster Response Force (NDRF).

### Intelligence Agencies

India's domestic intelligence agency, Intelligence Bureau (IB), along with state-level intelligence agencies, performs an important role in nuclear security by maintaining a close watch on the plans and activities of terrorist organisations and other violent non-state actors; monitoring physical security of the nuclear installations and movement of radioactive material; and performing periodic audits of nuclear installations. The external intelligence agency, Research and Analysis Wing, also plays a crucial role by monitoring the external environment, which may threaten India's nuclear security, including Pakistan-based terrorist organisations as well as the international nuclear black market.

## CISF

The agency is tasked with guarding India's critical installations and is the primary agency for physically protecting nuclear facilities. Towards this, it is responsible for access control and monitoring the movements of the staff and personnel posted at the facilities. In addition, it is one of the agencies responsible for radioactive materials' transportation security. The agency, which works under the Ministry of Home Affairs (MHA), imparts specialised training to its personnel in handling radiation leaks and other contingencies at nuclear facilities.

## State-Level Police Forces

As per MHA's guidelines, state-level police forces are tasked with the security of the outer periphery of nuclear installations. They often act as first responders in cases of theft and crimes committed at nuclear facilities. Along with other agencies, they carry out security audits and perform regular mock drills, besides providing armed escorts during the transportation of nuclear materials. The intelligence wings of the state police forces work in tandem with the IB to monitor suspicious activities that may imperil the security of nuclear installations.

## NDMA and NDRF

The NDMA is the designated agency for disaster mitigation and relief in India. It also includes NDRF, which acts as the primary force to respond to natural and man-made disasters, including any nuclear and radiological emergencies. The NDMA's guidelines on the Management of Nuclear and Radiological Emergencies list several contingency situations and steps that are to be taken to handle those situations. These guidelines are an important step in shaping a holistic, all-stakeholder-inclusive approach to handling post-disaster scenarios. These guidelines include "a series of actions on the part of the various stakeholders at different levels of administration that would (i) mitigate the accident at source;(ii) prevent deterministic health effects in individuals and limit the probability of stochastic effects in the population; (iii) provide first aid and treatment of injuries; (iv) reduce the psychological impact on the population; and (v) protect the environment and property, all under the constraint of available resources." The guidelines are also an important exercise in public awareness.

## Military

The Indian military's role in securing nuclear installations is limited, reflecting the general practice of utilising and deploying the military only when all other government agencies fail or if the task is beyond the capacity of civilian institutions. However, the Indian military imparts regular training on chemical, biological, radiological, and nuclear security to its personnel.

## Inter-Agency Coordination

Inter-agency coordination is a crucial component of nuclear security, involving emergency preparations and training modules utilised by respective agencies, among other aspects. Even before the 9/11 terrorist attacks in the U.S., which reiterated the importance of nuclear security to the world at large, in 1987, India had established a Standing Group for Coordination and Review of Security Arrangement (SG-CRSA) for all nuclear facilities. A multi-agency group meets every four months with the aim of exchanging threat information, including any changes in the threat scenario, new and emerging threats, and the views of other national intelligence agencies regarding these threats. If required, this group also prepares standard operating procedures (SOPs) to address nuclear security issues. For example, after a cybersecurity incident at the Kudankulam nuclear facility in 2019, SG-CRSA issued an SOP addressing various new threats, including unmanned aerial intrusions into vital installation facilities, which has been shared with all of them.

The DAE has also constituted specialist groups like the Computer and Information Security Advisory Group (CISAG) and the Task Force for Information and Control Security (TAFICS) to monitor the cyber/information security of the Nuclear Power Corporation of India Limited (NPCIL), among other associated institutions of DAE, including regular cybersecurity audit, to address further potential cybersecurity intrusions.

The Counter-Nuclear Smuggling Team (CNST) is another initiative that integrates multiple agencies with the functions of investigation, border management, and nuclear forensics while combating nuclear-smuggling cases. The CNST compiles information quarterly and conducts tabletop exercises to ensure that each agency knows its responsibilities and duties.

However, inter-agency coordination among the security agencies can be challenging. While this is not unique to India, given the density in the country's cities and towns, any nuclear calamity would need to be handled with greater care and sensitivity. The ability of different agencies to work together under such circumstances becomes even more important. Generally, the different security organisations have engaged in simulation exercises to ensure preparedness, but the periodicity of exercises involving all the different security agencies needs to be improved. Some recent examples include specialised training and advanced courses, along with workshops on CBRN operations conducted for NDRF battalion personnel at the North Eastern Police Academy (NEPA) and Bhabha Atomic Research Centre (BARC) in 2015-2016. Similarly, in 2017, a workshop on the medical management of CBRN casualties for medical officers was held in New Delhi and BARC, Mumbai. In 2019, the NRDF began an annual training and refresher course on CBRN emergencies, including for first responders. These courses were enhanced in 2024, when India deployed the NDRF to simulate potential attacks in the Ayodhya region as part of their continuous familiarisation exercise.

## Nuclear Facility Design and Security

India has a classified national Design Basis Threat (DBT) document, and each nuclear facility devises its own DBT document to design the physical protection aspects of the facilities. The Indian DBT takes into account existing threats from saboteurs, thieves, terrorists and other malicious actors, their characteristic capabilities and tactics, as well as the possibility of collusion with insiders. Various surveillance, detection, and response mechanisms as well as access control measures are in place at nuclear facilities. This helps institute a graded security approach over four layers surrounding the most sensitive parts of the facility. Physical protection systems are also regularly audited by the AERB. India's national system of nuclear material accounting and control and personnel reliability measures play an important role in the practice of nuclear security, thereby ensuring compliance.

Security and inspections have the same underlying philosophy as nuclear safety regulations and inspections. The AERB conducts planned and random inspections for operational nuclear power plants and during various development stages of ongoing projects. The planned inspection usually occurs once a year for operating plants. The inspection team (usually made up of four members) comprises members of the Committee for Reviewing Security Aspects of Nuclear Facility (CRSANF), who are trained and experienced in the nuclear security aspects. The AERB authorises the inspection team and the team leader or lead inspector. Inspections typically take three to four days, depending on the number of Operating Islands to be inspected.

## Emergency Response

In case of an emergency, India possesses 25 emergency response centres spread across the country to address any issues arising from input received from around 500 radiation monitoring stations, which are well connected and provide the real-time status of all activities in their respective areas. All nuclear power plants and related activities, including nuclear fuel cycle activities, are covered under this network so that no nuclear facility is out of the reach of nuclear radiation monitoring systems at any point of time. In the case of any eventuality, the NDMA is linked with local law enforcement agencies. In addition, the DAE has constituted a Crisis Management Group (CMG), which deals with nuclear and radiological emergencies and incidents. The CMG works out of a 24/7 control room, and its services are available to the NDMA if required. Periodic crisis management and off-site emergency exercises are conducted at all nuclear sites at intervals of two years, with active participation from all atomic energy and security agencies.

