Nuclear Security In A Time Of Crisis

Nickolas J. Roth, Christopher Hobbs, Daniel Salisbury
Stimson Center, Washington, DC, USA, Kings College, London, United Kingdom.

Abstract:

The COVID-19 global pandemic has had a significant impact on the implementation of security across a wide range of industrial sectors. As an event, it is largely unprecedented in terms of its global scale, its expected duration, and its targeted impact on the human element of organizations. In the nuclear sector, governments, regulators and operators have had to quickly put in place new measures to protect the health of staff, while at the same time continuing to ensure the security of nuclear material, sensitive information and systems. While the wide-ranging impact of the COVID-19 pandemic is arguably unique, this is not the first time that the nuclear industry has had to respond to external crises that have necessitated adaptation. The analysis of these incidents has largely focused on safety but maintaining security during a crisis is equally important. This paper will review findings from a recent handbook published by Kings College and the Stimson Center. The handbook includes case studies of how nuclear operators responded during times of crisis and how those crises impacted nuclear security operations, including security culture, physical protection measures, material accounting, and access control.

Introduction

Organizations responsible for reducing the risk of nuclear theft or sabotage must sustain high levels of security at all times. The COVID-19 pandemic has demonstrated that this can be particularly challenging during times of crisis.[1] Yet, this recent crisis is not the first time nuclear operators have had to provide security during a crisis. Nuclear facilities around the world have had to face political, economic, or societal turmoil, and natural disasters. Nor will this be the last. The effects of climate change, for example—from fires to storms to political instability—will impact ever industry in the world.

Kings College and the Stimson Center have published a handbook identifying lessons from historical case studies on how to sustain nuclear security during crises.[2] The handbook describes how four major crises impacted nuclear facilities: the Cerro Grande wildfire in the United States, the Break-up of the Soviet Union, perceived terrorist threats in Belgium, and Fukushima nuclear disaster in Japan. These crises have not been chosen to discuss specific nuclear incidents – nuclear accidents, security breaches at facilities or otherwise. Rather, like the Covid-19 pandemic, the cases selected consider the impact of broader events – wildfires, tsunamis, economic and political collapse – that are often external to an individual organisation or even the nuclear sector as a whole – and often have more far-reaching implications. The purpose of these case studies is to consider responses, challenges and opportunities in the organisational context.

What is a crisis?

There are many definitions for a crisis. We use Harmann's frequently cited definition. 'An organizational crisis (1) threatens high priority values of an organization, (2) presents a restricted amount of time in which a response can be made, and (3) is unexpected or unanticipated by the organization.'[3]

The cause, scale, and duration of crises vary greatly, but all have common characteristics. They all challenged nuclear organizations and their ability to meet basic missions goals; developed rapidly and required quick decision-making solutions—with the significance of the threat enhancing the urgency with which the crisis must be addressed; and were all unforeseen or deemed to be so unlikely that they didn't merit a great deal of consideration, often until it is too late.

Nuclear operators, regulators, government agencies, facilities and their personnel – in short all nuclear organisations – must respond to crises whether they are ready or not. Much focus is placed on emergency preparedness and response for nuclear emergencies in the area of nuclear safety.[4] Similarly, in the area of nuclear security, there has been much consideration of emergency preparedness and response to nuclear security events involving theft, sabotage or material out of regulatory control.[5] The following sections of the paper summarize findings and recommendations from the handbook.

Case Study I: Maintaining Nuclear Security during the Cerro Grande Wildfire in the United States

One of the most important and most extensively studied examples of a wildfire threatening a nuclear facility was the Cerro Grande Fire in May 2000. At the time, it was the largest fire in New Mexico's history, burning approximately 75 square miles of land in 16 days. The fire burned about a quarter of the 43-square mile area of Los Alamos National Laboratory (LANL)'s property, causing hundreds of millions of dollars in damage to the facility, destroying research, equipment, and many structures, and forcing it to shut down from May 7 until May 22.[6] While none of the five LANL locations, where weapons-useable nuclear material was stored at the time, were destroyed, catastrophe was only narrowly averted. There was extensive damage to areas around nuclear storage facilities.[7] The fire burned close to the plutonium facility at Technical Area 55 and its supporting buildings and damaged land near the Critical Assembly Facility at Technical Area 18.

