CENTRE FOR SCIENCE
& SECURITY STUDIES

KING'S College LONDON

Nuclear Security in Times of Crisis

Geoffrey Chapman, Rebecca Earnhardt, Christopher Hobbs, Nickolas Roth, Daniel Salisbury, Amelie Stoetzel and Sarah Tzinieris

STIMSON

2021

Table of Contents

Commonly Used Abbreviations

ACNS	Advisory Committee on Nuclear Security, Japan
ANRE	Agency for Natural Resources and Energy, Japan
BAER	Burned Area Emergency Rehabilitation, United States
BEIS	Department for Business, Energy and Industrial Strategy, United Kingdom
BLM	Bureau of Land Management, United States
CBRN	Chemical, biological, radiological and nuclear
CCTV	Closed circuit television
CPPNM	Convention on the Physical Protection of Nuclear Material
DAB	Directie van Beveiliging (Directorate of Security), Belgium
DBT	Design basis threat
DOE	Department of Energy, United States
DPRK	Democratic People's Republic of Korea (North Korea)
EDF	EDF Energy
FANC	Federal Agency for Nuclear Control, Belgium
FIMAD	Facility for Information Management, Analysis and Display, United States
FSU	Former Soviet Union
GAN	Gosatomnadzor (State Committee for Nuclear and Radiation Safety), Russia
GIS	Geographic information system
HEU	Highly enriched uranium
IAEA	International Atomic Energy Agency
INES	International Nuclear Event Scale
INFCIRC	IAEA's Information Circular
IPPAS	IAEA's International Physical Protection Advisory Service
LANL	Los Alamos National Laboratory, United States
LEU	Low enriched uranium
MAPI	Ministry of Atomic Power and Industry, Russia
MC&A	Material control and accountability
METI	Ministry of Economy, Trade and Industry, Japan
Minatom	Ministry for Atomic Energy, Russia
MPC&A	Material Protection, Control and Accounting
NISA	Nuclear and Industrial Safety Agency, Japan
NMAC	Nuclear material accounting and control
NRA	Nuclear Regulation Authority, Japan
NSC	Nuclear Safety Commission, Japan
NSCP	Nuclear Security Culture Programme, led by King's College London
NTI	Nuclear Threat Initiative, United States
OCAD	Coordination Unit for Threat Analysis, Belgium
RMTC	Methodological Training Center, Russia
SCK-CEN	Nuclear Research Centre, Belgium
SNM	Special nuclear material
TEPCO	Tokyo Electric Power Company, Japan
WMD	Weapons of mass destruction

Acknowledgements

This handbook has been developed by the Centre for Science and Security Studies (CSSS) at King's College London and the Nuclear Security Program at the Henry L. Stimson Center. The research and publication have been supported through the UK's Nuclear Security Culture Programme (NSCP), managed by the United Kingdom's Department for Business, Energy and Industrial Strategy (BEIS). The authors are grateful for the support provided by UK government under this programme, as well as the research assistance provided by Amport Risk Ltd, a specialist nuclear security and resilience consultancy.

Overview and Executive Summary

This publication explores how broader 'crises' – political, economic or societal turmoil, natural disasters or other major unforeseen events – may impact on nuclear security. The effects of these crises are examined through a series of case studies, which chart what can happen when nuclear security is placed under strain. In each case, intrinsic tensions and potential weaknesses are identified alongside the different steps taken to stabilise the situation and help ensure that the delivery of nuclear security remains effective. While the focus here is on the analysis of historical cases, general lessons are extracted which may help inform the implementation of nuclear security during the on-going global Covid-19 pandemic and future crises.

While Covid-19 is the latest crisis to impact nuclear facilities, it certainly will not be the last. For example, the effects of climate change are likely to have huge impacts on all sectors – including the nuclear industry. Natural disasters such as storms, flooding and forest fires exacerbated by global warming have already impacted upon the operations of nuclear facilities. Take for example the first case study in this publication, the 2000 Cerro Grande wildfire in the United States. Climate change will also have political and economic implications, with mass migration and enhanced competition for resources.[1] Studies, unfortunately, also suggest that the future will likely bring further and more frequent pandemic events.[2] Events of the recent past provide an important opportunity to learn and build resilience in nuclear organisations for a future rife with crises.

The cases considered in this handbook are diverse in terms of their underlying causes, scale and duration. Nevertheless, efforts have been made to extract a number of broader insights aimed at informing nuclear security measures at both the national and organisations levels, these are summarised below:

- Without the immediate threat posed by a crisis, generating buy-in to nuclear security reform can be challenging. However, the urgency to provide a solution in the face of crises can overcome prior organisational and political barriers. While this can be utilised to make improvements, the haste in implementing change to overcome a challenge may also lead to suboptimal solutions initially being imposed. The international community, government, regulators and operators must continue to work after the initial sense of crisis has passed to adapt reforms, in order to ensure they are effectively integrated into different organisations' ways of working. This approach will make organisations more sustainable in the longer term, improving resilience for future crises.

- Maintaining long-standing confidence in nuclear security outside of periods of crisis is crucial in determining the perceived resilience of a nuclear security system. In turn, this will determine how an organisation will be judged in the event of an unexpected security challenge. Perceptions about deficient performance or reluctance to reform in the face of cost or cultural issues are likely to heighten the sense of emergency, potentially undermining both governmental and public confidence in nuclear institutions. Therefore, government bodies, the regulator and operators should proactively improve their means of communicating with broader stakeholders and communicate efforts to improve nuclear security in order to avoid exacerbating a sense of emergency when challenged.

1 'Climate change 'will create world's biggest refugee crisis', The Guardian, 2 November 2017. https://www.theguardian.com/environment/2017/nov/02/climate-change-will-create-worlds-biggest-refugee-crisis
2 'Coronavirus: Pandemics will be worse and more frequent unless we stop exploiting earth and animals, top scientists warn', The Independent, 1 May 2020. https://www.independent.co.uk/environment/coronavirus-pandemic-virus-disease-wildlife-environment-farming-infectious-a9487926.html

- In extreme cases, it may be essential to also tackle some of the broader effects of the crisis, due to the significant impact they may have on both threats and the implementation of nuclear security. For example, in the case of Russia in the 1990s – following the collapse of the Soviet Union – 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 likelihood of insider threats. Tackling broader issues can go far beyond the responsibility or powers of nuclear organisations.

- It is essential to address not just technical deficiencies precipitated by crises but also to consider their impact on the human factor within nuclear security systems – and also how these can be strengthened. At some nuclear facilities the improvement of security culture may require considerable and sustained efforts. In the case of Russia in the 1990s, changing the security culture at Russian nuclear sites proved to be an undertaking far more challenging than upgrading technical security systems. In order to ensure sustainability, initiatives in this area should seek to take into account the existing culture within an organisation – with a focus on what drives behaviours and how targeted improvements can be made – rather than attempting to transplant another organisation's security culture wholesale.

- Nuclear facilities should have comprehensive institutional emergency and recovery plans for security operations that are documented and well-understood throughout the staff. Organisational leadership and security forces must have access to real-time, site-specific information in order to continually assess risk throughout the crisis. As demonstrated by the 2011 earthquake and tsunami in Japan, during a crisis, senior leadership should be present at the location where they can exert most impact in the course of events.

- In a crisis situation, the requirements for nuclear security and nuclear safety can sometimes come into conflict with one other. For example, in the case of a nuclear incident, safety personnel are focusing on preventing a nuclear meltdown and the release of radiation into the atmosphere, with the support of a wide range of emergency personnel who would not usually have access to the site. Even during a crisis, personnel onsite need to be authorised and monitored to ensure that nuclear materials and sensitive information are not removed or tampered with.

- During the response and recovery phase of a crisis the presence of unfamiliar contractors, new employees, emergency responders, and even the public (in the case where a facility is used as a shelter) at a nuclear facility can create significant confusion about who is authorised to enter. Emergency planning should include access control, including clearly defined access control management roles and responsibilities that scale according to the severity of the crisis. Procedures should be incorporated into plans for entry and re-entry into the facility during the emergency phase, and also during the recovery phase. This should include identification of key personnel, emergency responders, or other officials who require site access.

- Crises can help bring into the spotlight broader systemic weaknesses, providing opportunity for reform. For example, the 2011 Tōhoku earthquake and tsunami revealed that Japan's nuclear industry was suffering from 'regulatory capture'. Conflicts of interest between government and industry had resulted in a system where the delivery of nuclear safety and security was undermined by ineffective oversight, leadership and management structures.

- Performance evaluation is a valuable tool for assessing whether physical protection systems are effective; it can reveal vulnerabilities, reduce complacency and improve security implementation. Performance evaluation can take many forms like table-top exercises, computer simulations and force-on-force exercises, utilising a range of crisis scenarios. Broader security culture assessments can also yield important additional information on how an organisation may respond to different threats.

Before presenting the detailed case studies, the next section defines and introduces key concepts – outlining what constitutes a crisis and emphasising the importance of developing resilience and organisational culture.

Nuclear Security, Organisational Crises and Resilience

Before considering the case studies below, this section considers some key concepts and definitions, seeking to explain what factors are common to these diverse cases. The case studies contained in this handbook represent forms of 'organisational crisis' – a term used in wide range of fields from business studies to international relations. While there are many definitions of this term, there are a number of common characteristics. These are reflected in Hermann's much cited definition. He notes, 'An organisational crisis (1) threatens high priority values of an organisation,[3] (2) presents a restricted amount of time in which a response can be made, and (3) is unexpected or unanticipated by the organisation'. The utility of this definition is arguably its simplicity of capturing the nature of crises in the organisational context in terms of *challenge*, *urgency* and *surprise*. These three characteristics are expanded upon below in relation to the case studies explored:

- Challenge: Crises pose a challenge to the values of an organisation and its the ability to meet basic and fundamental goals. The crises explored below in this handbook all challenged the ability of nuclear organisations to undertake core business – whether generation of power in the case of Fukushima or conducting research in the cases of LANL and the Cerro Grande wildfire. With nuclear security increasingly being viewed as a core mission of nuclear organisations and as a business enabler, these crises also posed a challenge in this regard.
- Urgency: Crises develop rapidly and require quick decision-making and solutions – with the significance of the threat enhancing the urgency with which the crisis must be addressed. The crises explored in the handbook all developed relatively quickly – sometimes over a period of minutes and hours in the case of Fukushima, or in days and weeks with regard to the collapse of the Soviet Union.
- Surprise: Crises are often unforeseen or deemed to be so unlikely that they don't merit a great deal of consideration, often until it is too late. They might also be the result of complacency. Indeed, many of the crises explored in this handbook were to a large degree unforeseen.

The surprise and challenge characteristics mean that crises tend to be triggered by low probability-high consequence events.[4] However, when the three characteristics set out by Hermann are not met, the event in question is arguably not a crisis but a problem that has to be dealt with.[5]

True crises represent 'unique moments in the history of organisations', where their response can dictate their very survival.[6] Selecting case studies that feature these characteristics of organisational crises allows for insights to be drawn for mitigating the impacts of current and future crises on nuclear facilities.

Covid-19 has created challenges for most organisations in meeting their objectives. In 2019 few would have predicted a global pandemic, yet now a year into various lockdowns and other measures to control the spread of the virus Covid-19 has caused one of the largest economic recessions in human history. The 'urgency' characteristic means that responding to crises often requires 'uncertain

3 Charles F. Hermann, 'Some Consequences of Crisis Which Limit the Viability of Organisations', Administrative Science Quarterly, 1963, p.61-82.
4 K. E. Weick, 'Enacted sensemaking in crisis situations', Journal of Management Studies, 1988, p.305-317.
5 David Krackhardt and Robert N. Stern, 'Informal Networks and Organizational Crises: An Experiment Simulation', Social Psychology Quarterly, 1988, p.125.
6 Robert R. Ulmer, Timothy L. Sellnow, Matthew W. Seeger, Effective Crisis Communication: Moving From Crisis to Opportunity, Sage, 2011, p.5.

action under time pressure', and this has clearly been the case with Covid-19 – with governments rapidly enacting and modifying policies aimed at containing the spread of the virus, based on a slowly evolving understanding of the virus' characteristics and infection risks in different environments. Future crises – whether precipitated by humans or natural disasters and pandemics worsened by climate change – will see organisations face a combination of challenge, urgency and surprise.

This definition of organisational crises has loosely guided the selection of the case studies in this handbook – alongside the need to find examples where the impact upon nuclear organisations and operations has been particularly acute. The crises selected largely focus on the impact at the organisational level, although some also explore broader challenges experienced at the national level. It should be noted that the cases have been 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.

Resilience and Organisational Culture

Resilience is a term that has seen increasing use in recent decades – including in relation to nuclear security.[7] In simple terms, resilience encompasses the capacity of a system or an organisation to bounce back from internal or external shocks. As one recent study defines it, 'Resilience is the capacity of a social system (e.g., an organization, city, or society) to proactively adapt to and recover from disturbances that are perceived within the system to fall outside the range of normal and expected disturbances'.[8] A wide range of actions are commonly cited as helping to foster resilience; for example, information sharing, clear reporting structures and lines of communication, organisational learning, robust risk assessment methods and adequate training.[9] Building resilience within nuclear organisations – heightening their ability to respond and adapt to internal, but especially external, shocks – is hugely important to ensure nuclear security, safety and business continuity.

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.[10] 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.[11]

Preparedness and response are key elements of measures to build resilience within nuclear organisations. However, less emphasis has arguably been given to resilience within nuclear organisations in the context of preparing and responding to the impacts of non-nuclear crises on nuclear assets and nuclear security. The case studies in the handbook explore the concept of resilience in the context of these broader types of crises faced by nuclear organisations.

7 Louise K. Comfort, Arjen Boin and Chris C. Demchak, Designing Resilience: Preparing for Extreme Events, University of Pittsburgh Press, 2010, p.1-12.
8 Ibid., p.9.
9 Krista S. Langeland et al. How Civil Institutions Build Resilience, RAND Corporation, 2016, p.35-36.
10 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
11 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

A key tool to foster resilience and overcome crises is organisational culture. This concept has been a focus of study since the 1970s and is increasingly viewed as core to the success of failure of organisations. Edgar Schein, one of the key theorists of organisational culture, defines it as:

'A pattern of shared basic assumptions that the group learned as it solved its problems of external adaption and internal integration that has worked well enough to be considered valid and therefore to be taught to new members as the correct way to perceive, think and feel in relation to those problems.'[12]

The International Atomic Energy Agency (IAEA) has built from Schein's work to conceptualise safety and security culture in nuclear organisations, providing these organisations with means of trying to measure and enhance organisational culture.[13] The IAEA's model of nuclear security culture lists over 30 characteristics of an effective nuclear security culture.[14] Many of these characteristics – for example 'clear roles and responsibilities', 'training and qualification', 'professional conduct' – are also essential in building resilience. As will be shown in the following case studies, the strength of positive cultures within an organisation – in this case, nuclear security culture – frequently has huge implications for how organisations respond during times of crisis. Indeed, Schein and others have noted how crises can create opportunities for longer-term cultural change within organisations.

Against this background, the handbook now presents the four detailed case studies of nuclear security in times of crisis, extrapolating some key lessons from each case.