## Diplomatic Collaborations and Global Commitments

India's nuclear security capabilities are bolstered by its active diplomatic collaborations. The country's collaboration with the IAEA facilitates knowledge sharing, capacity building, and technical assistance programmes. Further, bilateral agreements with like-minded partners enhance information exchange and coordinated responses to transnational threats, demonstrating the crucial role of global cooperation in enhancing India's nuclear security. For instance, the Global Centre for Nuclear Partnership (GCNEP) has 14 MoUs with several countries, such as the U.S., Russia, and France, and organisations such as the IAEA and has conducted more than 56 international programmes, including training courses and workshops on nuclear safety and security such as the physical protection of nuclear materials, vulnerability assessment, insider threat, computer security and controls, and security and transport of radioactive materials, drawing more than 500 participants from around 60 countries alongside over 1,000 Indian participants.

India also invited the IAEA for an Integrated Regulatory Review Services (IRRS) mission in 2015. This mission, a first for India, affirmed the AERB's operational independence while recommending statutory reinforcement to solidify its regulatory autonomy.

In terms of its global commitments, India is party to all 13 international instruments that are accepted as benchmarks for a state's commitment to combat international terrorism, including the International Convention for Suppression of Acts of Nuclear Terrorism (2005) and the Convention on the Physical Protection of Nuclear Material (CPPNM), along with the 2005 amendment which, among other provisions, brought the domestic transport of nuclear materials within its ambit. Additionally, India supports the IAEA Code of Conduct on the Safety and Security of Radioactive Sources (2003) and has voluntarily adopted its provisions. India adheres to the Nuclear Suppliers Group (NSG) Guidelines on the supply of nuclear items, import and export of nuclear equipment, and physical protection of nuclear materials and facilities. India has also supported the implementation of the United Nations Security Council Resolution 1540 (2004) regarding the nonproliferation of WMDs, especially to non-state actors, towards preventing WMD terrorism. That India is a member/participating state in several international export control regimes such as the Wassenaar Arrangement and the Australia Group also signals its commitment to stringent export controls on sensitive technologies.

## Technical Innovations and Research

Investments in cutting-edge technologies and research initiatives are pivotal to advancing India's defences against nuclear terrorism. India has implemented technology that prevents

the diversion of radioactive material and pursued a closed fuel cycle for plutonium reactors, implying that plutonium is never stored in depositories; rather, it is purified and reused, effectively removing it from the public domain. This ensures the avoidance of the buildup of stockpiles and the need to store large amounts of spent fuel in underground depositories, potentially giving malevolent actors easy access to plutonium. Additionally, Indian scientists are adopting proliferation-resistant technologies such as advanced heavy water reactors, which makes access to uranium particularly difficult in case of intrusion.

## Insider Threat Detection

Considering its vulnerability to tampering and technical failures, there is a need to pay attention to the human dimension in nuclear security, highlighting that excessive reliance on technology is not advisable. However, with human elements, there are potential threats like insider threats. These aspects need to be examined and strengthened with an augmented nuclear security culture. India has mitigated insider threats by implementing the "two-man rule", which states that no responsibility is left to any individual within the nuclear setup. This measure has proved to be highly effective. At the same time, dealing with insider threats requires a dynamic approach. India has also established a solid personnel reliability process through rigorous vetting and screening. While India has not faced any serious insider threats while operating nuclear facilities, given India's plans to expand its nuclear programme, India needs to remain vigilant for any disgruntlement among employees that could potentially turn into insider threats.

## Other Radioactive Sources

The discussion on nuclear security extends beyond terrorism, as radioactive sources have several applications beyond nuclear facilities. Radioactive materials and equipment have thousands of licensees, including hospitals and industries, mainly due to an increasing number of medical centres and the importance of radiation-related diagnosis and procedures.

- Radiological equipment used by industry usually falls within Category 2 sources. It is generally not a cause for concern due to a well-organised corporate structure and stiff competition within the structure. The only vulnerability is short-distance transportation, particularly in instances such as last-minute orders, which may potentially lead to cutting corners. This is an area where enhanced security culture can help. In addition, care needs to be taken to prevent situations that can lead to paranoia and phobia among the general public.

- The only presence of large, Category 1 sources used for commercial purposes is in radiation

processing plants, where gamma radiation sources are widely employed. There are about 20 gamma-source-based plants in India, which have a substantial amount of stored cobalt, most of which has a half-life of 15-20 years. However, these sources are well-contained, usually within cells, and have sufficient physical protection. There is little scope for mishaps, except damage within the cell itself, which is not an appealing proposition for terrorists. There is a viable replacement for gamma sources in the form of electron beam accelerators, but this comes at a much higher cost and presents an economic challenge.

Cases such as the Mayapuri incident of 2010 have proven that orphaned sources can have potentially lethal consequences, albeit on a smaller scale. India has since taken measures to contain the threat posed by such sources. For instance, immediately after the incident, the AERB held awareness workshops for scrap dealers in Mayapuri and elsewhere. It also collaborated with the University Grants Commission to tighten the access of educational institutions' access to radiological material for scientific experiments.

This also raises the question about whether it is possible to transition to non-radioactive source-based equipment in some sectors. For example, in the case of radiotherapy for cancer treatment, the availability of linear accelerators that do not contain radioactive sources invalidates the need for cobalt-60-based telecobalt equipment. India is already implementing this; there are less than 300 telecobalt units in the country, and the number is diminishing.[13], X-ray-based systems are replacing blood irradiators that use cobalt and cesium. However, these alternatives are more expensive, and hospitals would require financial support to transition completely.

Therefore, fostering the adoption of proven alternative technologies to radioactive sources will benefit India. A consequential need will be mobilising resources and support to facilitate the transition. Moreover, when it comes to the human element, monitoring the human resources involved in facilities containing Category 1 and 2 sources is essential. Ensuring effective organisational management and culture and establishing operating solid procedures are critical. Radioactive sources are involved across various applications, making practice-specific approach and guidance extremely important.

13 There are certain types of treatment, however, where radioactive sources are introduced very close to the tumour, known as brachytherapy. There is no known viable replacement for them thus far.