The fire caught the facility off guard, disrupting security operations, creating confusion, and raising questions about the condition of nuclear material on-site. It also occurred at time where LANL was addressing longstanding systemic security problems.[8] The crisis also inspired employees to improvise, creating new analytical tools and information-sharing mechanisms.

During the fire, there was significant chaos and confusion among LANL leadership, emergency responders, and staff. LANL did not have a centralized list or method of tracking employees during the evacuation.[9] It was unclear what the access and re-entry requirements were for the site during the emergency because there was no single authority in charge of the process. Badges were created as individuals or organizations were added to the response efforts, often leaving the security contractor who managed perimeter access control addled, unsure of what badges were open to malicious use or duplication.

There was a notable success story that displayed coordination and communication, through the geographic information system (GIS) teams. GIS teams were formed ad hoc through the recognition during the crisis that critical facility information was not being communicated at the senior level.[10] They helped to provide local first responders with detailed maps of LANL and the location of nuclear material storage sites.

When employees returned to the site on May 23, “no one knew the status of the nuclear materials held at LANL and several questions needed to be addressed by the MC&A [Material Control and Accountability] personnel before normal MC&A operations could be permitted to resume.”[11] It took weeks for material balance areas to resume normal MC&A operations.

Many factors help to explain how LANL responded to the Cerro Grande fire, including lack of detailed contingency plans and performance testing, inadequate communications systems, and confusing lines of authority. Despite the many problems that occurred, this crisis could have been much worse. No lives were lost, and nobody was injured during LANL’s evacuation. The fire did not destroy any facilities that housed weapons-useable nuclear material and no material was stolen. While luck played a role, credit must be given to those who worked to prevent catastrophe.[12]

There are, however, numerous lessons to be learned from mistakes made prior to and during the crisis.[13] In terms of emergency preparation, nuclear facilities should have comprehensive emergency and recovery plans that are documented and well-understood by all staff. Furthermore, while cyber security was in its infancy when this fire occurred, many of the strategies employed during the crisis would raise serious concerns today about whether LANL systems or sensitive data could be compromised. Emergency planning must include contingencies for accessing data in a secure manner in the event of an evacuation. Facilities should also have an institutional prioritized list of essential facilities that need to be restarted in the event of a facility-wide shutdown in their emergency plans. And resources should be available to restart those facilities.

The response to the fire demonstrated the challenges with maintaining access control during the emergency response and recovery phases. Procedures should be incorporated into emergency response plans for entry and re-entry into the facility during the emergency phase and during the recovery phase. This should include identification of key personnel, emergency responders, or other officials who require site access. In addition, throughout the emergency response, organisational leadership and security forces must have access to real-time, site-specific information in order to continually assess risk throughout the crisis. Finally, rigorous performance testing of these plans is necessary to determine whether security forces can maintain security during a crisis.

After the event, an alarming report identified that while the protective force was prepared to provide security services in case of a “severe natural phenomena event or catastrophic event”, a written response had not been developed ‘to guide security operations after a catastrophic event with severe consequences’.[14] There has been further progress in strengthening LANL security during emergencies, though challenges remain.[15] The Cerro Grande fire was an unprecedented crisis that illustrated the many challenges associated with protecting a nuclear facility during a wildfire. Comprehensive planning, training, and communication are all critical in responding to such a potentially catastrophic event.

Case Study II: Nuclear Security in Russia following the Break-up of the Soviet Union

The dissolution of the Soviet Union prompted radical economic, social and political changes, resulting in an unprecedented crisis for the nuclear sector in Russia and other former Soviet states, with serious implications for the delivery of nuclear security.[16] By mid-1998, Russia’s economy had ‘reached the brink of economic collapse’, interest rates were exorbitant, and several major banks had gone bankrupt.[17] The situation then improved over the next decade, albeit slowly, as a result of increasing global oil and gas prices which boosted Russia's export earnings.[18] The initial economic downturn resulted in deep cuts to Russia's nuclear spending, with facilities unable to purchase essential nuclear security equipment.