12 Edgar Schein, Organisational Culture and Leadership, Fourth Edition, Jossey-Bass, 2010, p.18.
13 See 'Safety Culture: A Report by the International Nuclear Safety Advisory Group', INSAG Series No.4, 1991. https://www.iaea.org/publications/3753/safety-culture and https://www.iaea.org/publications/7977/nuclear-security-culture
14 'Nuclear Security Culture: Implementing Guide', IAEA Nuclear Security Series, No.7, 2008, p.18. https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1347_web.pdf

Case Studies

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

Overview of the Crisis

Maintaining security during wildfires has become a growing challenge for nuclear facilities around the world. In 2010, explosive materials were removed as a precautionary measure from the Russian nuclear facility Sarov due to nearby fires.[15] At the Idaho National Laboratory in the United States, a fire burning 456-square kilometres came dangerously close to the facility in July 2019, forcing the evacuation of non-essential employees.[16] In April 2020, a large forest fire in northern Ukraine came within a few kilometres of a waste storage facility near the Chernobyl nuclear site.[17] In the coming decades, climate change will exacerbate the frequency and severity of these fires, posing a greater threat to nuclear facilities.[18]

WILDFIRES NEAR CHERNOBYL IN 2019

15 Andrew E. Kramer and Kevin Drew, 'Wildfires Ravaging Swaths of Russia', New York Times, 2010. https://www.nytimes.com/2010/08/07/world/europe/07russia.html
16 Rebecca Boone and Felicia Fonesca, 'Fire no longer threatens key Idaho nuclear facilities', Associated Press News, 25 July 2019. https://apnews.com/015fb22933ea43f08d8fa886fdb584a3
17 'Wildfires edge closer to Chernobyl nuclear plant', BBC News, 13 April 2020. https://www.bbc.com/news/world-europe-52274242
18 'The Connection Between Climate Change and Wildfires', Union of Concerned Scientists, 2020. https://www.ucsusa.org/resources/climate-change-and-wildfires

One of the most significant and extensively studied example of a wildfire threatening a nuclear facility was the Cerro Grande fire of May 2000 in the United States. 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's (LANL's) property, causing hundreds of millions of dollars in damage to the facility, and destroying research, equipment and many structures. The facility was forced to shut down for two weeks.[19] While none of the five LANL locations – where weapons-useable nuclear material was being stored at the time – were destroyed, catastrophe was only narrowly averted. There was heavy damage to areas around the nuclear storage facilities[20] and the fire burned close to the plutonium facility at Technical Area 55 and its supporting buildings. It also damaged land near the Critical Assembly Facility at Technical Area 18.

For self-evident reasons, most of the focus on this incident has been on safety. Nevertheless, important lessons can be learned from how the fire impacted LANL's security operations and how the facility responded to the crisis. The fire caught the facility off guard – disrupting security operations, creating confusion and raising questions about the condition of nuclear material onsite. However, it also inspired employees to improvise, creating new analytical tools and information-sharing mechanisms.

A History of Nuclear Security Culture Problems

The Cerro Grande fire occurred at time when LANL was addressing long-standing systemic security problems. LANL had a history of poor or unsatisfactory security ratings, often involving issues that had been identified in previous surveys but not subsequently addressed. Of particular concern was that the Albuquerque Operations Office management would not permit the internal reporting of a previous force-on-force exercise where failures in the guard force response had been revealed. A subsequent internal investigation showed this exercise had reached a critical point at which facility security could be compromised.[21]

In addition, there had been a serious cheating scandal from within LANL's Security Operations Division. The internal investigation found that unfavourable reviews and associated scores were allegedly changed by the Department of Energy (DOE) Albuquerque Operations Office management after surveys had been administered. The Albuquerque Operations Office destroyed records from the 1997-1998 surveys in an attempt to obstruct the investigation, and Security Operations Division managers allegedly pressured employees to 'mitigate' their survey responses to make the division 'look good', indicating that 'retaliation' was imminent if they did not comply.[22] Survey reviewers who provided unfavourable reviews were replaced by LANL management with reviewers who provided satisfactory reviews.[23]

19 M. Diana Webb and Kelly Carpenter, 'The Cerro Grande Fire, 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 National Laboratory, 2001. https://www.osti.gov/servlets/purl/975592
20 William Earl Haag, 'Material Control and Accountability (MC&A): Recovery from the Cerro Grande Fire at Los Alamos National Laboratory' Los Alamos National Laboratory, 2001. https://www.osti.gov/servlets/purl/975592
21 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', United States Department of Energy, 2000. https://fas.org/sgp/othergov/doeig_0471.html.
22 Ibid.
23 Ibid.

There was further evidence of problems in the organisation's security culture prior to the fire. Just a month before, nuclear disarmament activists reportedly drove through the LANL site and near facilities – that contained highly enriched uranium and plutonium – without being stopped by security.[24] These issues were compounded by high turnover among security managers, leading to several departmental reorganisations. As a result, security and counterintelligence responsibilities were "'punted" from one office to the next'.[25]

Nuclear Security during the Fire

These existing problems in security culture set the stage for the enormous impact that the fire had on LANL operations and security. Prior to the crisis, there had been no comprehensive assessment of how a potential site-wide emergency and evacuation would impact operations, facilities, infrastructure systems or contingency plans.[26] The subsequent investigation conducted by LANL revealed the emergency operations centre (EOC) was not equipped to respond to an extended site-wide emergency of this kind. The EOC was relying on 'insufficient, unavailable, or outdated site-specific information'.[27] Furthermore, while security personnel were permitted onsite throughout the crisis, they were sometimes forced to retreat from protected and material balance areas due to safety concerns.[28]

Communications Challenges

Central to the chaos and confusion faced by LANL leadership and emergency responders was the lack of communication from managers to employees and contractors. In terms of basic tracking and communication tools for employees and managers, LANL did not have a centralised list or method of tracking employees during the evacuation. This meant that employees relied on different sources of information, allegedly causing some to attempt to return to work prematurely against the laboratory director's orders. Other employees were unsure if their facility was open or not. Furthermore, even a basic organisational tree for phone contacts did not exist, and employees relayed that their primary source of information was the news media.[29]

Managers were equally aggravated due to the lack of communication mechanisms in place to contact employees and contractors. Since there was no centralised contact list of employees, managers could not easily communicate with employees to tell them when to return to work. Similarly, two-way communication between facility managers and employees was problematic. Like the facility managers, employees typically relied on cellular phones or land lines for direct communication. Rapid evacuations led many employees to leave behind their work-related equipment, rendering their private land lines useless. While mobile phones were not in common usage at the time, generally, employees' LANL mobile phones and personal mobile phones proved to be unreliable as batteries went flat and call control centres were overwhelmed.[30]

24 Interview conducted by authors, 13 August 2020.
25 President's Foreign Intelligence Advisory Board, 'Science at Its Best, Security at Its Worst, Community Wildfire Protection Plan 2016, Los Alamos', The Office of the President of the United States, 2016, p.11.
26 Cristina A. Salazar-Langley, Debora L. Hall and Cindy G. Coffman, 'Cerro Grande Fire: Facility and Waste Operations Division and Facilities Lessons to be Learned Report' Los Alamos National Laboratory, 2000, p.5-6. https://permalink.lanl.gov/object/tr?what=info:lanl-repo/lareport/LA-UR-01-1304
27 Ibid., p.9.
28 William Earl Haag, "Material Control and Accountability (MC&A): Recovery from the Cerro Grande Fire at Los Alamos National Laboratory', Los Alamos National Laboratory, 2001. https://www.osti.gov/servlets/purl/975592
29 Cristina A. Salazar-Langley, Debora L. Hall and Cindy G. Coffman, 'Cerro Grande Fire: Laboratory Recovery Lessons to be Learned Report', Los Alamos National Laboratory, 2000, p.32. https://permalink.lanl.gov/object/tr?what=info:lanl-repo/lareport/LA-UR-01-1305
30 Cristina A. Salazar-Langley, Debora L. Hall and Cindy G. Coffman, 'Cerro Grande Fire: Facility and Waste Operations Division and Facilities Lessons to be Learned Report' Los Alamos National Laboratory, 2000, p.13 . https://permalink.lanl.gov/object/tr?what=info:lanl-repo/lareport/LA-UR-01-1304

When communications were established, it was done in an ad hoc manner. For employees providing emergency field support, communications and control centres were established as they were needed, utilising whatever type of communication devices that were available and in working order. This was particularly important for utilities personnel located closer to the laboratory, where they were awaiting instruction to shut off gas, electricity or other utilities at any moment. Although the site only lost power for 15 minutes throughout the entire crisis,[31] the lack of an established system for managing emergency response communications led to the double-booking of facility managers and employees to respond to multiple emergencies in different locations, or multiple teams being asked to respond to the same location.[32] This meant that human resources could not be efficiently allocated to respond to the crisis.

Access Control

This confusion during the emergency was also apparent for employees in divisions where the lines of authority overlapped, including those involved in access control, with staff seemingly making ad hoc decisions.[33] It was unclear what the access and re-entry requirements were for the site because there was no single authority in charge of the process. Badges were created as individuals or organisations were added to the response efforts. The security contractor who managed perimeter access control was left unsure of which badges were open to malicious use or duplication. Further complications arose as there were no pre-defined lists of individuals who were allowed to enter the facility, leading to an influx of people into LANL's Facility Recovery Center.[34] Building access control faced similar difficulties, wherein staff bypassed the required clearance (security and safety) process to re-enter buildings that had been designated as closed. Subsequent reports about the emergency noted that this practice was 'a potential compromise to security and safety'.[35]

Many of the facilities and emergency response staff who had to continue reporting to work throughout the emergency, in contrast, found it difficult at times to enter the gate to the facility. Gates and badge readers needed to be manually overridden to allow first responders into the facility, which took time. Manual locks around the site required keys to reopen them, requiring staff to contact the last staff member with the key. This was difficult because there was no emergency process and procedure for facility key inventory and control.[36] When staff returned to the site on 23 May 2000, the LANL Security Division released a report stating,

'The Pro Force…was able to maintain control over the site throughout the emergency. Special attention was given to protecting Category I SNM [special nuclear material]. For the three Category I SNM facilities, all building boundary and interior alarm records that could not be assessed in realtime [sic] for a short period on May 11 were rigorously analysed immediately thereafter and revealed no alarms, no alarm tampering, and no loss of alarm system power.'[37]

While no security incident occurred during the fire, whether material was at risk is clearly a more complicated issue.

31 Cristina A. Salazar-Langley, Debora L. Hall and Cindy G. Coffman, 'Cerro Grande Fire: Laboratory Recovery Lessons to be Learned Report', Los Alamos National Laboratory, 2000, p.18. https://permalink.lanl.gov/object/tr?what=info:lanl-repo/lareport/LA-UR-01-1305
32 Ibid.
33 Ibid. p.19.
34 Ibid., p.13.
35 Ibid., p.19.
36 Cristina A. Salazar-Langley, Debora L. Hall and Cindy G. Coffman, 'Cerro Grande Fire: Facility and Waste Operations Division and Facilities Lessons to be Learned Report' Los Alamos National Laboratory, 2000, p.13-14. https://permalink.lanl.gov/object/tr?what=info:lanl-repo/lareport/LA-UR-01-1304
37 William Earl Haag, 'Material Control and Accountability (MC&A): Recovery from the Cerro Grande Fire at Los Alamos National Laboratory' Los Alamos National Laboratory, 2001. https://www.osti.gov/servlets/purl/975592

Establishing Alternative Information Sharing Arrangements

There was one notable success story in the Cerro Grande fire, however, which centred on the geographic information system (GIS) teams. During the emergency, GIS teams were formed in an ad hoc manner due to staff becoming aware that critical facility information was not being communicated at the senior level. A 2003 report detailing the emergency support provided by GIS during the Cerro Grande wildfire revealed that LANL GIS staff (known as the Facility for Information Management, Analysis and Display [FIMAD] team) joined with external volunteers. Together, they provided local first responders and the Burned Area Emergency Rehabilitation (BAER) team with detailed mapping of LANL and nuclear material storage sites where, if fire approached, there could be catastrophic consequences. [38]

When the LANL leadership made the decision to close the site late on 7 May 2000, employees had travelled home on Friday without taking research or other remote working supplies with them.[39] A product of effective management at the time, or perhaps serendipity, two FIMAD team members had already been assigned to work from home prior to the shutdown, thus these individuals possessed disks for GIS software and critical map data for LANL. Furthermore, they were not in the evacuation area at the time of the shutdown. FIMAD servers remained online as electricity continued functioning, meaning that the FIMAD team members could still access the LANL intranet at an offsite location, such as the EOC.[40]

The GIS remote operations staff, consisting of experts from multiple agencies, were synergistic, providing decisive action and improvising when necessary, and were able to avoid the burden of paperwork. During the emergency, the Bureau of Land Management (BLM) provided frequent infrared images of the fire perimeter, after which the BLM would digitally transmit the images in a line and plot format, from which Sandia Environmental GIS unit could construct a comprehensive profile of the fire. Sandia then sent the files either through the FIMAD server or straight to an external site that had been established during the crisis. Lastly, FIMAD staff would finalise the maps, print them and hand deliver them to the LANL EOC. This process continued for 10 days, 24 hours per day, with staff deciding amongst themselves a system of shifts and breaks.[41]

Post-Incident Recovery

When employees returned to the site on 23 May 2000, apparently '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'.[42] It took weeks for material balance areas to resume normal MC&A operations. Following the fire, facilities possessing large quantities of nuclear material reported their

38 C. R. Mynard et al., 'Geographic Information Systems (GIS) Emergency Support for the May 2000 Cerro Grande Wildfire', Los Alamos National Laboratory, 2003), p.8. https://doi.org/10.2172/812177
39 Ibid.
40 Ibid.
41 Ibid.
42 William Earl Haag, 'Material Control and Accountability (MC&A): Recovery from the Cerro Grande Fire at Los Alamos National Laboratory' Los Alamos National Laboratory, 2001. https://www.osti.gov/servlets/purl/975592

status to LANL's physical inventory office. Since there had been material in process the day before the evacuation, LANL conducted an inventory of all weapons-useable nuclear material items greater than 200 grams; a total of 295 items within material balance areas were inventoried. At facilities with smaller quantities of materials, visual checks were conducted to determine that materials were present and had not been tampered with during the fire. By the end of June, every material balance area had been either inspected or inventoried.[43]

Regulatory Support

LANL and contractor management subsequently commented that, while DOE facility representatives had helped to provide a direct lifeline to DOE resources during the response, which helped reduce bureaucratic roadblocks, DOE and other state and local agencies visiting LANL had in fact diverted resources that could have been used in the emergency response and recovery.[44] Facility managers and employees across the site often worked overtime as the administrative services that typically assisted in procuring additional resources were overwhelmed and had a significant backlog. As a lessons-learned survey analysis reported, '[t]his contributed to feelings of isolation and perceptions of institutional unresponsiveness'.[45] The concentration of emergency response authority at the middle management level may have exacerbated the situation because the more junior facility staff did not possess the requisite expertise to properly assess the level of damage in the laboratories. Management later reflected extensively on the lack of clear roles and responsibilities across units and within divisions. [46]

Facility and programmatic staff faced similar hurdles when requesting money to begin purchasing replacement equipment. Analysis of the recovery process found that there was no office or individual at LANL or DOE with whom facility managers could discuss the damage assessments or the prioritisation of project requests.[47] Senior management did not serve a filtering function, resulting in disparate projects being funded based on when they were submitted to Congress. Additionally, the lack of a single point-of-contact for managers at LANL or DOE left managers in the lurch as they waited for months for projects to be approved. The pressure to re-start operations from LANL and DOE senior management was allegedly intense, and facility managers essentially had no additional emergency support.[48]

Inadequate management and oversight throughout the recovery process exemplifies the institutional culture problems LANL faced prior to the crisis. Moreover, the absence of clear lines of authority and responsibility and the chaotic funding request process significantly delayed recovery. Sustaining nuclear security depends on the provision of adequate resources grounded in strong security culture. It is unclear how quickly these were established in the wake of the fire.