## Public Awareness and Preparedness

Public awareness campaigns and community engagement initiatives play a crucial role in promoting vigilance and preparedness against nuclear terrorism. India has utilised various media platforms to disseminate positive and accurate information about nuclear power. For instance, at the Kudankulam Nuclear Power Plant, commercials on TV and radio were used to explain the safety of nuclear power. These media campaigns included short videos and audio advertisements, quickly reaching a broad audience. Further, officials participated in public debates and provided simple analogies to explain complex nuclear processes, making the information more accessible to the general public.

At a microscopic level, handouts and pamphlets have been distributed in regional languages, such as Tamil, Malayalam, and English, to ensure that information reaches a diverse audience. This method helped directly address local communities' fears and concerns, particularly in regions where nuclear power plants are being constructed or operated. Interactions with educational institutions, including presentations and Q&A sessions, have been crucial for raising awareness and building an understanding about nuclear power. Educational outreach has also been crucial to raising awareness and building understanding about nuclear power. These interactions targeted local opinion leaders in addition to students and academics, thereby influencing broader public opinion.

Finally, in a crisis, communications systems are detailed as part of a Standard Operating Procedure (SOP). Indian nuclear power plants need to have detailed crisis communication plans in place. These plans include clear and immediate communication with the public and media to prevent misinformation and provide accurate updates on the situation. The emphasis is on transparency and timeliness to build and maintain trust during critical situations.

## International Perceptions

Despite these robust measures, some international reports such as the Nuclear Threat Initiative's (NTI) *Nuclear Security Index* rank India low on metrics of nuclear security, even below Pakistan across most metrics. This is potentially due to the NTI's tick-mark approach, which merely tracks whether or not a particular country has a specific regulation. The NTI's approach does not account for complexities such as how well the legislation is implemented and/or how regulatory bodies function practically. Additionally, even when international regulations are followed in India, organisations such as the NTI perceive the situation differently due to differences in terminology, which India has rectified to a large extent in recent years. On the contrary, India's nuclear facilities have been examined by the IAEA,

which has declared them to be on par with others in the developed world. Additionally, a lack of transparency and external outreach by India's nuclear establishment also contribute to the misperception that requisite nuclear security measures are not in place in India. An additional complicating factor is that there is no single database on nuclear security in India, and consequently, multiple and scattered sources are utilised. The DAE has tried to correct this anomaly by introducing a nuclear security section in its annual reports, but this is relatively recent and somewhat limited in scope.

Overall, India has strengthened its nuclear security architecture in line with the rapidly changing security scenario and threat perceptions. However, it cannot afford to be complacent in nuclear security because, unlike most other countries, the Indian neighbourhood is fraught with unstable conditions.

## Recommenations

As India navigates the complex landscape of nuclear terrorism threats, drawing insights from international best practices can inform strategic recommendations to bolster defences and response capabilities. Examining successful approaches adopted by other nations would provide valuable lessons and actionable insights for enhancing India's preparedness and resilience.

### Public Awareness and Community Engagement

The primary step should be increasing public awareness through campaigns and community engagement initiatives. These are integral to a resilient nuclear security framework. Some states have remained proactive, but it has not been done uniformly across the country. Additionally, strengthened engagements between nuclear plant operators and state disaster management authorities, along with the involvement of local bodies, can be useful in enhancing the support for nuclear energy in India. This is a critical component in the context of dealing with contingencies in particular. Atomic energy agencies also need to prioritise public engagement with a focus on enhancing the public understanding of nuclear security risks, promoting transparent communication channels, and empowering local communities to safeguard critical infrastructure and respond effectively to potential threats. Disaster management agencies such as the NDRF and the state-level Response Force agencies could play a critical role in this regard.

### Adaptive Response Strategies and Exercises

Dynamic threat environments necessitate agile and adaptive response strategies tailored

to evolving scenarios. Models from countries like the U.S., France, UK, and South Korea demonstrate the efficacy of regular simulations, crisis management exercises, and inter-agency coordination drills in testing readiness, refining response protocols, and enhancing interoperability across security agencies. India can strengthen its preparedness by institutionalising comprehensive scenario-based exercises, fostering more efficient inter-agency collaboration, and institutionalising lessons learned from international best practices to enhance readiness and resilience against nuclear terrorism incidents.

## Cyber Warfare in Nuclear Establishment

The evolving nature of cyber threats necessitates robust cybersecurity measures to mitigate potential risks effectively. This involves a multi-layered defence strategy. The recommendations are tiered to advance from ground-level changes that can be approached immediately to overarching policy implementations to strengthen legal architecture in the long run. These include the following:

a. Employee Training and Awareness Programmes
    - Educating employees on cybersecurity best practices. Training staff to recognise phishing attempts, social engineering tactics, and other common attack vectors.
b. Regular Security Audits and Vulnerability Assessments
    - Conducting frequent security audits and vulnerability assessments to identify and address potential weaknesses in the nuclear infrastructure.
    - Employing ethical hackers to perform penetration testing and simulate cyberattacks, ensuring preparedness against real-world threats.
    - Adopting a zero-trust approach to cybersecurity, where no entity—internal or external—is inherently trusted. Incident Response and Recovery Planning:
c. Utilising Technological Tools
    - Utilising state-of-the-art intrusion detection systems and intrusion prevention systems to identify and mitigate cyber threats in real-time.
    - Implementing machine learning and artificial intelligence to enhance threat detection capabilities and swiftly respond to anomalies.
    - Developing comprehensive incident response plans to manage and mitigate the impact of cyber incidents and minimise recovery time.
d. Collaboration and Information Sharing
    - Engaging in threat intelligence and best practices sharing at a regional and international level with trusted countries, cybersecurity organisations, and industry partners.

## Investments in Technological Innovations

Advancements in technology play a pivotal role in fortifying defences against evolving

nuclear terrorism threats. Innovations in cybersecurity, radiation detection, and emergency response systems offer capabilities to pre-empt, detect, and mitigate potential risks. Countries like Israel and Japan exemplify proactive approaches through continuous research and development in cutting-edge technologies that enhance nuclear security resilience. India can benefit from intensifying investments in research partnerships, fostering collaboration between academia, industry, and government agencies to drive innovation and deploy state-of-the-art technologies across its nuclear infrastructure.

**Enhanced International Cooperation**

Successful international collaborations serve as force multipliers in combating nuclear terrorism threats. Models from collaborative platforms such as the Global Initiative to Combat Nuclear Terrorism showcase effective mechanisms for information sharing, capacity building, and joint exercises among participating states. India should prioritise expanding and deepening its partnerships with regional allies and like-minded partners as well as international organisations like the IAEA in order to leverage collective expertise and resources to strengthen mutual defences against shared threats.