Stagnating investment, production and consumption, delayed pay checks and mass-layoffs were an everyday reality in the nuclear and other industrial sectors.[19] Formerly well paid and highly privileged nuclear scientists and security managers were suddenly either poorly compensated for their work or laid off.[20] Due to the high level of inflation, purchasing power and personal savings and highly privileged nuclear scientists and security managers were suddenly either poorly compensated for their work or laid off.[21] An informal economy grew as people exchanged favours rather than money to make ends meet.[22] This societal turmoil was felt within Russia's nuclear workforce, where it translated into apathy with respect to security measures and, in certain extreme cases, 'insider' incidents – involving personnel stealing and attempting to sell nuclear materials.

The unstable environment in Post-Soviet Russia created two major interrelated proliferation concerns.[23] First, it was feared that nuclear weapons scientists, that had either been made unemployed or had their salaries dramatically reduced, could seek new more profitable employment working for rogue states or terrorist groups. Second, worries were voiced that nuclear personnel might attempt to steal sensitive nuclear materials or information from Russian facilities, for sale on the black-market, either acting alone or having been recruited by criminal organisations.

With the dissolution in effective nuclear security oversight and financial support, the management of many nuclear facilities increasingly 'failed to prioritise security over other tasks'; instead, there was greater 'emphasis on boosting production and improving sales'.[24] Responding to the economic decline, cuts were primarily made to physical protection systems and security personnel. At many sites, equipment was operated well beyond its service life; when such equipment finally broke down it was often left as sites lacked the funds to purchase a replacement, or expertise to conduct repairs.[25] Electronic systems were also affected by power outages, with electricity cut off by the energy utility if facilities failed to pay their bills on time. At certain facilities staff members also intentionally 'switched off the power on weekends to save money'.[26]

In the Soviet Union era, nuclear security was largely concerned with external adversaries and state espionage, with emphasis placed on denying unauthorised access to facilities rather than identifying potential internal adversaries. Such an approach was no longer effective in post-Soviet Russia, where increasingly demotivated staff working at many nuclear facilities struggled to make ends meet. This was particularly true in remote locations where the nuclear facility was often the only high-income employer. As unemployment rose and salaries declined, 'the morale at these remote facilities fell precipitously', with nuclear security an issue of little concern for most employees.[27]

In stealing nuclear materials insiders took advantage of the aforementioned degraded and outdated security measures. One area of particular weakness was Nuclear Material Accounting and Control, an essential process in guarding against material theft, particularly given the vast quantities of nuclear materials handled at many Russian facilities. This allowed both rogue individuals and facility managers to manipulate production figures, without internal or external detection. The lack of oversight in the system enabled materials to be removed without showing up on the balance sheet. Materials could then potentially be sold on the black-market, or alternatively artificially added to boost production outputs in order to meet key government quotas.[28]

Recognising the worsening state of nuclear security in the FSU, the United States and other Western countries launched a concerted programme of engagement with the Russian authorities on nuclear and broader CBRN security during the 1990s and beyond. These efforts provided funding, equipment and other support aimed at maintaining and improving security systems at key facilities. Major initiatives included the Nunn-Lugar Cooperative Threat Reduction Program, established in 1991, and later the G8 Global Partnership against the Spread of Weapons and Materials of Mass Destruction, launched in 2002.[29] Washington and Moscow also engaged in bilateral initiatives that, at least until the 2010s, were effective in building trust over nuclear security matters.