43 Ibid.
44 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
45 Ibid., p.7.
46 Ibid.
47 Ibid., p.9.
48 Ibid.

Lessons Learned

Many factors help to explain the failures in the response to the Cerro Grande wildfire from a nuclear security perspective, including lack of detailed contingency plans and performance testing, inadequate communications systems and confusing lines of authority. As a result, the facility staff were not prepared to respond to a fire of this magnitude. Despite the many problems that occurred, the 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.[49]

There are, however, numerous lessons to be learned from mistakes made prior to and during the crisis. 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. It is evident that emergency planning must include contingencies for accessing data in a secure manner in the event of an evacuation. Facilities should also have an institutional prioritised 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. Contingency plans should be in place for off-site access to this information. During the crisis, senior leadership should be present at a location where they can provide the most positive impact, which is often the EOC. Finally, rigorous performance testing of these plans is necessary to determine whether security forces can maintain security during a crisis.

Since the fire, LANL has taken various actions that have helped respond to crises like wildfires, including constructing a new EOC, eliminating and reducing materials that can fuel fire, improving information flows, and reducing the time required for decision-making.[50] Unfortunately a 2007 report identified that, while integration of emergency management and security planning had improved, the lab was still insufficiently prepared for future emergencies.[51] New security and emergency response measures were put to the test in 2011 during the Los Conchas Fire, which burned over 200 square miles in New Mexico. Unlike the Cerro Grande wildfire, Los Conchas did not destroy any laboratory structures or facilities. By all accounts, the response to this event was more effective despite similar challenges in responding to the crisis.[52]

49 Ibid.
50 'Operating Experience Summary', United States Department of Energy Office of Health, Safety and Security, 2012. https://www.energy.gov/sites/prod/files/2014/05/f15/OES_2012-03.pdf
51 'Independent Oversight Inspection of Emergency Management at the Los Alamos Site Office and Los Alamos National Laboratory', United States Department of Energy, 2007. https://www.energy.gov/sites/prod/files/2013/11/f5/2007_LANL_EM_report_%28final%29_0.pdf
52 Brenda Andersen, 'Los Alamos National Laboratory Response to Las Conchas Fire', Los Alamos National Laboratory, 2011. https://permalink.lanl.gov/object/tr?what=info:lanl-repo/lareport/LA-UR-11-06518

After the event, however, 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'.[53] Since the Los Conchas fire, there has been further progress in strengthening LANL security during emergencies, though challenges remain.[54] 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.

53 '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

54 '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

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

Overview of the Crisis

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. From 1990 to 1998 the gross national product in Soviet countries fell by over 40% and remained stagnant; in the case of Russia this lasted well into the 2000s.[55] In 1992, hyperinflation raised retail prices by over 2,500%, putting the wages of a third of Russians below a basic subsistence level.[56] By mid-1998, Russia's economy had 'reached the brink of economic collapse', interest rates were exorbitant, and several major banks had gone bankrupt.[57] 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.[58] The economic downturn resulted in deep cuts to Russia's nuclear spending, with facilities unable to purchase essential nuclear security equipment.

Politically, the 1990s saw a prolonged period of turbulence in Russia which triggered the collapse of a wide range of government services, including public utilities, policing and payroll. This served to stimulate a rise in provincialism, with two regional governments proclaiming complete independence and tens of others declaring 'sovereignty'.[59] It also led to a surge in organised crime, with various groups infiltrating and taking control of public services. Rampant corruption was evident at a wide range of state-run institutions and at all levels from junior bureaucrats to senior officials. This served to weaken the influence of the Russia's nuclear regulatory bodies and their ability to assess and enforce security standards.

Stagnating investment, production and consumption, delayed pay checks and mass-layoffs were an everyday reality in the nuclear and other industrial sectors.[60] Formerly well paid and highly privileged nuclear scientists and security managers were suddenly either poorly compensated for their work or laid off.[61] Due to the high level of inflation, purchasing power and personal savings

55 Angus Maddison, 'The World Economy', Development Centre Studies, OECD, 2006, p.155. https://www.stat.berkeley.edu/~aldous/157/Papers/world_economy.pdf
56 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.185; Lucio Vinhas De Souza, 'A Different Country – Russia's Economic Resurgence', Centre for European Policy Studies, 2008, p.7, 18. https://www.files.ethz.ch/isn/55936/CEPS%20Pb%202008-05%20A%20Different%20Country.pdf
57 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.
58 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.
59 Jeremy Azrael, Keith Crane and D.J. Peterson, 'Political and Economic Outlook for Russia and the Future of the Automotive Industry', RAND Working Paper, 2004, p.16. https://www.rand.org/content/dam/rand/pubs/working_papers/2004/RAND_WR145.pdf
60 National Research Council, Protecting Nuclear Weapons Material in Russia, The US National Academies Press, 1999, p.2. https://doi.org/10.17226/9469
61 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

declined rapidly, leading to financial insecurity.[62] An informal economy grew as people exchanged favours rather than money to make ends meet.[63] These conditions also stimulated an increase in Russian drug and alcohol abuse, with per capita vodka consumption nearly tripling from 1987 to 1994, and mortality from causes related to alcohol abuse increasing five-fold.[64] Suicide rates also jumped dramatically, doubling during the 1990s.[65] 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.

Nuclear Sector in 1990s Russia

Russia inherited a vast and sprawling nuclear estate from the Soviet Union, which consisted of both defence and civil elements. This included approximately 37,000 nuclear warheads, a vast nuclear weapons production complex and large stocks of weapons-grade fissile material.[66] These were spread across the country with many facilities purposely constructed in remote locations during the Soviet era in an effort to help protect weapons-related secrets. Russia also maintained a fleet of nuclear-powered submarines and ice-breakers, which utilised significant quantities of highly enriched uranium (HEU). Indeed, nuclear naval reactor consumption peaked in 1990 at approximately 4.5 tonnes per year.[67]

Russia's civil nuclear sector in the 1990s had stalled following the Chernobyl accident of 1986. The disaster had resulted in the temporary abandonment of new nuclear power plants across the Soviet Union. Nevertheless, there still existed more than 25 operational power reactors at 10 sites, supplying over 10% of Russia's electricity needs.[68] In addition, Russia operated tens of research reactors, many fuelled by HEU, which were generally used for research, training, radioisotope production and other industrial purposes. The country also hosted well over 1,000 facilities that housed radioactive sources.

During the Cold War, military competition with the United States had led to significant government investment in the Soviet nuclear sector, as well as associated 'prestige, high salaries and benefits' for those that worked within it.[69] However, by the 1990s Russia's economic difficulties led to a sharp decline in government investment in the defence sector, including its nuclear component, with cuts amounting to a loss of nearly 80% percent in total funding.[70] The operators of Russia's nuclear power plants also faced financial difficulties, with several reportedly close to the point of bankruptcy.[71] This served to cut physical investment in Russia's nuclear infrastructure and led to both unemployment and reduction and delays in paying staff salaries – with many nuclear scientists and engineers seeking employment elsewhere. The financial crisis also resulted in large scale protests and in some

62 National Research Council, Protecting Nuclear Weapons Material in Russia, The US National Academies Press, 1999, p.11. https://doi.org/10.17226/9469
63 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.
64 Jose Luis Bobadilla, Christine A. Costello and Faith Mitchell, Premature Death in the New Independent States, The US National Academies Press, 1997, Table 7-1 and Table 7-4b. https://www.ncbi.nlm.nih.gov/books/NBK233387/
65 Nick Paton Walsh, 'Russia's suicide rate doubles', The Guardian, July 9, 2003. https://www.theguardian.com/world/2003/jul/09/russia.nickpatonwalsh
66 'The Former Soviet Union: Russia, Ukraine, Kazakhstan and Belarus', Federation of American Scientists. https://fas.org/irp/threat/prolif96/fsu.html; Robert S. Norris and Hans M. Kristensen, 'Global nuclear weapons inventories, 1945–2010', Bulletin of the Atomic Scientists, Vol.66 No.4, 2010 p.77-83.
67 Pavel Podvig (ed.), The Use of Highly-Enriched Uranium as Fuel in Russia – Research Report No.16 International Panel on Fissile Materials, 2017 International Panel on Fissile Materials, 2017, p.7. https://spia.princeton.edu/system/files/research/documents/HEU.pdf
68 Susanne Oxenstierna, Russia's Nuclear Energy Expansion, Swedish Defence Research Agency (FOI), 2010, p.18.
69 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
70 'Military Industry Overview', Federation of American Scientists, 24 August 2000. https://fas.org/nuke/guide/russia/industry/overview.htm
71 Ibid.

cases suicides. Although denied by the authorities, Russia's broader drug and alcohol issues permeated the nuclear sector according to media and other reports at the time.[72] Indeed, drug and alcohol misuse was alleged to be widespread at certain facilities, with such issues – and scrutiny of them – compounded by the closed nature of Russia's nuclear cities.

The former Soviet Union had employed tens of thousands of nuclear scientists and engineers, some with valuable civil and weapons related knowledge.[73] Once the economic situation for these highly knowledgeable individuals became untenable, it was only to be expected that they would leave the nuclear sector in Russia and other Former Soviet Union (FSU) countries – in effect a 'brain drain' for the industry. While migration data was gathered only sporadically, some analysts estimate that between 1986 and 1990 more scientists and engineers left Russia than in the whole of the four preceding decades; and an additional 40% of the country's theoretical physicists left in the following three years.[74] According to a report by the United Nations Institute for Disarmament Research, an unspecified number of Russian nuclear scientists had migrated to the Democratic People' Republic of Korea (DPRK),[75]; by the end of 1995, an estimated 1,000 nuclear engineers had relocated to China and another 200 to Iran.[76]

The Ministry for Atomic Energy (Minatom) was established in 1992 to provide support and oversight of Russia's nuclear facilities, absorbing the responsibilities of the Ministry of Atomic Power and Industry (MAPI) that had operated during the Soviet era.[77] Regulatory oversight of Russia's civil nuclear power plants was provided by Gosatomnadzor (State Committee for Nuclear and Radiation Safety; GAN), with the Ministry of Defence responsible for military facilities. These organisations oversaw the development, approval and enactment of federal rules and regulations in relation to the use of atomic energy, including those relevant to nuclear safety and security.[78] These organisations were also responsible for the licensing of nuclear sites and activities and conducting safety and security-related inspections. However, as will be discussed later in this case study, it proved challenging for Minatom and GAN to implement the aforementioned activities, due to declining budgets, outdated nuclear laws and regulations, and disruptive competition between the two bodies.

Nuclear-Related Threats in Post-Soviet Russia

The unstable environment in Post-Soviet Russia created two major interrelated proliferation concerns.[79] 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.

72 Igor Khripunov and James Holmes (eds.), Nuclear Security Culture: The Case of Russia, Center for International Trade and Security, University of Georgia, 2004, p.27-28. https://media.nti.org/pdfs/analysis_cits_111804.pdf
73 Dorothy S. Zinberg, 'The Missing Link? Nuclear Proliferation and the International Mobility of Russian Nuclear Experts', Research Paper No.35, United Nations Institute for Disarmament Research, 1995, p.3. https://unidir.org/files/publications/pdfs/the-missing-link-nuclear-proliferation-and-the-international-mobility-of-russian-nuclear-experts-237.pdf
74 R. Adam Moody, 'Report: Reexamining Brain Drain from the Former Soviet Union', The Nonproliferation Review, 1996, p.92; Dorothy S. Zinberg, 'The Missing Link? Nuclear Proliferation and the International Mobility of Russian Nuclear Experts', Research Paper No.35, United Nations Institute for Disarmament Research, 1995, p.8. https://unidir.org/files/publications/pdfs/the-missing-link-nuclear-proliferation-and-the-international-mobility-of-russian-nuclear-experts-237.pdf
75 Dorothy S. Zinberg, 'The Missing Link? Nuclear Proliferation and the International Mobility of Russian Nuclear Experts', Research Paper No.35, United Nations Institute for Disarmament Research, 1995, p.18. https://unidir.org/files/publications/pdfs/the-missing-link-nuclear-proliferation-and-the-international-mobility-of-russian-nuclear-experts-237.pdf
76 R. Adam Moody, 'Report: Reexamining Brain Drain from the Former Soviet Union', The Nonproliferation Review, 1996, p.94.
77 'Military Industry Overview', Federation of American Scientists, 24 August 2000. https://fas.org/nuke/guide/russia/industry/overview.htm
78 A.B. Malyshev, 'Current Status and Development Perspectives of State Nuclear and Radiation Safety Regulation in the Russian Federation', International Conference on Fifty Years of Nuclear Power – the Next Fifty Years – Book of Extended Synopses, IAEA, IAEA-CN-114/D-1, 2004, p.88. https://inis.iaea.org/collection/NCLCollectionStore/_Public/35/087/35087513.pdf?r=1
79 Oleg Bukharin, 'Nuclear Safeguards and Security in the Former Soviet Union', Survival, Vol. 36, No.4, 1994, p.53.

Organised Crime, International Terrorism and Nuclear Material Smuggling

With organised crime already infiltrating large parts of the Soviet Union before its collapse, limited law enforcement in 1990s Russia allowed criminal groups to prosper.[80] By 1994, Russian organised crime controlled 'all types of activities', leading to then-president Yeltsin's to say, 'Russia is the biggest mafia state in the world'.[81] By 1997, approximately 9,000 gangs ruled large parts of Russia's economy and had successfully recruited members with military, scientific and engineering backgrounds.[82] These conditions, combined with degraded security at nuclear facilities and the interest expressed by terrorist organisations (including Aum Shinrikyo and al-Qaeda), in acquiring weapons of mass destruction (WMD) fuelled fears of nuclear and radiological material smuggling.[83] Concerns related to the weakening of nuclear security systems were subsequently borne out during the 1990s with numerous discoveries in Europe of illicit nuclear and radiological material out of regulatory control from FSU countries. In the first six months of 1994, 90 cases of nuclear or radiological smuggling were confirmed in Germany alone.[84] In 1993, the Russian Ministry of Internal Affairs recorded 700 attempts to steal materials or classified documents from nuclear facilities.[85] Analysis of these and other incidents revealed that almost every case of nuclear theft was connected to an individual employed within the nuclear sector, and that the vast majority had gone undetected by the facility security systems.[86]

Chechen Separatists' Pursuit of Nuclear and Radiological Materials

Taking advantage of the political vacuum following the fall of the Soviet Union, Chechnya declared itself independent of Russia in 1991. What followed was a bloody and protracted conflict between the Russian military and Chechen 'rebels', with estimates putting the number of deaths and casualties in the hundreds of thousands.[87] During the conflict the Chechen separatists pursued a coercive strategy against the Russian government, with their leader Shamil Basayev publicly threatening on multiple occasions to use CBRN weapons against Russian cities.[88] In 1995, acting on a tip from Basayev, Russian television discovered in a Moscow park what was reported to be a viable radiological dispersal device – a container holding caesium-137 surrounded by dynamite.[89] The radioactive source had allegedly been stolen from a hospital and placed in the park by Chechen rebels.[90] Other nuclear-related incidents included an unsuccessful attack by Chechen fighters at a Russian military airfield in Kizlyar in 1996 that was believed to house nuclear weapons, while in 1999 attempts were made to steal a nuclear waste container from a factory in the Chechen capital Grozny.[91]

80 Rensselaer W. Lee, Smuggling Armageddon – The Nuclear Black Market in the Former Soviet Union and Europe, St. Martin's Griffin, 1998, p.49-50; 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.760. https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=1504&context=jil
81 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.759. https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=1504&context=jil; Rensselaer W. Lee, Smuggling Armageddon – The Nuclear Black Market in the Former Soviet Union and Europe, St. Martin's Griffin, 1998, p.47.
82 Rensselaer W. Lee, Smuggling Armageddon – The Nuclear Black Market in the Former Soviet Union and Europe, St. Martin's Griffin, 1998, p.50.
83 Farhad Rezaei, 'Shopping for Armageddon: Islamist Groups and Nuclear Terror', Middle East Policy, Vol.23, No.3, 2016, p.119; Sara Daly, John Parachini and William Rosenau, Aum Shinrikyo, Al Qaeda, and the Kinshasa Reactor, RAND Corporation, 2005, p.13.
84 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.753. https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=1504&context=jil.
85 Rensselaer W. Lee, Smuggling Armageddon – The Nuclear Black Market in the Former Soviet Union and Europe, St. Martin's Griffin, 1998, p.29.
86 George Bunn, 'Raising International Standards for Protecting Nuclear Materials from Theft and Sabotage', The Nonproliferation Review, 2000, p.150.
87 'Chechnya profile – Timeline', BBC News, 17 January 2018. https://www.bbc.co.uk/news/world-europe-18190473
88 Jeffrey Bale, 'The Chechen Resistance and Radiological Terrorism', Nuclear Threat Initiative, 1 April 2004. https://www.nti.org/analysis/articles/chechen-resistance-radiological-terror
89 Charles Streeper, 'Preventing Dirty Bombs: Addressing the Threat at the Source," Nonproliferation Review, Vol.17, No.3, 2010, p.532.
90 Jeffrey Bale, 'The Chechen Resistance and Radiological Terrorism', Nuclear Threat Initiative, 1 April 2004. https://www.nti.org/analysis/articles/chechen-resistance-radiological-terror
91 Evolving Security Threats and Advanced Security Technologies, World Institute for Nuclear Security (WINS), 2018, p.57; Farhad Rezaei, 'Shopping for Armageddon: Islamist Groups and Nuclear Terror', Middle East Policy, Vol.23, No.3, 2016, p.119.