## Conclusion

India's security posture is influenced by its volatile geographical location. The interplay of historical animosities, ongoing conflicts, political instability in neighbouring countries, and the ever-present threat of terrorism necessitates a vigilant and dynamic approach to national security. Safeguarding its nuclear assets, addressing conventional military threats, and navigating the complex geopolitical landscape are integral to India's comprehensive security strategy.

By drawing from international comparisons and adopting proactive measures, India can enhance its response to nuclear terrorism threats, safeguard national security, and contribute to global stability. Recommendations centred on strengthening legislative frameworks, fostering international cooperation, investing in technological innovations, promoting public awareness, and refining adaptive response strategies are critical to fortifying India's defences and resilience against the complex challenges of nuclear terrorism. As threats evolve, India's commitment to continuous improvement and collaboration remains pivotal in maintaining effective deterrence and preparedness capabilities on the global stage.

Therefore, there is an imperative for India to leverage international lessons and strategic recommendations to fortify its defences against nuclear terrorism towards reinforcing its commitment to global security and resilience.

**Acknowledgements**

*The authors acknowledge CRDF Global's grant on "Expanding and Diversifying Counterproliferation Efforts" for the conduct of this research and the convening of related closed-door roundtable discussions in the first half of 2024.*

# ANNEXURE

## Annexure 1 - Survey Questionnaire

The following is a questionnaire that the ORF team circulated amongst the participants at the first focused group discussion, held on 26 February 2024. The objective of this exercise was to get more objective responses regarding threats and terrorism.

1. What is your general assessment of India's terrorism threat scenario?

- Low
- Moderate
- High
- Very high

2. How do you see linkages between nuclear issues and terrorism?

- Weak or non-existent
- Limited
- Moderate
- Strong

3. How do you assess border security in preventing nuclear material theft?

- Inadequate
- Somewhat effective
- Effective
- Highly effective

4. How vigilant are the policy and technical wherewithal to detect the movement of nuclear materials in border areas?

- Not vigilant at all
- Somewhat vigilant
- Vigilant
- Highly vigilant

5. What are the different types of non-state actors that could pose a nuclear threat to India?

- Terrorist groups
- Insurgent groups
- Extremist groups
- All of the above

6. Which of the following are threats posed to India.

- Cross-border terrorist groups
- India-based terrorist groups (on their own as well as with external support)
- ISIS
- Al-Qaeda / Al-Qaeda in South Asia
- Left-wing extremists
- Northeast insurgent groups

7. What are the known vulnerabilities in India's nuclear programme that terrorists could exploit?

- Insider threats
- Physical security weaknesses
- Cybersecurity vulnerabilities
- Interagency non-cooperation

8. What would be the potential consequences of a nuclear terrorist attack in India, and how would the international community respond?

- Isolation of India
- Humanitarian crisis
- Global security concerns
- All of the above

9. What policies or initiatives do you think should be prioritised to strengthen India's nuclear security posture?

- Enhanced border surveillance

- Improved intelligence-sharing mechanisms
- Strengthened regulatory frameworks.
- All of the above

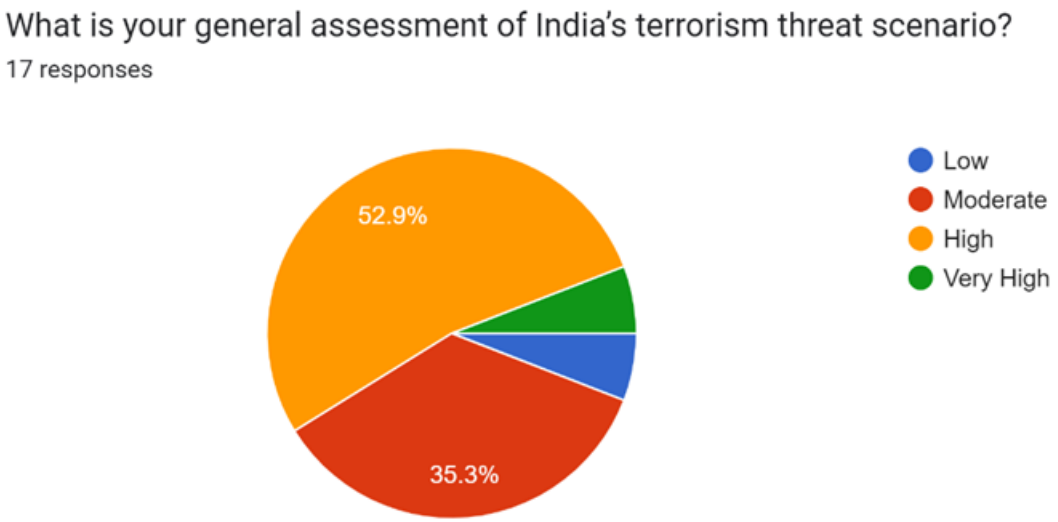
10. How resilient do you think India’s nuclear infrastructure is to cyber-attacks?

- Highly vulnerable
- Vulnerable
- Moderately resilient
- Highly resilient

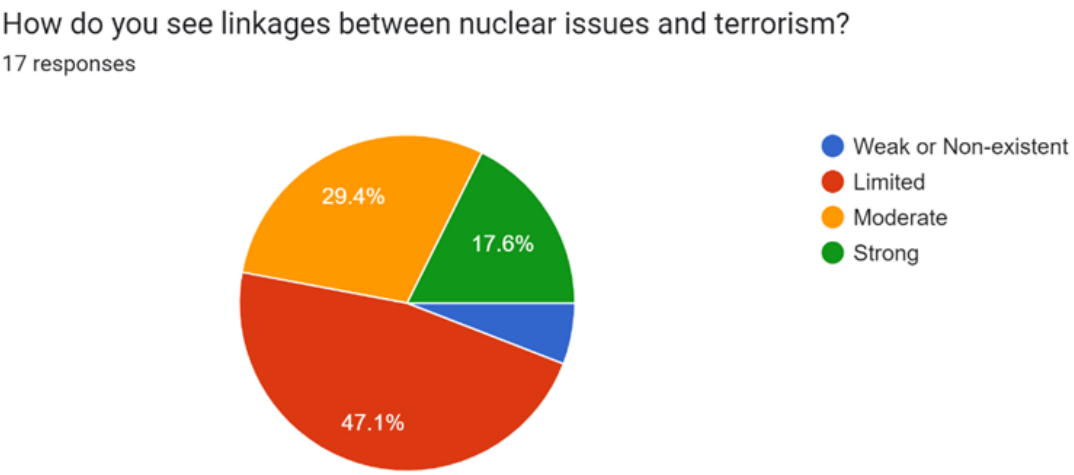
## Annexure 2 - Findings of Survey Conducted on 26 February 2024

Following are the findings from the survey questionnaire circulated among the participants.