Nuclear activities were focused on helping Russia improve its material protection, control and accounting (MPC&A), through efforts that included the provision of security equipment and technology to tens of Russian nuclear sites. New high-tech surveillance systems and alarms, and also more basic but crucial items such as security fences and barriers, were supplied to replace ageing infrastructure. Furthermore, key security processes were revised including new protocols for access control at sites and the introduction of a two-person rule in sensitive areas. In making these improvements, key security concepts and approaches utilised at US nuclear weapons facilities were transplanted to Russian sites.[30]

More broadly, efforts to strengthen Russia's nuclear security were hampered by an outdated legal and regulatory framework and ineffective security policies and procedures. The initial focus of international programmes on the provision of equipment and technology also lacked due consideration of how such programmes would fit into existing working practices. The impact of these challenges can be seen in remarks by Senator Richard Luger in 2004, in which he noted that hundreds of tonnes of fissile material had yet to be 'adequately secured', and that tens of sites 'needed more protection'.[31]

Given the potentially catastrophic consequences that could result from the theft of nuclear material, swift action was required by the international community, with emphasis placed on physical upgrades and provision of security technology. However, this narrow focus meant that little consideration was initially given as to how these new technologies would fit into existing systems and practices.[32] Such an approach served to created implementation challenges, with US observers reporting back that new security systems were not always operated reliably.[33] Here difficulties stemmed from a lack of detailed training, the expense of maintaining and updating high-tech equipment, and a prevailing sense of suspicion by Russian security personnel in relation to US technology.[34] In addition, the regular testing of high-tech MPC&A equipment and systems, necessary to ensure their effectiveness, was not common practice in Russia – and it took considerable time for appropriate protocols to be introduced.[35]

It soon became clear that the human factor within nuclear security systems would also need to be strengthened. Essentially, nuclear security depends to a considerable extent on the ability, understanding and motivation of personnel to recognise potential threats and take appropriate actions. This was particularly important in Russia in the early 1990s given the broader social and economic challenges of the time and the ongoing transition away from a Soviet system that was 'characterized by Communist ideology and strong, indeed totalitarian, control, [which] powerfully discouraged personal initiative and responsibility'.[36]

In an effort to promote and strengthen nuclear security culture in Russia, particular attention was focused on changing the attitudes and behaviours of senior managers at facilities and developing a new cadre of nuclear leaders. The issue of leadership and management was deemed particularly important given that ‘Russian political culture has traditionally combined collectivism and suppression of personal initiative with a high reliance on leadership’, in stark contrast ‘with the individualism and personal initiative encouraged’ in Western countries.[37] This was reflected in the Russian nuclear sector where leaders exhibited significant influence as well as a considerable amount of leeway and personal discretion when it came to nuclear security decision making. Leaders could have a huge impact on changing security culture, as demonstrated at the aforementioned Luch Scientific Production Association, where a change to a facility leadership ‘who made security… a priority’ resulted in the facility becoming viewed as ‘a model site’.[38]

While the ‘crisis’ discussed in this case study – focusing on the turmoil of 1990s Russia – is arguably unique in terms of scale and duration, a number of broader lessons can be extracted that may support efforts to tackle ongoing and future crises.

First is the importance of taking a holistic and fully integrated approach to improving a national nuclear security regime. This should take into account not just the strengthening of security at the facility but also the potential development of new laws and legislations and regulatory approaches. At the site level the introduction of new security technology should be accompanied by the potential revision of associated guidance, process and protocols. Here it is essential that due consideration is given to how they fit into existing working practices, particularly if delivered as part of an international programme, as national differences may require modifications to how these systems are operated.

Second, in extreme cases it may be necessary to tackle some of the broader effects of the crisis, due to the significant impact they may have on both nuclear threats and the implementation of security. In the case of Russia during the 1990s, the provision of subsidised meals, staff wages and the restructuring of nuclear organisations to help avoid additional unemployment all helped to strengthen nuclear security, while reducing the potential for insiders.

Third, it is essential to address not just the technical but also the human factor within nuclear security systems. This was neglected in early efforts to strengthen nuclear security in Russia in the 1990s but became an important part of subsequent engagement programmes. Here it was recognised that changing the culture at Russian nuclear sites proved to be a difficult undertaking, far greater than ‘building a fence or installing an alarm’.[39] It was ultimately recognised that taking into account the existing culture, and considering how this can be enhanced, was a more sustainable approach, as opposed to attempting to transplant nuclear security practices wholesale with what may be a very different culture and way of working.