Impact of the Crisis on Nuclear Security

Russia's significant political, economic and social turmoil in the 1990s had serious repercussions for the security at nuclear facilities, both in terms of creating new problems and highlighting the weakness in increasingly outdated Soviet approaches.[92] As discussed below, the major impacts of this upheaval on the nuclear sector included: a reduction in federal influence and oversight; degradation of physical systems and technology; demotivated staff who struggled to recognise the importance of nuclear security; and a surge in actions by 'insiders' – individuals with malicious intent and authorised access to nuclear assets.

Reduced Regulatory Influence and Oversight

As a result of Russia's broader economic decline, Minatom's budget shrunk significantly in the early 1990s; by the end of the decade only approximately 20% of Russia's nuclear operating costs could be covered by the government.[93] This served to reduce Minatom's influence over the nuclear sector, which was further compounded by the rise in regionalism in Russia, limiting the ministry's ability to assess and enforce security standards.

Degraded Security Systems and Technology

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'.[94] 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.[95] 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'.[96]

Unmotivated Personnel

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. Indeed, the focus was on trusting rather than monitoring employees.[97] Externally focused security systems at nuclear facilities were also relatively low-tech, with reliance placed on the actions of a large intelligence service and security force.[98] 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

92 Igor Khripunov and James Holmes (eds.), Nuclear Security Culture: The Case of Russia, Center for International Trade and Security, University of Georgia, 2004, p.22. https://media.nti.org/pdfs/analysis_cits_111804.pdf
93 Igor Khripunov, 'Minatom at the edge', The Bulletin of the Atomic Scientists, Vol.55, No.3, 1999, p.56. https://journals.sagepub.com/doi/pdf/10.2968/055003016
94 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
95 Ibid., p.22.
96 Ibid., p.23.
97 Todd Perry, 'Securing Russian Nuclear Materials: The Need for an Expanded US Response', The Nonproliferation Review, Vol.6, No.2, 1999, p.89.
98 National Research Council, Protecting Nuclear Weapons Material in Russia, The US National Academies Press, 1999, p.9. https://doi.org/10.17226/9469

declined, 'the morale at these remote facilities fell precipitously', with nuclear security an issue of little concern for most employees.[99]

Rise in Insider Threats

The financial hardship faced by nuclear personnel served as a direct trigger for many cases of insider action. For example, an employer at the Luch Scientific Production Association in Podolsk, Leonid Smirnov, stole approximately 1.5 kg of 90% enriched uranium (i.e. HEU) over a period of several months in 1992.[100] Struggling to make ends meet, Smirnov planned to sell the material, although did not succeed in locating a buyer and ultimately the material was recovered by the authorities. In other cases of insider incidents, close colleagues were co-opted or bribed to look the other way. In fact, the economic situation had become so acute that even if other employees became aware of illegal activities, these were frequently perceived as a 'way out of poverty' and consequently not reported. One notable case involved the theft of millions of dollars of rare isotopes from Elektrokhimpribor, a remote facility in Lesnoy, over several years in early 1990s by multiple cooperative insiders. When the perpetrators were finally revealed by the authorities, colleagues working at the facility, but not involved in the theft, justified their actions by claiming 'there was no other way for people to make money.'[101]

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 (NMAC), an essential process in guarding against material theft, particularly given the vast quantities of nuclear materials handled at many Russian facilities. However, even during Soviet times, NMAC in Russia was relatively primitive, and largely utilised a paper-based system, which could be readily altered. 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.[102]

International Efforts to Strengthen Nuclear Security in Russia

Recognising the worsening state of nuclear security in the FSU, the US 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.[103] 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

99 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
100 Christopher Hobbs and Matthew Moran, Insider Threats: An Educational Handbook of Nuclear and Non-Nuclear Case Studies, Centre for Science and Security Studies, King's College London, 2015, p.12-13.
101 Igor Khripunov and James Holmes (eds.), Nuclear Security Culture: The Case of Russia, Center for International Trade and Security, University of Georgia, 2004, p.83. https://media.nti.org/pdfs/analysis_cits_111804.pdf
102 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
103 '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

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.[104]

As discussed, the salaries received by guards and other employees at nuclear facilities had deteriorated significantly in the 1990s, which led to apathy among personnel with respect to security measures and, in extreme cases, to turning a blind eye to insider actions. At certain facilities guards did not even receive appropriate food supplies and reportedly abandoned their posts to search for food on the streets.[105] At other facilities, guards were ill-equipped for the cold weather and hence refused to leave their station for patrols or to investigate potential security issues. To counter these basic problems, the international support programmes provided coats and heaters to nuclear facility personnel and subsidised meals. Focus was also placed on supporting timely payments to scientists and security workers and restructuring of the workforce in order to prevent further unemployment.[106]

104 Todd Perry, 'Securing Russian Nuclear Materials: The Need for an Expanded US Response', The Nonproliferation Review, Vol.6, No.2, 1999, p.86.
105 Ibid., p.88.
106 Ibid., p.84.; Matthew Bunn, Oleg Bukharin, Jill Cetina, Kenneth Luongo and Frank von Hippel, 'Retooling Russia's Nuclear Cities', Partnership for Global Security, September-October 1998. https://oconnell.fas.harvard.edu/files/matthew_bunn/files/bunn_retooling_russia_s_nuclear_cities.pdf

Programmes were also set up to support new security-related education and training initiatives. In partnership with the US National Nuclear Laboratories, the US Department of Energy and US Department of Defence initiated a 'long-term education and awareness project' to help ameliorate physical and procedural nuclear security in post-Soviet States.[107] This included both high-level nuclear security and counter-proliferation seminars and detailed training on the use of new 'computerized inventory controls and electronic security measures.'[108] Facility-specific programmes were complemented by the foundation of national and international nuclear security educational programmes.[109] For example, Minatom in conjunction with the DOE established the Russian Methodological Training Center (RMTC) at the Institute of Physics and Power Engineering in Obninsk in 1998, with the primary goal to equip Russian scientists with knowledge on MPC&A.[110] A similar programme was established at the Moscow Institute of Physics and Engineering.[111]

The financial contribution provided by the US and other international partners in support of these activities was significant. Between 1996 and 1999, the Russian MPC&A budget was increased ten-fold from its original US$15 million, with the programme expanded to over 200 nuclear sites in 1997.[112] In 2002, the US pledged to contribute approximately US$10 billion over the next decade to 'address non-proliferation, disarmament, counter-terrorism and nuclear safety issues'.[113]

Challenges Encountered in Nuclear Security Implementation

The vast size and sprawling nature of Russia's nuclear sector in the 1990s presented an intrinsic challenge to achieving the effective implementation of nuclear security across all facilities. Here the ad hoc nature of initial international engagements, combined with variations in how these were inculcated, created a patchwork of protection. Nuclear security implementation ranged from high-functioning facilities equipped with modern security systems to facilities with old or non-operational security technology, beset by performance issues.

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'.[114] Estimates by a Harvard University study from that year showed that only approximately 26% of Russia's nuclear material was secured appropriately.[115]

107 Igor Khripunov and James Holmes (eds.), Nuclear Security Culture: The Case of Russia, Center for International Trade and Security, University of Georgia, 2004, p.60. https://media.nti.org/pdfs/analysis_cits_111804.pdf
108 Rensselaer W. Lee, Smuggling Armageddon – The Nuclear Black Market in the Former Soviet Union and Europe, St. Martin's Griffin, 1998, p.10; 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.774. https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=1504&context=jil
109 Igor Khripunov and James Holmes (eds.), Nuclear Security Culture: The Case of Russia, Center for International Trade and Security, University of Georgia, 2004, p.60. https://media.nti.org/pdfs/analysis_cits_111804.pdf
110 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.156.
111 Igor Khripunov and James Holmes (eds.), Nuclear Security Culture: The Case of Russia, Center for International Trade and Security, University of Georgia, 2004, p.59. https://media.nti.org/pdfs/analysis_cits_111804.pdf
112 Todd Perry, 'Securing Russian Nuclear Materials: The Need for an Expanded US Response', The Nonproliferation Review, Vol.6, No.2, 1999, p.86.
113 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.154; 'Statement by G8 Leaders: The G8 Global Partnership Against the Spread of Weapons and Materials of Mass Destruction', Kananaskis, 27 June 2002. http://www.g7.utoronto.ca/summit/2002kananaskis/arms.html
114 'Persistent Diplomacy Needed for Nonproliferation Advances', United States Department of State, 11 August 2004. https://media.nti.org/pdfs/170.pdf
115 Nathan E. Busch and James R. Holmes, "The 'Human Factor' and the Problem of Nuclear Security in Russia', Perspectives on Political Science, 34, No.3, 2005, p.156.

Legal and Regulatory Issues

As previously noted, in the early 1990s, a rise in regionalism and reductions in funding made it difficult for the newly formed Minatom to provide effective security oversight at Russia's nuclear facilities. The situation had improved by the late 1990s, thanks to a Minatom campaign which sought to address the broader social and economic issues faced by different regions through improving 'infrastructure development, employment, and higher living standards'.[116] Nevertheless, issues remained, both with regards to inter-agency cooperation and the interpretation of laws and regulations, which were viewed by many as 'ambiguous, leaving unacceptably wide discretion for interpretation'.[117] For example, at facilities that had both defence and civil components, Minatom officials would regularly deny GAN inspectors access on the pretext that they housed activities that were defence-related. As for regulatory guidance, documents were 'sometimes obsolete and poorly structured, as well as too general, formalized, and lengthy'.[118] In addition, they tended focused on the 'technical minutiae rather than providing solutions to problems likely to be encountered by the workforce'.[119]

Integrating New Security Technologies into Existing Systems

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.[120] Such an approach served to created implementation challenges, with US observers reporting back that new security systems were not always operated reliably.[121] 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.[122] 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.[123]

In an effort to overcome these challenges, a greater focus was placed on the sustainability of upgrade work, for example through incorporating indigenously produced security equipment. Russian nuclear personnel were also encouraged to 'take ownership of MPC&A', through leading the development of new systems.[124] Greater focus was also placed on training activities for both facility staff and regulatory officials, and support was provided for new cross-cutting nation-wide initiatives, including the creation of a national fissile material inventory database.[125] However, the implementation of such programmes was not without its challenges. For example, in the case of the national fissile material database Minatom and GAN disagreed on which inventory methods should be used and which agency should oversee the process. Ultimately, Minatom won the dispute, but decided to abandon most of its existing projects realised through US investment, instead initiating its own project.

116 Igor Khripunov and James Holmes (eds.), Nuclear Security Culture: The Case of Russia, Center for International Trade and Security, University of Georgia, 2004, p.24. https://media.nti.org/pdfs/analysis_cits_111804.pdf
117 Ibid., p.65.
118 Ibid.
119 Ibid.
120 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.
121 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.
122 Ibid.
123 National Research Council, Protecting Nuclear Weapons Material in Russia, The US National Academies Press, 1999, p.18-19.
124 Todd Perry, 'Securing Russian Nuclear Materials: The Need for an Expanded US Response', The Nonproliferation Review, Vol.6, No.2, 1999, p.86.
125 Ibid., p.87.

Developing Nuclear Security Culture and Leadership

As discussed, initial international efforts focused on providing vital physical infrastructure and upgrading nuclear security technologies at Russian sites. However, it subsequently 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'.[126]

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.[127] 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'. [128]

Although the Soviet system had arguably been effective at providing nuclear security, through a '3G' security model – guns, guards and gates – where the responsibility fell largely on the guard and response forces, this could not deal with the full range of threats facing nuclear facilities, in particular those posed by insiders. To this end, efforts focused on promoting personal responsibility for nuclear security amongst all employees through the concept of nuclear security culture, in an effort to change the prevailing viewpoint at the time that 'security will, and should, be assured by others'.[129] At the time, such a mentality was deeply entrenched in the Russian ethos, which was rooted in both traditional Orthodoxy, Communism and collective thinking. This discouraged any questioning of authority and taught passive reliance on command rather than staff assuming personal responsibility.[130] Lack of initiative was further exacerbated by complex, and sometimes contradictory nuclear security-related laws, regulations and guidance, which were difficult for personnel to understand.

126 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
127 Ibid., p.29.
128 National Research Council, Protecting Nuclear Weapons Material in Russia, The US National Academies Press, 1999, p.2.
129 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
130 Ibid., p.52.

Concluding Thoughts

The dissolution of the Soviet Union had a significant negative effect on nuclear security in Russia and other FSU countries, which took decades of sustained international efforts and billions of dollars of funding to resolve. 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'.[131] 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.

131 Ibid., p.viii.

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

Overview of the Crisis

Between 2015 and 2016, Belgium experienced a series of incidents that created the perception of a security crisis for its civil nuclear sector. Belgian nuclear security had previously been persistently criticised by US officials, and was found wanting in 2014 when one of the costliest ever acts of industrial sabotage at a nuclear facility was undertaken at the Doel nuclear power plant.[132] In combination with the subsequent discovery of hostile surveillance of a Belgian nuclear official in 2015 and the Brussels terrorist attacks of March 2016, this incident led to intense local and global media pressure on Belgium's government, the nuclear regulator and nuclear operators. Although there may never have been a credible plot against Belgium's nuclear industry, such fears forced the rapid implementation of security measures, overcoming prior inhibitions.