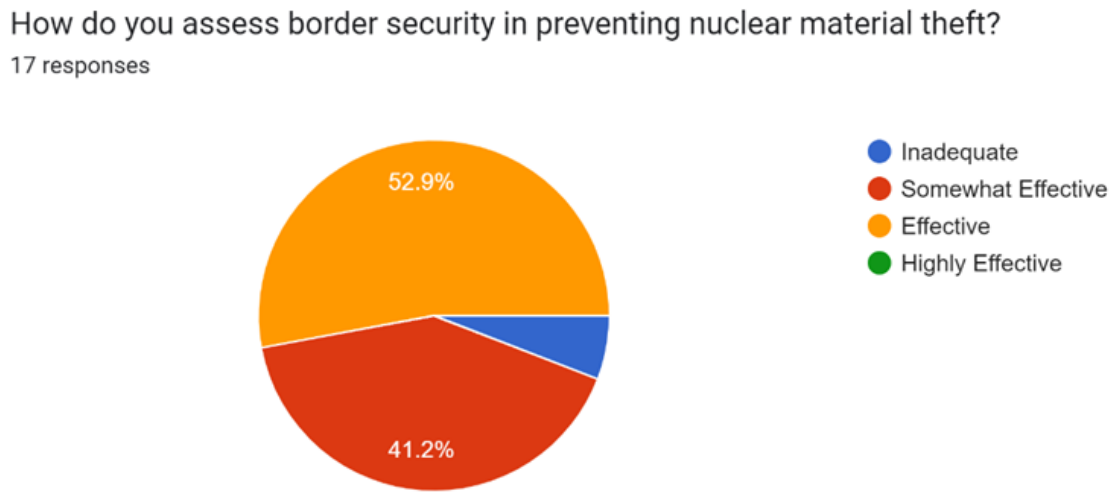
### Q. 1: What is your general assessment of India's terrorism threat scenario?



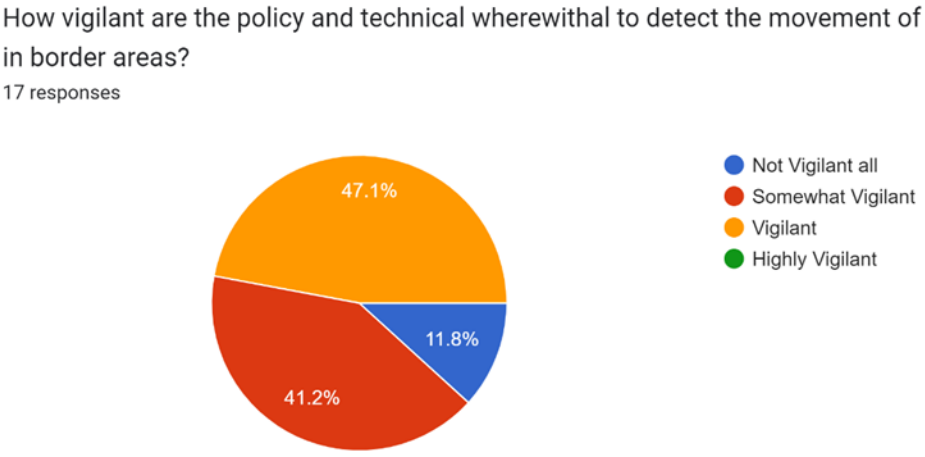

### Q. 2: How do you see linkages between nuclear issues and terrorism?



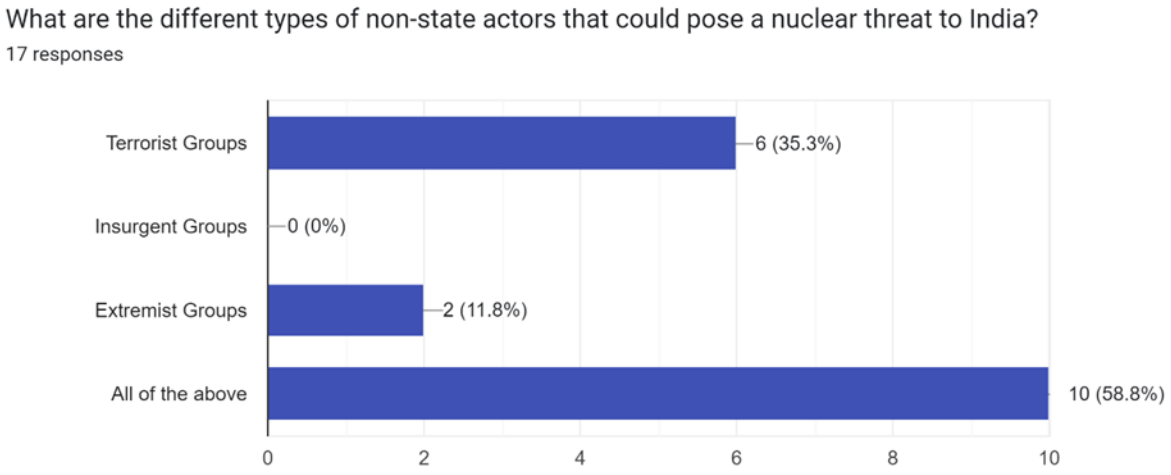
**Q. 3: How do you assess border security in preventing nuclear material theft?**



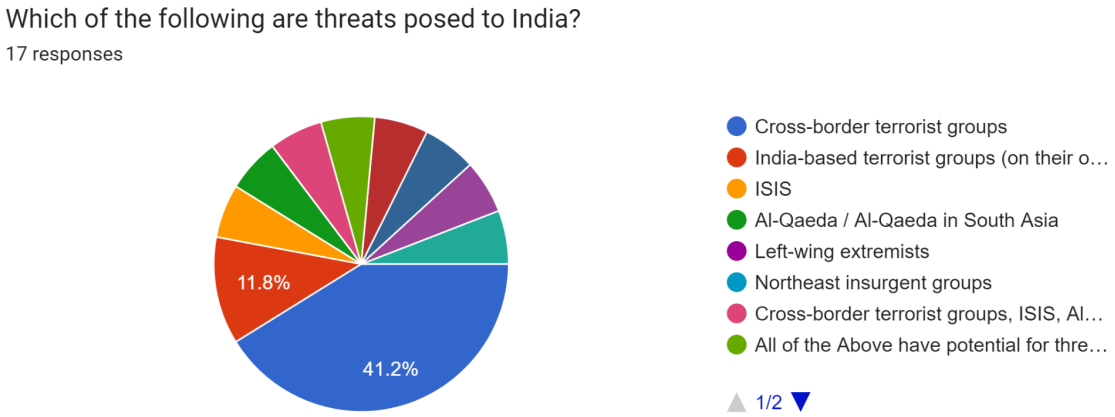

**Q. 4: How vigilant are the policy and technical wherewithal to detect the movement of nuclear materials in border areas?**