Case Study III: Maintaining Nuclear Security Confidence amid a Perceived Terrorist Threat in Belgium

Between 2015 and 2016 Belgium faced an elevated terrorist risk to its nuclear facilities. Since 2014, radicalised Belgian nationals had indicated potential to launch highly lethal terrorist attacks. When the potential of a nuclear plot became public knowledge, it created a crisis in confidence, which was further elevated by terrorist bombings in Brussels. The Belgian Federal Agency for Nuclear Control responded by introducing temporary measures to mitigate the outstanding security threat as well as to dispel rumours circulating in the press. While Belgium’s regulator and operators had proven reticent to introduce additional security procedures due to the unique nuclear politics of the country, the perception of crisis allowed for the introduction of new security measures, overcoming prior barriers. These changes were significant to the extent that by the end of March 2016, previously critical US observers remarked that "Belgium… [had] made some of the most substantial nuclear security improvements in the world."[40]

However, it is clear that the apparent reluctance to introduce more robust measures and prior incidents influenced contemporary perceptions of nuclear security even as improvements were underway. Some measures that were rapidly introduced, such as the introduction of armed guards, were initially operationally constrained and it has taken time to fully integrate them into Belgium's nuclear security regime.[41] This highlights that upholding credibility in nuclear security needs to be undertaken proactively and before a crisis unfolds to maintain confidence. This allows for the progressive introduction and socialisation of new security measures to ensure effective implementation before they are potentially tested with a real-life event.

Case Study IV: Nuclear Security Reform in Japan following the 2011 Nuclear Disaster

The Fukushima Daiichi nuclear disaster confronted not only Japan's nuclear industry but nuclear stakeholders across the world with the reality of a low-probability, high-consequence event. In doing so, false assumptions and lazy confidence about nuclear safety in advanced nuclear countries were overturned. The Fukushima disaster also highlighted the benefits of exploiting the synergies between nuclear safety and nuclear security incidents, not only as implementing mechanisms are often relevant for both spheres but because during an unfolding crisis, key decisions will need to be made that may impact the other. Meanwhile, the disaster served as a first 'test case' of Japan's response to a potential CBRN (chemical, biological radiological or nuclear) attack, which would require a large-scale civil evacuation and site contamination.[42] It revealed that a multi-agency operation would be required, involving not just the deployment of the various emergency services but the integration of public and private entities.

Crucially, inadequate communication across all levels of decision-making undermined the emergency response in the days following the Fukushima Daiichi disaster.[43] The impacts of the earthquake and particularly the tsunami on security systems at Fukushima Daiichi were considerable. The disaster caused 'substantial' degradation in aspects of particular relevance to nuclear security.[44] This included the enormous damage to physical infrastructure, most notably to plant access controls in the protected areas and security equipment failure lasting days. [45] The disaster also resulted in the absence of onsite security personnel as a result of evacuation.[46]

Another weakness in nuclear security was the lack of documentation for many of the workers engaged in the clean-up operation. At least 69 of them were not traceable in 2013, a year after they had last entered the site which prevented follow-up health checks.[47] Indeed, there was a general weakness in monitoring of onsite personnel throughout the acute crisis phase, despite the vast numbers of TEPCO staff, contractors and multi-agency personnel entering and leaving the plant. Few of these workers had been subjected to thorough background checks.[48]

Conclusion

Although they rarely receive attention, crises are not unprecedented in nuclear operations. As shown by the preceding case studies, nuclear operators often have to adapt in the face of natural disasters. When these types of stories are shared, the focus is frequently on the more established, and sometimes more immediate concern, surrounding nuclear safety. Yet, it is equally critical to maintain security during these events.

A resilient nuclear security system – that is capable of adapting to shocks – is one where security is prioritised throughout an organisation. Nuclear security culture is a concept that has developed in recent decades to encompass this continual prioritisation. A strong security culture should not only be central to effective nuclear security in normal times, but without good security culture organisations are more likely to buckle under the pressure of a crisis situation.