This case study demonstrates how security incidents and unreformed practices can undermine public confidence in a country's nuclear security during a period of elevated threat. In turn, the series of incidents led to security measures being hastily implemented that were either suboptimal or unsustainable. The Belgian regulator, the Federal Agency for Nuclear Control (FANC), played a leading public relations role and committed to ongoing security assessment and improvement, as well as further engagement with international partners to rectify outstanding issues. Whether the attention paid to nuclear security issues will be retained as Belgium moves to end nuclear power generation and the terrorist threat recedes is to be seen. Nonetheless, Belgium's experience serves to demonstrate the need to continually review potential threats outside of periods of crisis. This will assist in mobilising resources and consensus towards any needed security reforms, thereby helping in their effective deployment.

Nuclear Security in Belgium

Since the 1990s, Belgium has operated seven commercial nuclear power reactors and several research reactors. After the 9/11 attacks in the United States, security at these facilities became a national concern.[133] In 2003, Belgium empowered the FANC – its nuclear regulatory body – to inspect physical protection measures and improve operator procedures.[134] However, the George W. Bush administration did not believe that improvements were being implemented quickly enough, and in 2004 the US suspended deliveries of highly enriched uranium.[135] US officials in particular were concerned that during 'normal operations' Belgium permitted unarmed civilian guards within

132 Steven Mufson, 'Brussels attacks stoke fears about security of Belgian nuclear facilities', Washington Post, 25 March 2016. https://www.washingtonpost.com/world/europe/brussels-attacks-stoke-fears-about-security-of-belgian-nuclear-facilities/2016/03/25/7e370148-f295-11e5-a61f-e9c95c06ed-ca_story.html

133 Rony Dresselaers and Sylvain Fanielle, 'Nuclear Security in Belgium', in Tom Sauer (ed.), Nuclear Terrorism: Countering the Threat, Routledge, 2016, p.144.

134 Ibid., p.146.

135 R. Jeffrey Smith and Patrick Malone, 'A Terrorist Group's Plot to Create A Radioactive 'Dirty Bomb', The Center for Public Integrity, 29 February 2016. https://publicintegrity.org/national-security/a-terrorist-groups-plot-to-create-a-radioactive-dirty-bomb

their nuclear facilities.[136] There was a national capability to deploy a rapid response Federal Police Special Unit or proximate military forces in the event of an incident, but the response time of these forces was in doubt.[137]

Although Belgium committed to continuing security improvements, political initiative appeared to be indifferent during this period. Belgian officials relayed to their US counterparts that delays in 2007 were due to 'unforeseen technical, budgetary, and management issues' and a 'force on force' exercise run in 2009 was judged by US observers to be lacking in rigour.[138] Gradual improvements were made: in 2011, new site access conditions and security zones were introduced at nuclear power plants;[139] and in 2013, Belgium criminalised several nuclear security-related offences and improved insider threat prevention measures.[140] Despite these efforts, US officials believed that Belgian nuclear security improvements lagged behind their Europe neighbours.[141] The lack of a belief in a credible threat meant that bureaucratic inertia slowed progress.[142]

Reticence to introduce armed guards can be attributed to Belgium's domestic politics. Despite nuclear power accounting for 60% of Belgium's electricity generation capacity, the country committed in 2003 to phase out nuclear power by not replacing its present reactors.[143] Nuclear decommissioning in Belgium is politically contested as it runs counter to emission and energy security policy goals.[144] To remain in operation, the Belgian nuclear industry has tended to prioritise maintaining its image as safe and reliable. According to one commentator, this conflicts with nuclear power's 'perception problem,' where it is associated with accidents, proliferation and terrorism.[145] Belgian operators were hesitant to introduce armed guards as it would confirm accusation that nuclear power held inherent security risks.[146] Therefore even facing criticism from US counterparts, motivation for radical reform was lacking. Nevertheless, a November 2014 review of nuclear security in Belgium by the IAEA's International Physical Protection Advisory Service (IPPAS) found that the '[nuclear] physical protection system… is robust, with a program of continuous improvement in place at both the operator and government level… [the team also] identified numerous good practices.'[147]

The 2014 Doel Turbine Incident

The IPPAS finding of 'robust' security conflicted with the one of the costliest acts of suspected industrial sabotage in history. In August 2014, 65,000 litres of lubrication oil were drained from a power generation turbine into a sump at Doel 4, one of the four reactors at the Doel Nuclear Power Plant in East Flanders. The emergency firefighting valve regulating the lubricant was normally padlocked shut (in hindsight, a rudimentary security feature) but had been opened and the lock

136 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
137 Steven Mufson, 'Brussels attacks stoke fears about security of Belgian nuclear facilities', Washington Post, 25 March 2016. https://www.washingtonpost.com/world/europe/brussels-attacks-stoke-fears-about-security-of-belgian-nuclear-facilities/2016/03/25/7e370148-f295-11e5-a61f-e9c95c06edca_story.html; interview with nuclear security expert with experience of Belgian nuclear security, 20 August 2020.
138 R. Jeffrey Smith and Patrick Malone, 'A Terrorist Group's Plot to Create A Radioactive 'Dirty Bomb'
139 Christine Scharff, 'Les bons et les mauvais points en matière de sûreté nucléaire', L'Echo, 30 November 2016. https://www.lecho.be/entreprises/energie/Les-bons-et-les-mauvais-points-en-matiere-de-surete-nucleaire/9836774
140 R. Jeffrey Smith and Patrick Malone, 'A Terrorist Group's Plot to Create A Radioactive 'Dirty Bomb', The Center for Public Integrity, 29 February 2016. https://publicintegrity.org/national-security/a-terrorist-groups-plot-to-create-a-radioactive-dirty-bomb
141 Ibid.
142 Interview with nuclear security expert with experience of Belgian nuclear security, 20 August 2020.
143 Aviel Verbruggen, 'Belgian nuclear power life extension and fuss about nuclear rents', Energy Policy, Vol.60, September 2013, p.91.
144 Ibid., p.93.
145 Gilbert Eggermont, 'Kernenergie, een geloof met veel belangen,' SAMPOL, Vol.26, No.3, March 2019, p.52-57.
146 Luc Barbé, 'Moeten we opnieuw bang zijn van een vuile bom?' Mondiaal Nieuws, 9 March 2016. https://www.mo.be/opinie/moeten-we-opnieuw-bang-zijn-van-een-vuile-bom
147 'IAEA Reviews Nuclear Security in Belgium', IAEA News, 11 December 2014. https://www.iaea.org/newscenter/news/iaea-reviews-nuclear-security-belgium

discarded.[148] As a result, insider sabotage was suspected, although no one was ever charged in relation to the incident.[149] This event cost around 130 million euros in damage and lost income, and forced an emergency halt to operations – threatening Belgium's supply of electricity over the winter.[150] Although the contemporary security arrangements are unclear, they were insufficient to prevent the incident. Security measures also failed in sufficiently proving the identity of the perpetrator to see them charged. [151]

The failure to prevent the Doel 4 incident led the FANC to reflect that its prior focus for the previous decade had been 'at preventing external threats'.[152] Security improvements aimed at preventing future insider scenarios were enacted. These included the installation of additional CCTV cameras, restrictions on bringing mobile phones onsite, improvements to the workforces' ID badges and implementation of the two (or three) person rule in additional sensitive areas.[153] Training workshops on the insider threat were organised and the FANC instructed operators to proceed with 'increased internal vigilance'.[154] In addition, operators and the FANC undertook a six-year plan of security improvements.[155] Later in 2014, a project was also initiated that aimed to improve the security of Belgium's high-risk radiological sources.[156] Although improvements were already underway, when threats emerged two years later to Belgium's nuclear industry, they prompted a fresh crisis of confidence which saw further changes rapidly implemented in response.

THE DOEL NUCLEAR POWER PLANT

COPYRIGHT: BOUDEWIJN HUYSMANS

148 'Twijfels over snelle herstart van Doel 4', De Standaard, 9 August 2014. https://www.standaard.be/cnt/dmf20140808_01210540?
149 Brigitte Vermeersch and Luc Pauwels, 'Doel 4 ligt mogelijk tot einde van het jaar uit,' VRT NWS, 12 August 2014. https://www.vrt.be/vrtnws/nl/2014/08/12/doel_4_ligt_mogelijktoteindevanhetjaaruit-1-2058549
150 Thierry Goeman, 'Nog twee andere sabotagepogingen in Doel 4: gerecht komt nu voor het eerst met robotfoto' Nieuwsblad, 4 November 2019. https://www.nieuwsblad.be/cnt/dmf20191104_04699869; Brigitte Vermeersch and Luc Pauwels, 'Doel 4 ligt mogelijk tot einde van het jaar uit,' VRT NWS, 12 August 2014. https://www.vrt.be/vrtnws/nl/2014/08/12/doel_4_ligt_mogelijktoteindevanhetjaaruit-1-2058549
151 Interview with nuclear security expert with experience of Belgian nuclear security, 20 August 2020.
152 Rony Dresselaers and Sylvain Fanielle, 'Nuclear Security in Belgium', in Tom Sauer (ed.), Nuclear Terrorism: Countering the Threat, Routledge, 2016, p.153.
153 Maria Novak, 'The AFCN imposes stricter security measures for Belgian nuclear power stations', The Brussels Times, 16 December 2014. https://www.brusselstimes.com/news/belgium-all-news/30724/the-afcn-imposes-stricter-security-measures-for-belgian-nuclear-power-stations/
154 Rony Dresselaers, 'Security of Nuclear facilities in Belgium in a period of increased threat,' International Regulators Conference on Nuclear Security, May 2016. https://csnsecurityconference.org/presentations/may-11-2016/RDresselaers.pdf
155 Interview with nuclear security expert with experience of Belgian nuclear security, 20 August 2020.
156 Rony Dresselaers and Sylvain Fanielle, Nuclear Security in Belgium, in Tom Sauer (ed.), Nuclear Terrorism: Countering the Threat, Routledge, 2016, p.152.

Rising Terrorism Risk in Belgium

The threat posed to nuclear and radiological sites in Belgium stemmed from the rising overall terrorism risk within the country. This elevation in risk was linked to the activities of the now banned 'Shariah4Belgium' extremist group which openly operated between 2010 and 2012. The Shariah4Belgium network freely recruited and radicalised its members, with many going to fight overseas, mainly in Syria and Iraq.[157] By 2016, Belgium had the highest levels of foreign fighters per capita acting for Islamic State of any European country.[158]

One of these fighters included Ilyass Boughalab who was radicalised by Shariah4Belgium. Ilyass Boughalab worked as a weld inspector at Doel, where he had access to some of the site's sensitive areas until he left for Syria in November 2012.[159] Although not associated with any interests in nuclear terrorism according to public sources, Ilyass Boughalab allegedly passed his security clearance in Belgium after being radicalised by Islamist militancy.[160] Some contemporary media reports have mis-attributed a second worker at Doel having joined Islamic State, but these reports were in fact referring to another worker at the same subcontractor who did not have access to nuclear facilities.[161] Nonetheless, Ilyass Boughalab's case raised questions over Belgian nuclear security.

The elevated perceptions of risk posed by domestic radicalisation in Belgium during this period was paired with the rise of Islamic State and their apparent interest in CBRN terrorism.[162] By 2016, Islamic State had used chemical weapons in the Middle East and had communicated its intent to use radiological and nuclear weapons abroad.[163] Fortunately, Islamic State's aspirations outmatched its capabilities; cells interested in CBRN attacks exhibited limited expertise and there were several missed opportunities to exploit available materials.[164] Nonetheless, CBRN terrorism being perpetrated by Islamic State posed a looming threat for a number of countries.[165]

The rising terrorism risk to Europe manifested by returning Islamic State fighters was first demonstrated in May 2014 with an attack on the Jewish Museum of Belgium.[166] Following the attack on the Paris offices of magazine Charlie Hebdo in January 2015, police disrupted an Islamic State cell that was preparing to conduct a follow-up attack from within Belgium.[167] In light of the declining security situation, the Belgian government launched 'Operation Homeland', which saw the Belgian army deployed alongside the police to protect high-profile targets.[168] Although the prevailing terrorist security situation and sabotage to the Doel 4 turbine had heightened Belgium's awareness of

157 Guy Van Vlierden, 'How Belgium Became a Top Exporter of Jihad', Terrorism Monitor, The Jamestown Foundation, 29 May 2015. https://jamestown.org/program/how-belgium-became-a-top-exporter-of-jihad/
158 Andrea Rönsberg, 'A nuclear terrorism threat made in Belgium?' Deutsche Welle, 15 April 2016. https://www.dw.com/en/a-nuclear-terrorism-threat-made-in-belgium/a-19191458
159 'Belgian jihadist, former worker at Doel nuclear plant, dies in Syria', The Brussels Times, 16 October 2014. https://www.brusselstimes.com/news/belgium-all-news/29743/belgian-jihadist-former-worker-at-doel-nuclear-plant-dies-in-syria/
160 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. https://www.belfercenter.org/sites/default/files/legacy/files/PreventingNuclearTerrorism-Web.pdf
161 Personal correspondence to authors.
162 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. https://www.belfercenter.org/sites/default/files/legacy/files/PreventingNuclearTerrorism-Web.pdf
163 Columb Strack, 'The Evolution of the Islamic State's Chemical Weapons Efforts,' CTC Sentinel, Vol.10, No.9, October 2017.
164 Jennifer Smith, 'Islamic State has a 'dirty bomb' says British jihadi, amid claims 40kg of URANIUM was taken from Iraqi university,' Daily Mail, 30 November 2014. https://www.dailymail.co.uk/news/article-2854729/Islamic-State-dirty-bomb-says-British-jihadi-amid-claims-40kg-uranium-taken-Iraqi-university.html; 'Cobalt 60 Sources in Mosul: Recovery and Lessons for the Future,' Institute for Science and International Security, 22 July 2017. https://isis-online.org/isis-reports/detail/cobalt-60-sources-in-mosul-recovery-and-lessons-for-the-future
165 Columb Strack, 'The Evolution of the Islamic State's Chemical Weapons Efforts,' CTC Sentinel, Vol.10, No.9, October 2017.
166 Kenneth Lasoen, 'War of Nerves: The Domestic Terror Threat and the Belgian Army,' Studies in Conflict & Terrorism, Vol.42, No.11, February 2018.
167 Ibid.
168 Ibid.

THE DOEL NUCLEAR POWER PLANT
COPYRIGHT: FREDERIC PAULUSSEN

nuclear security issues, in early 2015 the FANC judged that there was 'no direct threat to the nuclear industry'.[169] This would change with the discovery of evidence that suggested an interest in targeting Belgium's nuclear industry.

An Increasing Security Threat?