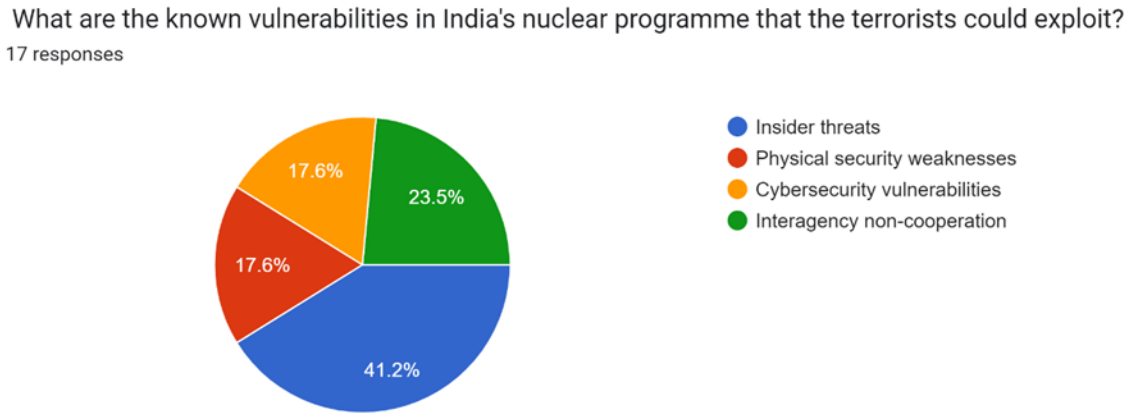
## Q. 5: What are the different types of non-state actors that could pose a nuclear threat to India?



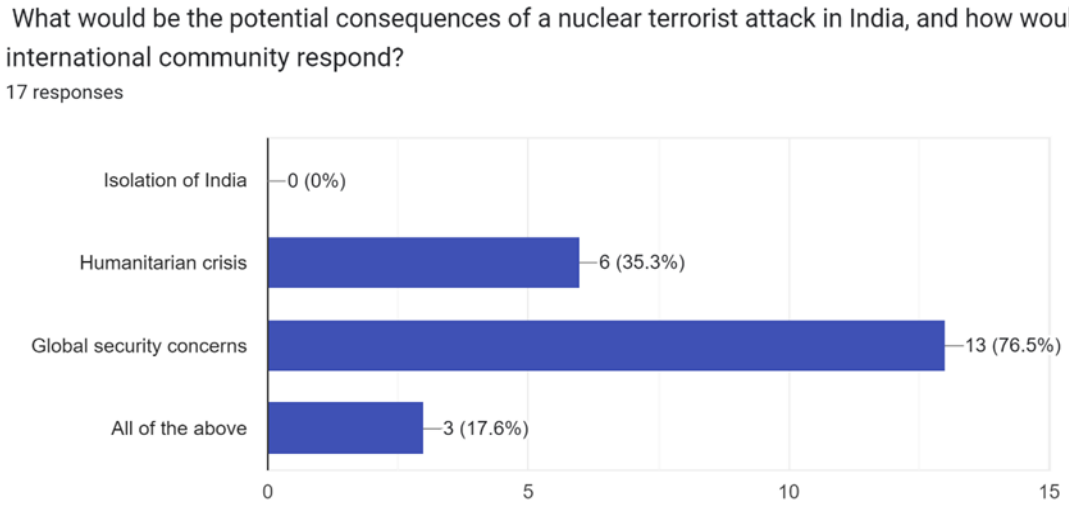

## Q. 6: Which of the following are threats posed to India?



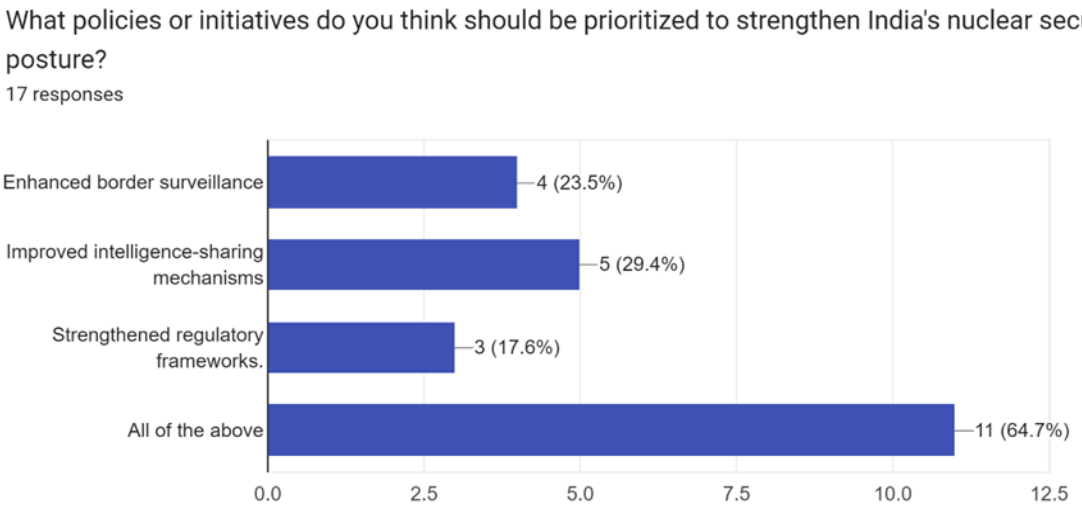
**Q. 7: What are the known vulnerabilities in India's nuclear programme that terrorists could exploit?**