A number of other lessons have been extracted from the above crisis case studies: Nuclear operators should have focused programmes that address the human elements of nuclear security within their organisations; mechanisms in place to provide adequate assurances to stakeholders about nuclear security implementation; plans in place for fast recovery from shocks; and rigorous programmes that evaluate nuclear security performance under a range of realistic scenarios and then incorporate that data into security operations. Regulators must also provide strong independent oversight to ensure security remains a continuous priority. Governments, sometimes in cooperation, must ensure there are dedicated resources to recapitalise security infrastructure during the recovery period.

[1] Christopher Hobbs, Nickolas Roth & Daniel Salisbury (2021) Security Under Strain? Protecting Nuclear Materials During the Coronavirus Pandemic, The RUSI Journal, 166:2, 40-50, https://www.tandfonline.com/doi/full/10.1080/03071847.2021.1937302.

[2] Geoffrey Chapman, Rebecca Earnhardt, Christopher Hobbs, Nickolas Roth, Daniel Salisbury, Amelie Stoetzel and Sarah Tzinieris, “Nuclear Security in Times of Crisis,” Kings College London and Stimson Center, 2021, https://www.stimson.org/wp-content/uploads/2021/07/nuclear-security-in-times-of-crisis-handbook.pdf.

[3] Charles F. Hermann, ‘Some Consequences of Crisis Which Limit the Viability of Organisations’, Administrative Science Quarterly, 1963, p.61-82.

[4] See for example ‘Preparedness and Response for a Nuclear or Radiological Emergency’, IAEA Safety Standards, No. GSR Part 7, 215. https://www. iaea.org/publications/10905/preparedness-and-response-for-a-nuclear-or-radiological-emergency.

[5] See for example ‘Developing a National Framework for Managing the Response to Nuclear Security Events’, IAEA Nuclear Security Series, No.370G, 2019. https://www.iaea.org/publications/13489/developing-a-national-framework-for-managing-the-response-to-nuclear-security-events.

[6] Webb, M. D and K. Carpenter, "The Cerro Grande Fire, Los Alamos, New Mexico" (Los Alamos, New Mexico: Los Alamos National Laboratory, 2001), https://permalink.lanl.gov/object/tr?what=info:lanl-repo/lareport/LA-UR-01-1630.; William Earl Haag, "Material Control and Accountability (MC&A): Recovery from the Cerro Grande Fire at Los Alamos National Laboratory" (Los Alamos, New Mexico: Los Alamos National Laboratory, 2001), https://www.osti.gov/servlets/purl/975592.

[7] William Earl Haag, "Material Control and Accountability (MC&A): Recovery from the Cerro Grande Fire at Los Alamos National Laboratory" (Los Alamos, New Mexico: Los Alamos National Laboratory, 2001), https://www.osti.gov/servlets/purl/975592.

[8] Gregory Friedman, "Summary Report on Inspection of Allegations Relating to the Albuquerque Operations Office Security Survey Process and the Security Operations' Self-Assessment at Los Alamos Laboratory” (Washington, D.C.: Department of Energy,2000), https://fas.org/sgp/othergov/doeig_0471.html.

[9] C. A. Salazar-Langley, D. L. Hall, and C. G. Coffman, "Cerro Grande Fire: Laboratory Recovery Lessons to be Learned Report" (Los Alamos, New Mexico: Los Alamos National Laboratory, 2000), p. 13, https://permalink.lanl.gov/object/tr?what=info:lanl-repo/lareport/LA-UR-01-1305.

[10] C. R. Mynard et al., "Geographic Information Systems (GIS) Emergency Support for the May 2000 Cerro Grande Wildfire" (Los Alamos, New Mexico: Los Alamos National Laboratory, 2003), https://doi.org/10.2172/812177.