Hostile Surveillance

On 13 November 2015, nine terrorists conducted a coordinated suicide bombing and gun attack in Paris – most notably at the Bataclan theatre – which resulted in the deaths of 130 people. Investigations by the Belgian authorities led them to search an apartment of a suspect connected with the Paris attacks.[170] Inside the apartment, police uncovered 10 hours' worth of covert surveillance footage of a scientist who worked at SCK-CEN, Belgium's nuclear research facility located in Antwerp province.[171] The camera had been hidden outside the scientist's house and recorded his daily schedule,[172] with the indication of a possible plot against a nuclear facility leaked to the Belgian press on 18 February 2016.[173] This was shortly followed by media reporting that information security at the SCK-CEN was lacking as the personal information of 50 employees could easily be found online, further heightening security concerns.[174] What, if any, plans this cell had made to attack parts of the Belgian nuclear industry remains unclear. A FANC official 'imagined' that the cell may have been in the early stages of planning a kidnapping plot, with the hostage being

169 Rony Dresselaers, 'Security of Nuclear facilities in Belgium in a period of increased threat', International Regulators Conference on Nuclear Security, May 2016.
170 R. Jeffrey Smith and Patrick Malone, 'A Terrorist Group's Plot to Create A Radioactive 'Dirty Bomb', The Center for Public Integrity, 29 February 2016. https://publicintegrity.org/national-security/a-terrorist-groups-plot-to-create-a-radioactive-dirty-bomb
171 Ibid.
172 Ibid.
173 Marie-Béatrice Baudet and Jean-Pierre Stroobants, 'Le nucléaire belge, cible potentielle des terroristes,' Le Monde, 26 March 2016. https://www.lemonde.fr/europe/article/2016/03/26/les-sites-nucleaires-belges-cibles-potentielles-des-terroristes_4890475_3214.html
174 Kurt Wertelaers, 'Zelfs familiefoto posten maakt van personeel doelwit,' Het Laatste Nieuws, 26 February 2016. https://www.hln.be/nieuws/zelfs-familiefoto-posten-maakt-van-personeel-doelwit~aeb61719

leveraged to obtain access to fissile or radiological material.[175] Further possibilities included plots to sabotage a nuclear facility, given the precedent at Doel in 2014, or a direct assault on a nuclear facility with the intention to cause a radioactive release.[176]

The Brussels Bombings

On 22 March 2016, a series of suicide bombings occurred at Brussels Airport and at a central metro station in the city, resulting in 32 deaths. Concerns over nuclear security within Belgium were further heightened after these attacks. Following the Brussels bombings, Belgium's national body empowered with setting the nation's threat level, the Coordination Unit for Threat Analysis (OCAD), raised its rating to level 4 (the highest rating) for the first time, signalling that further attacks were expected imminently.[177] Although a conventional attack, two of the suicide bombers were the brothers suspected of conducting the hostile reconnaissance uncovered on the SCK-CEN official in 2015.[178] Fears over nuclear security were further stoked that month by the murder of a G4S security guard in an apparent robbery at his home. In some media reporting, the guard was incorrectly identified as working at the Tihange nuclear powerplant rather than his actual workplace of the National Institute of Radioelements; it was also erroneously reported that his security badge had been stolen.[179] Belgian prosecutors denied both claims and any connection to terrorism.[180]

Efforts to Ensure Nuclear Security

Following increased Islamic State terrorist activity across Europe in 2015, the OCAD raised its threat level from level 2 to 3, as further attacks were judged 'possible and probable'.[181] Following the Brussels attacks on 22 March, the threat level was again raised by OCAD to level 4, then three days later reduced back to level 3.[182] These changes impacted the security postures of nuclear facilities across Belgium, with the FANC obliging operators to implement 'increased vigilance' under level 3.[183] During the immediate period after the Brussels bombings, when the OCAD level was set to 4, even more stringent measures were introduced to uphold security. This included all non-essential staff being sent home from Tihange and Doel, with the plants operating with staffing levels equivalent to a weekend shift.[184] Further access limits to nuclear facilities were implemented, alongside more thorough vehicle inspections.[185] In addition, the application of the two-person rule was expanded to more areas.[186] Although intended to reduce the chances of unauthorised access or hostile external action, these changes were clearly unsustainable if maintained over an extended

175 R. Jeffrey Smith and Patrick Malone, 'A Terrorist Group's Plot to Create A Radioactive 'Dirty Bomb', The Center for Public Integrity, 29 February 2016. https://publicintegrity.org/national-security/a-terrorist-groups-plot-to-create-a-radioactive-dirty-bomb; Steven Mufson, 'Brussels attacks stoke fears about security of Belgian nuclear facilities', Washington Post, 25 March 2016. https://www.washingtonpost.com/world/europe/brussels-attacks-stoke-fears-about-security-of-belgian-nuclear-facilities/2016/03/25/7e370148-f295-11e5-a61f-e9c95c06edca_story.html

176 Geert De Clercq and Christoph Steitz, 'Militant interest in attacking nuclear sites stirs concern in Europe,' Reuters, 30 March 2016. https://uk.reuters.com/article/uk-belgium-blast-nuclear/militant-interest-in-attacking-nuclear-sites-stirs-concern-in-europe-idUKKCN0WW1UC

177 Rony Dresselaers, 'Security of Nuclear facilities in Belgium in a period of increased threat', International Regulators Conference on Nuclear Security, May 2016.

178 'Brussels suspects linked to nuclear facility plot,' CBS, 24 March 2016. https://www.cbsnews.com/news/brussels-attacks-ibrahim-khalid-bakraoui-plot-belgium-nuclear-abdeslam

179 Jennifer Newton, 'Two Belgian nuclear power plant workers have joined ISIS leading to fears the jihadis have the intelligence to cause a meltdown disaster,' The Daily Mail, 26 March 2016. https://www.dailymail.co.uk/news/article-3510384/Belgian-nuclear-plant-guard-murdered-security-pass-stolen-two-days-Brussels-attacks.html

180 'Murder of Belgian man in charge of security at nuclear facility was "not linked to terror"', AFP, 26th March 2016. https://www.thejournal.ie/belgium-murder-not-linked-to-terror-2682143-Mar2016

181 'Jaarverslag 2016', FANC, 7 June 2017, p.92. https://fanc.fgov.be/nl/system/files/2016-jaarverslag-fanc-vf.pdf; Gert Vercauteren, 'Contribution by The Belgian Coordination Unit for Threat Analysis (CUTA),' International Conference on National and International Coordination In Counterterrorism, October 2013. https://rm.coe.int/1680640c5c

182 FANC, 7 June 2017, p.93. https://fanc.fgov.be/nl/system/files/2016-jaarverslag-fanc-vf.pdf

183 Ibid.

184 'Non-essential staff at Belgian nuclear plants Doel and Tihange sent home,' Reuters, 22 March 2016. https://uk.reuters.com/article/uk-belgium-blast-tihange/non-essential-staff-at-belgian-nuclear-plants-doel-and-tihange-sent-home-idUKKCN0WO1RK

185 Engie Electrabel, 'Verhoogde waakzaamheid in kerncentrales', 24 March 2016. https://web.archive.org/web/20170302032809/http://corporate.engie-electrabel.be/nl/nieuws/verhoogde-waakzaamheid-in-kerncentrales/

186 Ibid.

period – and were only upheld for several days during the peak of the crisis.[187]

A further measure intended to improve security, but which inadvertently contributed to the sense of crisis, was a decision to revoke four security passes and temporarily withdraw seven others from workers at the Tihange site.[188] According to a government official, three of the passes had already been under review, but withdrawal accelerated following the Brussels attacks, while the other had been revoked because an employee had commented positively on the attacks.[189] The FANC stressed that security clearances were constantly under review and that in the course of the past year, access had been revoked for 40 personnel.[190] However, Human Rights Watch later noted that all those immediately targeted in March were Muslims and were not informed about their suspended status or provided with subsequent explanation; by October 2016 two of the security clearances that had been suspended in March had been returned on appeal.[191]

Armed Onsite Guards

A more lasting change resulting from the concerns over security was the implementation of armed guards at Belgium's nuclear sites. On 22 December 2015, the federal government decided to create a federal police unit to protect critical infrastructure, including nuclear sites.[192] This was in response to the persistent security concerns in Belgium and the need to reduce reliance on the military forces that had been deployed in Operation Homeland since the start of 2015.[193] After considering the prevailing security situation and the time needed to create the new police force, the Belgian federal government decided on 4 March 2016 to deploy military personnel at nuclear sites, pending their eventual replacement.[194] On 18 March 2016, these new military guards first entered nuclear sites, four days before the Brussels bombings as part of Operation Spring Guardian.[195]

Given the events of March 2016, the OCAD threat level 4 and the limited but credible intelligence that suspects had considered nuclear-related terrorist action, the introduction of armed guards was a necessary reaction to the crisis. However, it was clear that the provision of 140 army personnel for this assignment was a transitionary arrangement. Belgian parliamentarians questioned whether these nuclear site deployments were sustainable alongside the protection of other vital national infrastructure and the normal defence and training commitments of the Belgian armed services.[196] The military rather than civilian nature of the guard force also ensured suboptimal compromises; the regular rotation of deployed military forces across nuclear sites meant that soldiers lacked site-specific knowledge.[197] In addition, soldiers were deployed only in sensitive areas of nuclear sites; in the event of an incident, this could introduce irregularities in a response as they might struggle to communicate and coordinate with the unarmed civilian guards, still charged with patrolling the majority of nuclear sites and on whom the military guards depended for detailed site awareness and access.[198]

187 Ibid.
188 Rachel Middleton, 'Fears Brussels cell was plotting radioactive attack after 11 nuclear workers' access passes revoked', ibtimes.co.uk, 25 March 2016. https://www.ibtimes.co.uk/fears-brussels-cell-plotting-radioactive-attack-after-11-nuclear-workers-have-access-passes-revoked-1551536
189 Ibid.
190 Steven Mufson, 'Brussels attacks stoke fears about security of Belgian nuclear facilities', Washington Post, 25 March 2016. https://www.washingtonpost.com/world/europe/brussels-attacks-stoke-fears-about-security-of-belgian-nuclear-facilities/2016/03/25/7e370148-f295-11e5-a61f-e9c95c06edca_story.html
191 'Grounds for Concern: Belgium's Counterterror Responses to the Paris and Brussels Attacks', Human Rights Watch, 3 November 2016. https://www.hrw.org/report/2016/11/03/grounds-concern/belgiums-counterterror-responses-paris-and-brussels-attacks
192 Federaie Politie 'Directie van Beveiliging'. http://www.politiestudies.be/userfiles/DAB%20Eric%20Delhez.pdf
193 Ibid.
194 Rony Dresselaers, 'Security of Nuclear facilities in Belgium in a period of increased threat', International Regulators Conference on Nuclear Security, May 2016.
195 B. Carlé and M. Vanderthommen, 'SCK-CEN's security awareness program after Paris & Brussels attacks' Ricomet Conference, 13 June 2018. https://ricomet2018.sckcen.be/-/media/Files/Ricomet2018/Presentations/Wednesday/5_Carle-SCK-security-awareness.pdf?
196 Kenneth Lasoen, 'War of Nerves: The Domestic Terror Threat and the Belgian Army,' Studies in Conflict & Terrorism, Vol.42, No.11, February 2018.
197 Interview with nuclear security expert with experience of Belgian nuclear security, 20 August 2020.
198 Ibid.

The new Directorate of Security (DAB; Directie van Beveiliging in Dutch) was launched in March 2017 but in fact spent the next year recruiting and training its first cohort of armed guards.[199] The first detachment of DAB personnel were assigned to Doel and Tihange in September 2018 to start the transition process away from military guards, who by then still deployed 63 military personnel in protection of nuclear sites.[200] While the transition from the military to the DAB was originally intended to be completed by 2020 across all of Belgium's critical infrastructure, the DAB has suffered recruitment issues and the protection of vital infrastructure by the military is ongoing.[201]

Public Relations during a Crisis

The perception of historically flawed security at nuclear sites, the murder of the G4S guard, deployment of the military, the revocation of access passes and an inflated sense of radicalisation in Belgium's nuclear industry all combined to generate intense media coverage of nuclear security. The level of media speculation over Belgian nuclear security was assisted by the existence of the surveillance footage uncovered in November having been leaked to the press in February 2016 rather than announced, thereby undermining trust.[202] Even if Belgium's nuclear infrastructure faced no credible threat between 2015 and 2016, the previous events created at least the perception of a crisis. This lack of faith in Belgian nuclear security also resonated internationally, as demonstrated by a specific motion on Belgian nuclear security in the European Parliament.[203]

The FANC felt under intense pressure to respond and communicate to mitigate the elevated levels of anxiety.[204] FANC officials played an important public-facing role in dispelling panic by routinely offering comments to media in March 2016; this included reiterating that there was no known intelligence beyond the surveillance footage there was ever a plot against a nuclear facility, that increased measures were being taken in line with the OCAD threat levels, and that security improvement were being made as part of an ongoing process since 2014.[205] These efforts were assisted by officials from the Foreign Ministry, Ministry of Interior, local and federal prosecutors' offices and the plant operators themselves.[206] Beyond the immediate crisis in March, the FANC played an important role in reassuring the international community that nuclear security was being upheld in Belgium. This included statements on progress and firm commitments of improvements at the 2016 Nuclear Security Summit, a state-level international event to discuss the prevention of nuclear terrorism. During the summit, senior officials from the FANC briefed the global nuclear security community as to how it had responded to the events in Belgium.[207]

Lasting Impacts for Nuclear Security

The extent to which the events of 2016 allowed for a reprioritisation towards nuclear security is contested. Gradual improvements were already underway and clearly accelerated after 2014 when it

199 Marie-Madeleine Courtial, 'La DAB sur le point de reprendre les missions de l'opération Spring Guardian,' DefenceBelgium.com, 12 September 2018. https://defencebelgium.com/2018/09/12/la-dab-sur-le-point-de-reprendre-les-missions-de-loperation-spring-guardian/
200 Ibid.
201 Ibid.
202 'Exclusif: les kamikazes des attentats de Paris visaient nos centrales nucléaires!' La Dernière Heure, 17 February 2016. https://www.dhnet.be/actu/belgique/exclusif-les-kamikazes-des-attentats-de-paris-visaient-nos-centrales-nucleaires-56c392303570b1fc1130638b
203 Mara Bizzotto, 'Motion for a Parliament resolution on security at nuclear sites in Belgium' European Parliament, 25 May 2016. https://www.europarl.europa.eu/doceo/document/B-8-2016-0556_EN.html?redirect
204 Rony Dresselaers, 'Security of Nuclear facilities in Belgium in a period of increased threat', International Regulators Conference on Nuclear Security, May 2016.
205 Steven Mufson, 'Brussels attacks stoke fears about security of Belgian nuclear facilities', Washington Post, 25 March 2016. https://www.washingtonpost.com/world/europe/brussels-attacks-stoke-fears-about-security-of-belgian-nuclear-facilities/2016/03/25/7e370148-f295-11e5-a61f-e9c95c06edca_story.html
206 Matthias Verbergt, 'Belgian Police Find Surveillance Tape of Nuclear Worker's Home' The Wall Street Journal, 17 February 2016. https://www.wsj.com/articles/belgian-police-find-surveillance-tape-of-nuclear-workers-home-1455708344
207 Rony Dresselaers, 'Security of Nuclear facilities in Belgium in a period of increased threat', International Regulators Conference on Nuclear Security, May 2016; Belgian Government, 'National Progress Report: Belgium', Nuclear Security Summit 2016, 31 March 2016. http://www.nss2016.org/document-center-docs/2016/3/31/national-progress-report-belgium

became apparent that the terrorist risk in Europe was increasing. However, the 2015 attacks in Paris, uncovering of the surveillance footage in Belgium, media fears over nuclear security and Brussels bombings allowed the voices of security professionals to be heard to an extent previously not possible.[208] Although government spokespeople denied a 'direct link' between the hostile reconnaissance and 'the decision to take… additional security measures,' it is reasonable to conclude that the perceived security crisis spurred action.[209] For example, the addition of armed guards had been a US priority since 2001 and had been under consideration since the IAEA IPPAS mission in 2014.[210] Their introduction was a significant shift in Belgium's approach to nuclear security.[211] It appears that the rising security risk between 2015 and 2016 was sufficient to overcome outstanding social, political and economic concerns.[212]

Whether the events during this period in Belgium will ensure that nuclear security will be proactively maintained is an area of concern. Scholars Ackerman and Halverson expressed their concerns that the initiative could be lost when the events of 2015 and 2016 'fade from the front pages'.[213] The terrorism risk in Belgium has lowered to the extent that OCAD reduced its threat level back to 2 in 2018.[214] Even so, since 2016 the regulator has stressed the ongoing importance of continuous assessment and liaison between licensees, OCAD and the FANC.[215] The FANC and plant operators have also continued to engage the international community, and particularly with the National Nuclear Security Administration in the United States, to ensure ongoing review of nuclear security in Belgium.[216] Engagement has included a follow up IAEA Integrated Regulatory Review Service in 2017 and another IPPAS mission in 2019 which 'saw significant enhancements since 2014'.[217]