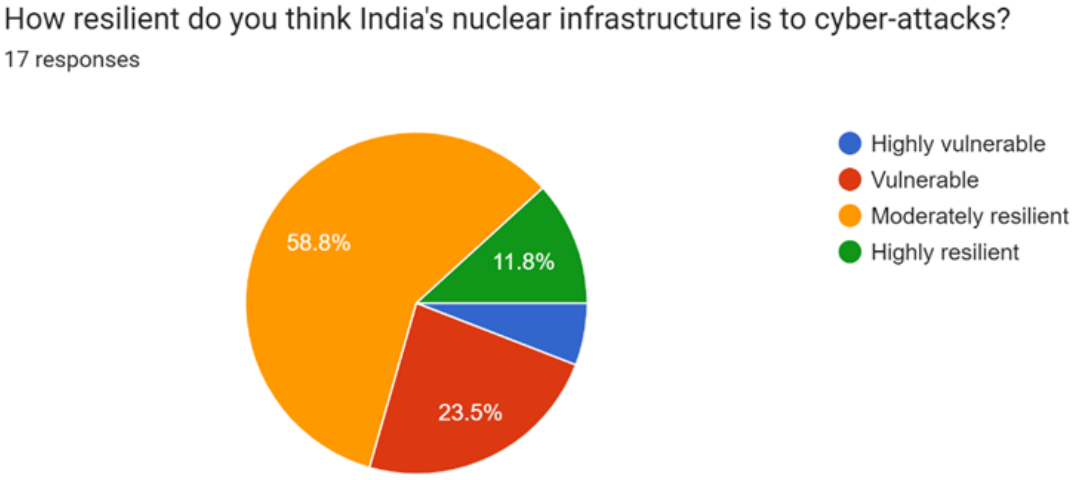

**Q. 8: What would be the potential consequences of a nuclear terrorist attack in India, and how would the international community respond?**



Q. 9: What policies or initiatives do you think should be prioritised to strengthen India's nuclear security posture?




Q. 10: How resilient do you think India's nuclear infrastructure is to cyber-attacks?




## Endnotes

Steven E. Miller, "Soviet Collapse and Nuclear Dangers: Harvard and the Nunn-Lugar Program," Stimson Centre, 20 October 2023, https://www.stimson.org/2023/soviet-collapse-and-nuclear-dangers-harvard-and-the-nunn-lugar-program/

William Walker, "The International Nuclear Order After the Cold War—Progress and Regress | The Rise and Decline of the Post-Cold War International Order," Oxford Academic, November

2018, https://academic.oup.com/book/5737/chapter-abstract/148878074?redirectedFrom=full-text&login=false.

"IAEA Database On Trafficking Of Nuclear and Other Radioactive Material Records 4243 Incidents Since 1993," International Atomic Energy Agency, May 20, 2024, https://www.iaea.org/newscenter/pressreleases/iaea-database-on-trafficking-of-nuclear-and-other-radioactive-material-records-4243-incidents-since-1993

FBIS, "Compilation of Osama Bin Ladin Statements 1994," Federation of American Scientists, January 2004, https://irp.fas.org/world/para/ubl-fbis.pdf.

Rolf Mowatt-Larssen, "Al Qaeda Weapons Of Mass Destruction Threat: Hype Or Reality?" Belfer Center for Science and International Affairs, January 2010, https://www.belfercenter.org/publication/al-qaeda-weapons-mass-destruction-threat-hype-or-reality

Muhammed Ali Alkış, "Threat Of Nuclear Terrorism: The Developing Nuclear Security Regime," International Journal of Nuclear Security, January 1, 2020, https://doi.org/10.7290/ijns07e3t1.

Sameer Lalwani and Hannah E. Haegeland, "Anatomy Of a Crisis: Explaining Crisis Onset In India-Pakistan Relations," Stimson Center, 2018, https://www.semanticscholar.org/paper/ANATOMY-OF-A-CRISIS-Explaining-Crisis-Onset-in-Lalwani-Haegeland/a5d10ee2ff4d81348c9bf57105927a0a55ff4d92.

Christine Fair, "Fighting To the End: The Pakistan Army's Way of War," Oxford University Press, 2014: 227

Lalwani and Haegeland, "Anatomy Of a Crisis: Explaining Crisis Onset in India-Pakistan Relations."

"Pakistan Army and Terrorism; an Unholy Alliance," European Foundation for South Asian Studies, https://www.efsas.org/publications/study-papers/pakistan-army-and-terrorism%3B-an-unholy-alliance/.

Sharad Joshi, "The China-Pakistan Nuclear Deal: A Realpolitique Fait Accompli," The Nuclear Threat Initiative, December 10, 2011, https://www.nti.org/analysis/articles/china-pakistan-nuclear-deal-realpolitique-fait-accompli-1/.

Sharad Joshi, "The China-Pakistan Nuclear Deal: A Realpolitique Fait Accompli."

Rajeswari Pillai Rajagopalan, "India's Latest Concerns With the China-Pakistan Economic Corridor," Observer Research Foundation, August 10, 2022, https://www.orfonline.org/research/indias-latest-concerns-with-the-cpec.

Prime Minister's Office, "Cabinet Committee On Security Reviews Progress In Operationalizing India's Nuclear Doctrine," Press Information Bureau, January 4, 2003, https://archive.pib.gov.in/release02/lyr2003/rjan2003/04012003/r040120033.html

Ramesh Thakur, "The Inconsequential Gains and Lasting Insecurities Of India's Nuclear Weaponization," International Affairs (2014), https://www.jstor.org/stable/24538615.

Daniel Markey, "The Persistent Threat Of Nuclear Crises Among China, India and Pakistan," United States Institute of Peace, February 1, 2023, https://www.usip.org/publications/2023/02/persistent-threat-nuclear-crises-among-china-india-and-pakistan.

United Nations Treaty Collection, "International Convention For the Suppression Of Acts Of Nuclear Terrorism," United Nations Treaty Collection, April 13, 2015, https://treaties.un.org/pages/ViewDetailsIII.aspx?src=TREATY&mtdsg_no=XVIII-15&chapter=18&Temp=mtdsg3&clang=_en.

United Nations Office for Disarmament Affairs, "UN Security Council Resolution 1540," United Nations Office for Disarmament Affairs (2004), https://disarmament.unoda.org/wmd/sc1540/.

Ashley J. Tellis, C. Christine Fair, and Jamison Jo Medby, "Limited Conflicts Under the Nuclear Umbrella: Indian and Pakistani Lessons From the Kargil Crisis," RAND, January 1, 2001, https://www.rand.org/pubs/monograph_reports/MR1450.html.