[11] William Earl Haag, "Material Control and Accountability (MC&A): Recovery from the Cerro Grande Fire at Los Alamos National Laboratory" (Los Alamos, New Mexico: Los Alamos National Laboratory, 2001), https://www.osti.gov/servlets/purl/975592.

[12] C. A. Salazar-Langley, D. L. Hall, and C. G. Coffman, "Cerro Grande Fire: Laboratory Recovery Lessons to be Learned Report" (Los Alamos, New Mexico: Los Alamos National Laboratory, 2000), https://permalink.lanl.gov/object/tr?what=info:lanl-repo/lareport/LA-UR-01-1305.

[13] Cristina A. Salazar-Langley, Debora L. Hall and Cindy G. Coffman, 'Cerro Grande Fire: Laboratory Recovery Lessons to be Learned Report', Los Alamos, New Mexico: Los Alamos National Laboratory, 2000, p.6. https://permalink.lanl.gov/object/tr?what=info:lanl-repo/lareport/LA-UR-01-1305.

[14] 'Independent Oversight Review of Site Preparedness for Severe Natural Phenomena Events at the Los Alamos National Laboratory', United States Department of Energy, 2012, p.25. https://www.energy.gov/sites/prod/files/hss/Enforcement%20and%20Oversight/Oversight/docs/reports/semevals/2012_LANL_Site_Preparedness_for_Severe_Natural_Phenomena_Events.pdf

[15] 'Emergency Management Assessment at the Los Alamos National Laboratory', Office of Enterprise Assessments, United States Department of Energy, August 2020. https://www.energy.gov/sites/prod/files/2020/08/f77/LANL%20Emergency%20Mgmt%20Report.pdf

[16] Angus Maddison, 'The World Economy', Development Centre Studies, OECD, 2006, p.155. https://www.stat.berkeley.edu/~aldous/157/Papers/world_economy.pdf

[17] National Research Council, *Protecting Nuclear Weapons Material in Russia*, The US National Academies Press, 1999, p.11. https://doi.org/10.17226/9469; Homi Kharas, Brian Pinto and Sergei Ulatov, 'The Analysis of Russia's 1998 Meltdown: Fundamentals and Market Signals', *Brookings Papers on Economic Activity,* No.1, 2001, p.8.

[18] Kristi Govella and Vinod K. Aggarwal, 'Introduction: The Fall of the Soviet Union and the Resurgence of Russia', in Vinod K. Aggarwal and Kristi Govella (eds.), *Responding to a Resurgent Russia: Russian Policy and Responses from the European Union and the United States*, New York: Springer, Science and Business Media, 2012, p.6.

[19] Wendy L. Mirskey, 'The Link between Russian Organized Crime and Nuclear-Weapons Proliferation: Fighting Crime and Ensuring International Security', Penn Law: Legal Scholarship Repository, 2014, p.764. https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=1504&context=jil.

[20] Wendy L. Mirskey, 'The Link between Russian Organized Crime and Nuclear-Weapons Proliferation: Fighting Crime and Ensuring International Security', Penn Law: Legal Scholarship Repository, 2014, p.764. https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=1504&context=jil.

[21] Wendy L. Mirskey, 'The Link between Russian Organized Crime and Nuclear-Weapons Proliferation: Fighting Crime and Ensuring International Security', Penn Law: Legal Scholarship Repository, 2014, p.764. https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=1504&context=jil

[22] John Round and Colin Williams, 'Coping with the social costs of 'transition': Everyday life in post-Soviet Russia and Ukraine', *European Urban and Regional Studies,* Vol.17, No.2, 2010, p.188.

[23] Oleg Bukharin, 'Nuclear Safeguards and Security in the Former Soviet Union', *Survival,* Vol. 36, No.4, 1994, p.53.

[24] Igor Khripunov and James Holmes (eds.), *Nuclear Security Culture: The Case of Russia*, Center for International Trade and Security, University of Georgia, 2004, p.56. https://media.nti.org/pdfs/analysis_cits_111804.pdf

[25] Ibid., p.22.

[26] Ibid., p.23.