The FANC continues to both assess security at facilities under its purview by conducting exercises and contracting national and international consultants.[218] After a cyber security incident in early 2016 and the leak of Tihange's site plans onto the darknet in the same year, the FANC has highlighted the improvements made to cybersecurity and a new law strengthening regulation at all sites housing radioactive material was passed in 2019.[219] Belgium has also recently launched a programme to review and improve security at research reactors and is now using low enriched uranium (LEU) to produce medical isotopes.[220] Nonetheless, in the immediate years following the Brussels bombings, challenges were identified in upholding Belgian nuclear security. External

208 Interview with nuclear security expert with experience of Belgian nuclear security, 20 August 2020.
209 'Belgian army to protect nuclear sites: interior ministry', Reuters, 4 March 2016. https://www.reuters.com/article/us-belgium-nuclear-security-idUSKCN0W61KR; Steven Mufson, 'Brussels attacks stoke fears about security of Belgian nuclear facilities', Washington Post, 25 March 2016. https://www.washingtonpost.com/world/europe/brussels-attacks-stoke-fears-about-security-of-belgian-nuclear-facilities/2016/03/25/7e370148-f295-11e5-a61f-e9c95c06edca_story.html
210 Interview with nuclear security expert with experience of Belgian nuclear security, 20 August 2020.
211 Luc Barbé, 'Moeten we opnieuw bang zijn van een vuile bom?', Mondiaal Nieuws, 9 March 2016.
212 Interview with nuclear security expert with experience of Belgian nuclear security, 20 August 2020.
213 Gary Akerman and James Halverson, 'Not Secure Enough: The Threat Of Terrorists Acquiring Nuclear Materials Is Still Serious', War on the Rocks, 6th April 2016. https://warontherocks.com/2016/04/not-secure-enough-the-threat-of-terrorists-acquiring-nuclear-materials-is-still-serious/
214 'Belgium lowers terror alert level', VRT NWS, 22 January 2018. https://www.vrt.be/vrtnws/en/2018/01/22/belgium_lowers_terroralertlevel-1-3130814/
215 Rony Dresselaers, 'Security of Nuclear facilities in Belgium in a period of increased threat', International Regulators Conference on Nuclear Security, May 2016.
216 'NNSA Administrator, Belgium Ambassador announce new international working group to address insider threats', National Nuclear Security Administration (NNSA), 11 February 2020. https://www.energy.gov/nnsa/articles/nnsa-administrator-belgium-ambassador-announce-new-international-working-group-address
217 'IAEA Completes Nuclear Security Advisory Mission in Belgium,' IAEA News, 21 June 2019. https://www.iaea.org/newscenter/pressreleases/iaea-completes-nuclear-security-advisory-mission-in-belgium; 'Integrated Regulatory Review Service (IRRS) Follow-Up Mission to Belgium,' FANC (2017). https://fanc.fgov.be/nl/system/files/irrs-belgium-2017-follow-up-final-mission-report.pdf
218 Interview with nuclear security expert with experience of Belgian nuclear security, 20 August 2020.
219 Alissa J. Rubin and Milan Schreuer, 'Belgium Fears Nuclear Plants Are Vulnerable', New York Times, 25 March 2016. https://www.nytimes.com/2016/03/26/world/europe/belgium-fears-nuclear-plants-are-vulnerable.html; Christine Scharff, 'Les bons et les mauvais points en matière de sûreté nucléaire', L'Echo, 30 November 2016. https://www.lecho.be/entreprises/energie/Les-bons-et-les-mauvais-points-en-matiere-de-surete-nucleaire/9836774; Rony Dresselaers and Sylvain Fanielle, Nuclear Security in Belgium, in Tom Sauer (ed.), Nuclear Terrorism: Countering the Threat, Routledge, 2016. p.150-151.
220 World Nuclear News, 'Belgium starts producing Mo-99 using LEU,' WNN.org, 4 May 2020. https://world-nuclear-news.org/Articles/Belgium-starts-producing-Mo-99-using-LEU

experts and internal exercises identified flaws with the security at Belgian nuclear power plants.[221] Although the FANC recognised in 2016 that it needed to improve its security culture, these assessments identified examples of complacency where flaws that could serve to weaken security implementation had been overlooked.[222]

A further concern is the sustainability of security measures introduced after the events of 2016. Due to a desire for uniformity across nuclear sites, the FANC employs a partially prescriptive approach to security regulation.[223] The general problem with such an approach is that urgency combined with a lack of dialogue between the regulator and operators could lead to the implementation of systems that could potentially be less secure and more expensive than alternatives.[224] The uncertain long-term future of Belgium's nuclear sector has also affected industry-wide appetite for ongoing improvements. While the FANC had planned to require new investments to improve Belgium's reactors resilience to terrorist attacks, uncertainty over the future of the nuclear industry has led to delays.[225] Retaining a suitable priority for nuclear security will also prove challenging now the decommissioning of Belgium's nuclear power stations has now been confirmed for 2025.[226]

Concluding Thoughts

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 the Brussels bombings. The FANC 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.'[227]

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. 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.

221 Interview with nuclear security expert with experience of Belgian nuclear security, 20 August 2020.
222 Ibid.
223 Rony Dresselaers and Sylvain Fanielle, Nuclear Security in Belgium, in Tom Sauer (ed.), Nuclear Terrorism: Countering the Threat, Routledge, 2016. p.148.
224 Interview with nuclear security expert with experience of Belgian nuclear security, 20 August 2020.
225 Christine Scharff and Tobe Steel, 'Le gendarme du nucléaire prépare la prolongation,' L'Echo, 20 February 2019. https://www.lecho.be/entreprises/energie/le-gendarme-du-nucleaire-prepare-la-prolongation/10099427.html; Daphne Psaledakis and Bate Felix, 'Belgium unprepared for phasing out nuclear power by 2025: grid operator,' Reuters, 28 June 2019. https://www.reuters.com/article/us-belgium-nuclearpower/belgium-unprepared-for-phasing-out-nuclear-power-by-2025-grid-operator-idUSKCN1TT233
226 Maxime Vande Weyer, '7.000 emplois menacés par la fermeture des centrales nucléaires', L'Echo, 9 October 2020. https://www.lecho.be/entreprises/energie/7-000-emplois-menaces-par-la-fermeture-des-centrales-nucleaires/10256991.html
227 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

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

Introduction

The case of the 2011 Fukushima Daiichi nuclear disaster in Japan serves as a dramatic example of how weaknesses in organisational culture, senior leadership and the wider regulatory system can lead to catastrophic consequences for a country's nuclear industry. The Fukushima disaster was classified as level 7 on the International Nuclear Event Scale (INES), making it the second most serious nuclear incident in history after the 1986 Chernobyl disaster.[228] A series of subsequent investigations recognised that natural causes – namely the earthquake and tsunami – triggered the crisis itself, but also identified human error as a key contributing factor and showed that many of the technical failures could have been anticipated. The Fukushima disaster marked a significant turning point for the global nuclear industry by highlighting the dangers of 'regulatory capture' in an advanced nuclear country. It also drew attention to the powerful impact of cultural and social norms on the effective implementation of nuclear safety and security.

Most studies on the Fukushima disaster have focused on its nuclear safety aspects, which is a logical approach given the impact on human health and the environment. Nevertheless, there are valuable lessons to be drawn from viewing the disaster through a nuclear security lens; indeed, it is not outlandish to hypothesise that the events leading to the crisis phase could have been set up by malicious actors – to launch either a terrorist attack or an act of sabotage. In particular, the case indicates what a successful insider attack could potentially achieve if both the regular and the back-up cooling systems of a nuclear power plant were to be disrupted. This case study looks in detail at how the events unfolded during the crisis phase, and then takes a broader view by comparing the situation at Japan's other nuclear power plants. While the locus of the crisis was the Fukushima Daiichi power plant, this case study highlights how organisational, regulatory and leadership failures can undermine nuclear safety and security across a country's entire nuclear industry.

Overview of the Crisis

The crisis unfolded on 11 March 2011 after a 9.0-magnitude earthquake struck near the north-east coastline of Japan's main Honshu island, triggering a tsunami which in places reached heights up to 40 metres. Coastal settlements were inundated, and an estimated 19,000 people were killed. Preceding the earthquake, 11 reactors at four nuclear power plants across the region had been operating: Tokyo Electric Power Company's (TEPCO's) Fukushima Daiichi reactors 1, 2 and 3; TEPCO's Fukushima Daini reactors 1, 2, 3 and 4; Tohoku's Onagawa reactors 1, 2 and 3; and Japco's Tokai.[229] Automated systems enabled the fission reactions of all these active reactors to be shut down

228 'Fukushima Daiichi Accident', World Nuclear Association, May 2020. https://www.world-nuclear.org/information-library/safety-and-security/safety-of-plants/fukushima-daiichi-accident.aspx#:~:text=Following%20a%20major%20earthquake%2C%20a,in%20the%20first%20three%20days
229 'Fukushima Daiichi Accident', World Nuclear Association, May 2020. https://www.world-nuclear.org/information-library/safety-and-security/safety-of-plants/fukushima-daiichi-accident.aspx#:~:text=Following%20a%20major%20earthquake%2C%20a,in%20the%20first%20three%20days

immediately. The earthquake severely impaired Fukushima Daiichi's 40-year-old plant, but a newly-constructed emergency operations centre built on higher ground ensured that staff were able to evacuate safely.[230] However, crucially, the earthquake had knocked out power lines supplying electricity from the local grid – prompting onsite emergency diesel generators and batteries to operate.[231]

It was when the tsunami waves overcame the seawall at Fukushima Daiichi 40 minutes later that the situation deteriorated,[232] with flooding in the lower ground floors of reactors 1, 2 and 3, as well as reactor 4 which had been undergoing routine maintenance. Critically, a wave of approximately 14 metres in height disabled 12 out of 13 diesel generators that had been providing back-up power to reactors 1, 2 and 3. Heat exchangers for transferring reactor waste heat to the ocean were also damaged. As a result, the three reactors were unable to maintain their cooling and water circulation functionality, and their fuel cores largely melted down. Exacerbating the crisis, hydrogen gas that had built up inside the reactors was vented to relieve the pressure, but this triggered a series of hydrogen explosions which destroyed the outer buildings of the reactors. The ensuing release of volatile radioisotopes into the atmosphere led to Fukushima's level 7 classification on the INES scale.[233] For residents, an evacuation order was issued that day for those living within 10km of the plant. By the following day, the radius was extended to 20km – resulting in over 100,000 people being evacuated.[234] The vast majority of those displaced never returned.[235]

Due to the lethal doses of radiation inside the reactors, the clean-up operation was beset by technical challenges and, ultimately, required a long lineage of remotely piloted robots to undertake clearing and decontamination tasks over the next decade.[236] At the time of writing, Fukushima Daiichi has moved from a crisis management and emergency situation to a more stabilised environment.[237] Fuel assemblies have been partially removed and efforts are ongoing to limit radioactive contamination. The next steps involve a full decommissioning of the plant, which TEPCO estimates will take 30-40 years.[238]

Impact of the Crisis at Fukushima Daiichi

In the aftermath of the earthquake and tsunami, the immediate priority was responding to the acute crisis phase.[239] Owing to the nature of the disaster – but also because nuclear security was a peripheral matter in Japan at the time – this was overwhelmingly a crisis management response focused on nuclear safety. Hundreds of TEPCO workers, contractors, firefighters and military personnel were deployed to the scene. Their primary goal was averting a nuclear meltdown through re-establishing cooling systems, restoring power and replenishing the overheated spent fuel ponds.

230 Scott Sagan and Edward Blandford (eds.) Learning from a Disaster: Improving Nuclear Safety and Security after Fukushima, Stanford: Stanford University Press, 2016.
231 James M. Acton and Mark Hibbs, 'Why Fukushima was Preventable', Carnegie Endowment for International Peace, 6 March 2012. https://carnegieendowment.org/2012/03/06/why-fukushima-was-preventable-pub-47361
232 'The Fukushima Daiichi Accident: Report by the Director General', IAEA, GC(59)/14, 2015. https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1710-ReportByTheDG-Web.pdf
233 'Fukushima-Daiichi INES rating Increased to Level 7', Independent Nuclear News Agency (NUCNET), 12 April 2011. https://www.nucnet.org/news/fukushima-daiichi-ines-rating-increased-to-level-7
234 'The Fukushima Daiichi Accident: Report by the Director General', IAEA, GC(59)/14, 2015. https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1710-ReportByTheDG-Web.pdf
235 Xuan Bien Do, 'Fukushima Nuclear Disaster Displacement: How far people moved and determinants of evacuation destinations', International Journal of Disaster Risk Reduction, February 2019, Vol.33, p.235-252
236 'The Robot Assault on Fukushima', Wired, 26 April 2018. https://www.wired.com/story/fukushima-robot-cleanup/
237 'Fukushima Decommissioning moves forward', World Nuclear News, 17 September 2019. https://www.world-nuclear-news.org/Articles/Fukushima-decommissioning-moves-forward
238 Mid-and-Long Term Roadmap towards the Decommissioning of TEPCO's Fukushima Daiichi Nuclear Power Station Units 1-4', Japanese Ministry of Economy, Trade and Industry (METI). https://www.meti.go.jp/english/earthquake/nuclear/decommissioning
239 Tero Varjoranta, 'Management of Nuclear Crises: Accidents and lessons learned', Managing Nuclear Projects, Woodhead Publishing Series in Energy, 2013. https://www.sciencedirect.com/science/article/pii/B9780857095916500159

These early efforts were vital in preventing further releases of radiation contamination. However, although onsite staff broadly followed established safety protocols, the earthquake had paralysed telecommunications networks and other critical infrastructure, undermining the pace and efficiency of the operation. Exacerbating the crisis, public transportation ceased to function, and roads descended into chaos as people tried to escape from the area.

Crucially, inadequate communication across all levels of decision-making undermined the emergency response in the days following the Fukushima Daiichi disaster.[240] In particular, the locus of emergency command was obscured because TEPCO's senior management team was unable to travel to the company headquarters or issue instructions to onsite staff; equally, the offsite emergency operations centre 5km from the plant was inoperable due to physical damage. This led the Prime Minister's office taking the extraordinary step of overseeing the crisis management response at Fukushima Daiichi, supported by Japan's then-regulator, the Nuclear and Industrial Safety Agency (NISA). The government itself suffered telecommunications difficulties, and an over-reliance on outdated information hampered the wider relief effort. Relations between the government and TEPCO's management quickly deteriorated.

Despite the responsibility for the emergency operation resting with TEPCO, the then-Prime Minister Naoto Kan took the unprecedented decision of setting up a joint government-TEPCO command centre within TEPCO. This new structure ultimately improved communication in the multi-agency operation (for example, it helped shore up work on water injections to stabilise the reactors).[241] Nevertheless, the debacle highlighted that emergency preparedness mechanisms in Japan were inadequate. It also drew attention to weaknesses in the country's multi-agency response to a serious incident.