Sandeep Unnithan, "From the India Today archives (2013) | 26/11: Inside the Secret World Of David Coleman Headley," India Today, May 22, 2023, https://www.indiatoday.in/india-today-insight/story/from-the-india-today-archives-2013-2611-inside-the-secret-world-of-david-coleman-headley-2382649-2023-05-22

Neeraj Chauhan, "Indian Mujahideen Wanted To Nuke Surat, Yasin Bhatkal Tells Cops," Times of India, December 30, 2013, https://timesofindia.indiatimes.com/india/indian-mujahideen-wanted-to-nuke-surat-yasin-bhatkal-tells-cops/articleshow/28116663.cms

Rajeswari Pillai Rajagopalan et al., "Nuclear Security In India, Second Edition," Observer Research Foundation (2016), https://www.orfonline.org/public/uploads/posts/pdf/20230411113546.pdf.

International Atomic Energy Agency, "IAEA Safeguards Glossary 2001 Edition," International Atomic Energy Agency, June 2002, https://www.iaea.org/sites/default/files/iaea_safeguards_glossary.pdf.

International Atomic Energy Agency, "IAEA Safeguards Glossary 2001 Edition,"

"Nuclear Notebook," Bulletin of the Atomic Scientists, May 7, 2024, https://thebulletin.org/nuclear-notebook/.

World Nuclear Association, "Nuclear Power In India | Indian Nuclear Energy," World Nuclear Association, February 2024, https://world-nuclear.org/information-library/country-profiles/countries-g-n/india.aspx.

Amitav Mallik, "National Security Challenges and Competition for India: Defence and Space R&D In a Strategic Context," Technology in Society, August 1, 2008, https://doi.org/10.1016/j.techsoc.2008.04.015; and Harsh V. Pant and Kartik Bommakanti, "India's National Security: Challenges and Dilemmas," International Affairs, July 1, 2019, https://doi.org/10.1093/ia/iiz053.

Yashwant Raj, "Lashkar Also Pak Proxy, Says Mullen," Hindustan Times, September 29, 2011, https://www.hindustantimes.com/world/lashkar-also-pak-proxy-says-mullen/story-QPvrNL6wwhYtKohD0JNq9N.html.

John P. Dickerson, A. Mannes, and V. S. Subrahmanian, "Dealing With Lashkar-e-Taiba: A Multi-player Game-Theoretic Perspective," European Intelligence and Security Informatics Conference (2011), https://www.semanticscholar.org/paper/Dealing-with-Lashkar-e-Taiba%3A-A-Multi-player-Dickerson-Mannes/9116eaaeb545e423ee1ffa66b9a88b5449a845f2.

Daniel S. Markey, "No Exit From Pakistan," Council on Foreign Relations, August 19, 2013, https://www.cfr.org/book/no-exit-pakistan.

Neeraj Chauhan, "Indian Mujahideen Wanted To Nuke Surat, Yasin Bhatkal Tells Cops," The Times of India, December 13, 2013, https://timesofindia.indiatimes.com/india/Indian-Mujahideen-wanted-to-nuke-Surat-Yasin-Bhatkal-tells-cops/articleshow/28116663.cms

Press Trust of India, "China Defends Blocking Listing Of Azhar As Global Terrorist; Says Not Protecting Violent Islamists," The Economic Times, March 29, 2019, https://economictimes.indiatimes.com/news/defence/azhar-listing-in-un-china-denies-its-action-amounted-to-sheltering-terrorists/articleshow/68630125.cms?from=mdr.

Neeraj Chauhan, "Indian Mujahideen wanted to nuke Surat, Yasin Bhatkal tells cops."

Graham Allison, "Could Terrorists Be Seeking a Nuclear Bomb?," Belfer Center for Science and International Affairs, March 18, 2014, https://www.belfercenter.org/publication/could-terrorists-be-seeking-nuclear-bomb

Christoph Wirz and Emmanuel Egger, "Use of Nuclear and Radiological Weapons by Terrorists?" International Review of the Red Cross, Vol 87, September 2005, https://international-review.icrc.org/sites/default/files/irrc_859_5.pdf.

World Nuclear Association, “Nuclear Power in India | Indian Nuclear Energy.”

Rajeswari Pillai Rajagopalan, “Nuclear Security in India.”

Shaun Gregory, “Terrorist Tactics In Pakistan Threaten Nuclear Weapons Safety,” CTC Sentinel, June 2011, https://ctc.westpoint.edu/terrorist-tactics-in-pakistan-threaten-nuclear-weapons-safety/

Michelle Macander, “Examining Extremism: Lashkar-e-Taiba,” CSIS, October 28, 2021, https://www.csis.org/blogs/examining-extremism/examining-extremism-lashkar-e-taiba.

Mohammed Sinan Siyech, “The Return Of the Taliban: ‘Foreign Fighters’ and Other Threats To India’s Security,” Observer Research Foundation, December 4, 2023, https://www.orfonline.org/research/the-return-of-the-taliban-foreign-fighters-and-other-threats-to-india-s-security.
Michelle Macander, “Examining Extremism: Lashkar-e-Taiba.”

National Counterterrorism Centre, “Jaish-E-Mohammed (JeM),” Office of the Director of National Intelligence, United States of America, https://www.dni.gov/nctc/groups/jem.html.

BBC News, “Pulwama Attack: Pakistan Warns India Against Military Action,” BBC News, February 19, 2019, https://www.bbc.com/news/world-asia-india-47290107.

C. Christine Fair, “The Milli Muslim League: The Domestic Politics Of Pakistan’s Lashkar-e-Taiba,” Hudson Institute, June 3, 2018, https://www.hudson.org/national-security-defense/the-milli-muslim-league-the-domestic-politics-of-pakistan-s-lashkar-e-taiba; Ashley J. Tellis, “The Menace That Is Lashkar-e-Taiba,” Carnegie Endowment for International Peace, March 13, 2012, https://carnegieendowment.org/posts/2012/03/the-menace-that-is-lashkar-e-taiba?lang=en

Dickerson, Mannes, and Subrahmanian, “Dealing With Lashkar-e-Taiba: A Multi-Player Game-Theoretic Perspective.”

Pratul Ahuja and Rajat Ganguly, “The Fire Within: Naxalite Insurgency Violence In India,” Small Wars & Insurgencies, June 1, 2007, https://doi.org/10.1080/09592310701400861.

P. Ahuja and Rajat Ganguly, “The Fire Within: Naxalite Insurgency Violence in India,” (2007), https://www.semanticscholar.org/paper/The-Fire-Within%3A-Naxalite-Insurgency-Violence-in-Ahuja-Ganguly/e1695bd9c4192b006a2c5a1c6b62f6d5e40aea55.

Binalakshmi Nepram and Brigitta W. Schuchert, “Understanding India’s Manipur Conflict and Its Geopolitical Implications,” United States Institute of Peace, June 2, 2023, https://www.usip.org/publications/2023/06/understanding-indias-manipur-conflict-and-its-geopolitical-implications.