[27] Igor Khripunov and James Holmes (eds.), *Nuclear Security Culture: The Case of Russia*, Center for International Trade and Security, University of Georgia, 2004, p.20. https://media.nti.org/pdfs/analysis_cits_111804.pdf

[28] National Research Council, *Proliferation Concerns: Assessing U.S. Efforts to Help Contain Nuclear and Other Dangerous Materials and Technologies in the Former Soviet Union,* The US National Academies Press, 1997, p.55. https://doi.org/10.17226/5590

[29] 'The Evolution of Cooperative Threat Reduction: Issues for Congress', Congressional Research Service, 23 November 2005, p.19. https://fas.org/sgp/crs/nuke/R43143.pdf

[30] Todd Perry, 'Securing Russian Nuclear Materials: The Need for an Expanded US Response', *The Nonproliferation Review,* Vol.6, No.2, 1999, p.86.

[31] 'Persistent Diplomacy Needed for Nonproliferation Advances', United States Department of State, 11 August 2004. https://media.nti.org/pdfs/170.pdf

[32] Igor Khripunov, Nikolay Ischenko and James Holmes, 'Nuclear Security Culture: From National Best Practices to International Standards', *NATO Science for Peace and Security Studies,* Vol. 28, 2007, p.76.

[33] Nathan E. Busch and James R. Holmes, ''The 'Human Factor' and the Problem of Nuclear Security in Russia', *Perspectives on Political Science,* Vol.34, No.3, 2005, p.157.

[34] Ibid.

[35] National Research Council, *Protecting Nuclear Weapons Material in Russia*, The US National Academies Press, 1999, p.18-19.

[36] Igor Khripunov and James Holmes (eds.), *Nuclear Security Culture: The Case of Russia*, Center for International Trade and Security, University of Georgia, 2004, p.58. https://media.nti.org/pdfs/analysis_cits_111804.pdf

[37] Ibid., p.29.

[38] National Research Council, *Protecting Nuclear Weapons Material in Russia*, The US National Academies Press, 1999, p.2.

[39] Ibid., p.viii.

[40] Matthew Bunn, Martin B. Malin, Nickolas Roth and William H. Tobey, 'Preventing Nuclear Terrorism: Continuous Improvement or Dangerous Decline?' Belfer Center, Harvard Kennedy School, 2016, p.54. https://www.belfercenter.org/sites/default/files/legacy/files/PreventingNuclearTerrorism-Web.pdf

[41] Patrick Malone, 'Belgium Orders Immediate Security Upgrade at Its Nuclear Sites', Center for Public Integrity, 11 March 2016. https://publicintegrity.org/national-security/belgium-orders-immediate-security-upgrade-at-its-nuclear-sites

[42] Nobumasa Akiyama, 'Japan's Nuclear Security after the Fukushima Nuclear Accident', Nautilus Institute, 19 May 2017. https://nautilus.org/napsnet/napsnet-special-reports/japans-nuclear-security-after-the-fukushima-nuclear-accident/

[43] Scott Sagan and Edward Blandford (eds.) *Learning from a Disaster: Improving Nuclear Safety and Security after Fukushima,* Stanford: Stanford University Press, 2016

[44] 'Lessons Learned from the Fukushima Nuclear Accident for Improving Safety and Security of U.S. Nuclear Plants: Phase 2', National Academy of Sciences, 2016. https://www.nap.edu/catalog/21874/lessons-learned-from-the-fukushima-nuclear-accident-for-improving-safety-and-security-of-us-nuclear-plants

[45] Ibid.

[46] Ibid.

[47] Nobumasa Akiyama, 'Japan's Nuclear Security after the Fukushima Nuclear Accident', Nautilus Institute for Security and Sustainability, 19 May 2017. https://nautilus.org/napsnet/napsnet-special-reports/japans-nuclear-security-after-the-fukushima-nuclear-accident/

[48] Scott Sagan and Edward Blandford (eds.) *Learning from a Disaster: Improving Nuclear Safety and Security after Fukushima,* Stanford: Stanford University Press, 2016.