The impacts of the earthquake and particularly the tsunami on security systems at Fukushima Daiichi were considerable. In 2016, the National Academy of Sciences in the United States produced a technical study on lessons learnt from the disaster and identified evidence of 'substantial' degradation in aspects of particular relevance to nuclear security.[242] This included the enormous damage to physical infrastructure, most notably to plant access controls in the protected areas. The report also claimed that loss of offsite power 'probably' resulted in security equipment that required electricity not operating continuously during the blackout period, which lasted until 9-11 days after the disaster.[243] A third aspect identified in the report was the absence of onsite security personnel. The majority of plant workers were evacuated to higher ground just before the tsunami struck and there was a short period when the Security Guidance Team, which was responsible for access control at the plant, was removed completely.[244]

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.[245] 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.

240 Scott Sagan and Edward Blandford (eds.) Learning from a Disaster: Improving Nuclear Safety and Security after Fukushima, Stanford: Stanford University Press, 2016.
241 Kenji E. Kushida, 'Japan's Fukushima Nuclear Disaster: An Overview', Scott Sagan and Edward Blandford (eds.) Learning from a Disaster: Improving Nuclear Safety and Security after Fukushima, Stanford: Stanford University Press, 2016.
242 '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
243 Ibid.
244 Ibid.
245 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/

And as discussed in more detail below, few of these workers had been subjected to thorough background checks. All of these factors made the site vulnerable to a potential adversary – particularly in terms of an insider – who might take advantage of the confusion created by the crisis, such as gaining unauthorised access to potentially unsecured nuclear materials.

Impact of the Crisis at other Nuclear Facilities

The earthquake and tsunami that overwhelmed Fukushima Daiichi had a very different impact on Japan's other nuclear power plants not far away. At Tohoku's Onagawa plant, 180 km to the north-east, the natural disaster caused widespread damage, though not to the same extent as at Fukushima Daiichi. This was perhaps surprising considering the Onagawa plant is situated on the Oshika Peninsula, only 125 km from the hypocentre of the earthquake.[246] The damage at Onagawa included fires in the turbine building, severing of most connections to offsite power, disabling of emergency generators, a halt to spent fuel cooling, the collapse of a heavy oil storage tank and access roads being cut off. Meanwhile at Fukushima Daini, Daiichi's sister plant 12km to the south, the damage from the earthquake and tsunami was even less severe. These other two cases are useful to consider alongside Fukushima Daiichi as they provide insights about how similar events led to different outcomes as a result of human factors such as leadership and communication.

In particular, the role of leadership was an important differentiating factor in the response at these two other nuclear plants. At Fukushima Daini, site superintendent Naohiro Masuda received widespread praise for his part in helping protect the facility. According to one account, Masuda was able to persuade his colleagues to take action to prevent a crisis unfolding despite the known risks of radiation contamination by acknowledging the 'evolving reality' in which they were operating.[247]

In what the organisational theorist Karl Weick and others call the 'sensemaking' process, Masuda arrived at a common understanding with his team through recalibrating and iterating their actions at each stage of the emergency response – enabling them to adapt their behaviour and work through challenges.[248] Crisis management protocols were strictly followed in the early phase of the disaster but the unfolding events – in particular, when three of the four reactors lost their cooling functions – required a more flexible approach. Masuda responded by sharing frequent updates with the workers as information became available, thereby replacing uncertainty with meaning. In effect, the team 'acted their way into a better understanding of the challenges they faced'.[249]

Meanwhile when the earthquake struck Tohoku's Onagawa plant, the site superintendent was not onsite, and an acting superintendent took charge. Access control was a critical element of implementing the response plan and the Onagawa workforce was well-prepared owing to emergency response exercises being conducted regularly in the past.[250] The General Affairs Division, responsible for security, asked its sub-contractor to 'secure personnel in accordance with the manual for a general disaster'.[251] Nevertheless, in the immediate aftermath of the tsunami, the Japanese Self-Defense Forces were initially unavailable to attend Onagawa, being preoccupied with other emergency calls. Instead, the national police provided patrol and access control support and the Mayor of the evacuated ward was designated 'guarantor' for nuclear material protection. Following the tsunami warning, patrols assessed damage at Onagawa while also securing lines of

246 'Responses to the Tohoku-Pacific Ocean Earthquake and Tsunami at the Onagawa Nuclear Power Station and Tokai No.2 Power Station', Japan Nuclear Safety Institute, August 2013. http://www.genanshin.jp/english/archive/disastersitereaction/data/report_OnTk.pdf
247 Ranjay Gulati, Charles Casto and Charlotte Krontiris, 'How the Other Fukushima Plant Survived', Harvard Business Review, July-August 2014. https://hbr.org/2014/07/how-the-other-fukushima-plant-survived
248 Ibid.
249 Ibid.
250 'Responses to the Tohoku-Pacific Ocean Earthquake and Tsunami at the Onagawa Nuclear Power Station and Tokai No.2 Power Station', Japan Nuclear Safety Institute, August 2013. http://www.genanshin.jp/english/archive/disastersitereaction/data/report_OnTk.pdf
251 Ibid.

IAEA REMEDIATION EXPERT MISSION IN FUKUSHIMA
COPYRIGHT: IAEA

communication.[252] With capacity to provide sanctuary – in effect demonstrating that its nuclear materials were considered secure – Onagawa opened as a shelter and makeshift medical centre to evacuees from the local ward. The nuclear facility also allowed nearby ships to dock at the facility's bay as nearby ports were damaged. Nevertheless, tracking all these individuals entering and leaving the facility proved challenging to sustain.[253]

While the impact of the earthquake and tsunami did not lead to a nuclear crisis at Onagawa and Daini – and there were localised examples of 'good practice' – neither of these plants were insulated from the broader governance, regulatory and organisational weaknesses endemic in the country's wider nuclear industry. It is notable that the Japanese scholar Kazuto Suzuki has argued that the comparative lack of damage to other nuclear sites from the March 2011 earthquake and tsunami led to some duty-holders 'to resist substantial investments in improved safety and security systems'.[254] In effect, some interest groups preferred to frame the crisis at Fukushima as localised problem specific to one particular site and duty-holder. This raises the issue of how to proportion responsibility for when things go wrong (or right) to the various decision-making processes that determine the dynamics of a crisis, whether it be at the level of the plant, regulator or government.

Findings of Investigations into the Nuclear Disaster

The Fukushima disaster fundamentally overhauled global perceptions about the safety of nuclear power plants. While the earthquake and tsunami could not have been avoided, organisational and regulatory weaknesses had hampered the development of robust safety measures in Japan and, correspondingly, the crisis management response too. An IAEA report released in 2015 highlighted the failure of staff to challenge authority and an industry-wide complacency about nuclear safety.

252 Ibid.
253 Ibid.
254 Kazuto Suzuki, 'Encouraging Transnational Organizational Learning' in Scott Sagan and Edward Blandford (eds.) Learning from a Disaster: Improving Nuclear Safety and Security after Fukushima, Stanford: Stanford University Press, 2016.

The IAEA's Director General Yukiya Amano stated, 'A major factor that contributed to the accident was the widespread assumption in Japan that its nuclear power plants were so safe that an accident of this magnitude was simply unthinkable'.[255]

In addition to the IAEA report, several investigations were launched domestically to examine the causes of the Fukushima disaster and make future policy recommendations. Offering some overlapping but also distinct conclusions – mostly focused on nuclear safety – these investigations were initiated by various stakeholders, among them: The Cabinet of Japan led by Kan Naoto of the ruling Democratic Party of Japan[256]; the National Diet (Japan's parliament)[257]; a private group of citizens led by Funabashi Yoichi, former editor of the Asahi newspaper[258]; and TEPCO itself[259]. The reports of these investigations serve as useful reference points for Japan's ongoing reform of its nuclear sector, including the evolution of nuclear security in the country.

These four 'official' investigations displayed broad consensus about the underlying human factors behind the disaster. Indeed, the public dissection of the national psyche was unprecedented in some of the findings. The Japanese parliament (National Diet) had established an Independent Investigation Commission to 'determine the causes of the accident…and those of the damages generated by the accident, and…[make] policy proposals designed to prevent the expansion of the damages and the recurrence of similar accidents in the future.'[260]. Its final report, released in July 2012, contended that the natural causes of the disaster were not unanticipated, and that TEPCO had failed to invest in basic safety requirements, including risk assessments, evacuation plans and containment contingencies. The report concluded, 'What must be admitted – very painfully – is that this was a disaster "Made in Japan."…Its fundamental causes are to be found in the ingrained conventions of Japanese culture: our reflexive obedience; our reluctance to question authority; our devotion to "sticking with the program"; our groupism, and our insularity'.[261] Most controversially, the report argued that the accident was a result of 'collusion' between the government, regulators and TEPCO.[262]

The conclusions of the four investigations had far-reaching implications for nuclear security too. Fukushima had exposed the vulnerability of existing security measures that went beyond the installation of expensive physical protection systems. The crisis revealed that it was possible for a serious nuclear incident to potentially occur through the sabotage of vital facilities, for instance by an insider – highlighting the previously under-explored scenario of disruption to both regular and back-up cooling systems. There was also greater recognition across the global nuclear industry of how security risks are elevated in the aftermath of a disaster, whether this is triggered by a safety or a security incident, due to the arrival onsite of large numbers of emergency and contract workers. Even despite the relative 'success' of crisis management efforts at Onagawa, tracking the movements of individuals entering and leaving the site proved to be a challenge.[263] This highlighted the need to maintain protective functions for the duration of a crisis, including when there exist high levels of

255 Yukiya Amano, Message from the Director General, 'The Fukushima Daiichi Accident: Report by the Director General and Technical Volumes', International Atomic Energy Agency (IAEA), 2 September 2015. https://www.iaea.org/sites/default/files/fr-brochure.pdf
256 Investigation Committee on the Accident at Fukushima Nuclear Power Stations of Tokyo Electric Power Company, 23 July 2012. https://www.cas.go.jp/jp/seisaku/icanps/eng/finalgaiyou.pdf
257 National Diet of Japan, The Official Report of The Fukushima Nuclear Accident Independent Investigation Commission, 2012. https://www.nirs.org/wp-content/uploads/fukushima/naiic_report.pdf
258 Independent Investigation Commission on the Fukushima Daiichi Nuclear Accident, 28 February 2012. https://apinitiative.org/en/project/fukushima (also see Routledge edition in English published on 6 March 2014)
259 Fukushima Nuclear Accident Analysis Report, TEPCO, 20 June 2012. https://www.tepco.co.jp/en/press/corp-com/release/betu12_e/images/120620e0104.pdf
260 Website of the Investigation Committee on the Accident at the Fukushima Nuclear Power Stations of the Tokyo Electric Power Company, 2011. https://www.cas.go.jp/jp/seisaku/icanps/eng/
261 'The Fukushima Nuclear Accident Independent Investigation Commission', The National Diet of Japan, July 2012. http://large.stanford.edu/courses/2013/ph241/mori1/docs/NAIIC_report_hi_res10.pdf
262 Ibid.
263 'Responses to the Tohoku-Pacific Ocean Earthquake and Tsunami at the Onagawa Nuclear Power Station and Tokai No.2 Power Station', Japan Nuclear Safety Institute, August 2013. http://www.genanshin.jp/english/archive/disastersitereaction/data/report_OnTk.pdf

radiation in the proximity of nuclear power plant. From a nuclear security perspective, it would not be a case of integrating security into an existing protection and crisis management framework in Japan – alongside nuclear safety – but the construction of an entirely new framework.

Genesis of Nuclear Security in Japan

At the time of the Fukushima disaster, Japan's regulatory framework already included nuclear security as an objective. The Nuclear Regulation Law contained provisions on the physical protection of nuclear materials – aligned to the IAEA's Information Circular 225 (INFCIRC 225) – and Japan had ratified the Convention on the Physical Protection of Nuclear Material (CPPNM). Yet the implementation of nuclear security as advocated by the IAEA's Nuclear Security Series was not widespread among Japanese operators; indeed, even the IAEA's Fundamentals guidance was still being deliberated by the Japanese nuclear authorities.[264] To illustrate this point, an Advisory Committee on Nuclear Security (ACNS) had been set up by the Japanese Atomic Energy Commission in 2006, and from 2007 onwards it began studying nuclear security in relation to 'international circumstances'.[265] Crucially, it was only after the Fukushima disaster of March 2011 that the ACNS issued its first formal report. Released in September 2011, the report reflected on the need to shore up nuclear security in Japan with, for the first time, explicit reference to the IAEA's Fundamentals guidance.[266]

IAEA REMEDIATION EXPERT MISSION IN FUKUSHIMA
COPYRIGHT: IAEA

264 See the IAEA's Nuclear Security Series: https://www.iaea.org/resources/nuclear-security-series
265 'Strengthening of Japan's Nuclear Security Measures', Advisory Committee on Nuclear Security, Japan Atomic Energy Commission, 9 March 2012. http://www.aec.go.jp/jicst/NC/senmon/bougo/kettei120309.pdf
266 Ibid.

The timing of this intervention was directly related to the Fukushima disaster, but it also came in the wake of the Nuclear Security Summits, a series of four state-level summits held between 2010 and 2016 which galvanised global efforts at preventing nuclear terrorism. Indeed, a key theme of the 2012 Nuclear Security Summit was the safety-security interface, stemming from international concerns about the tsunami-induced nuclear disaster at Fukushima. Japan was an active participant at the 2012 summit, featuring more than almost any other government in the 13 'Joint Commitments'.[267] A year after the Fukushima disaster, the ACNS went further by releasing a second report entitled, 'Strengthening of Japan's Nuclear Security Measures'.[268] However, the report noted that Japan was yet to implement the recommendations set out in the IAEA's NSS and set out measures to promote a more proactive approach.

Despite the ACNS's valuable intervention, however, the synergies between the safety and security aspects of the crisis were not exploited in any formal remediation channels, such as the four official investigations or the ACNS report. More progress was made after the IAEA's International Physical Protection Advisory Service (IPPAS) undertook its first mission in Japan in 2015 to review nuclear security.[269] The IPPAS mission especially focused on the implementation of physical protection measures, the regulatory framework, and computer and information security arrangements.[270] A follow-up IPPAS mission took place in 2018 which assessed Japan's implementation of the recommendations offered in the initial IPPAS mission. According to the IAEA, Japan's nuclear security regime was now 'robust and well-established, and incorporates the fundamental principles of the amended CPPNM'.[271]

However, nuclear security concerns have re-emerged more recently in Japan. In March 2021, the Nuclear Regulation Authority (NRA) announced it was suspending the restart of the No.7 reactor at the Kashiwazaki-Kariwa nuclear power plant on Japan's northern coast. According to the regulator, malfunctioning equipment for anti-terrorism measures had been identified. Weak organisational management also allowed for the possibility of intruders onto the site.[272] Nevertheless, while this development has dealt a severe blow to TEPCO which operates the plant, it at least indicates that Japan's new regulatory authority is prepared to implement tough measures to shore up nuclear security across the country.[273]

Applying Lessons Learnt from the Disaster for Nuclear Security

Unsurprisingly, the four 'official' investigations into the Fukushima disaster concluded the proximate origins lay in the earthquake and tsunami. However, all investigations acknowledged that the resultant impacts could have been avoided. It was human factors that conditioned the organisational structures underpinning the safety of Japan's nuclear complex, as well as the emergency response framework. This is not to say that Japan was uniquely vulnerable to a double natural disaster involving an earthquake and tsunami; nevertheless, human factors had allowed the country's nuclear industry to overlook critical safety measures which in hindsight could have made the accident preventable. Above all, the disaster revealed social and cultural norms were indivisible

267 Wyn Bowen, Matthew Cottee, Christopher Hobbs, Luca Lentini, Matthew Moran and Sarah Tzinieris, 'Nuclear Security Briefing Book', King's College London, 2019. https://www.kcl.ac.uk/security-studies/assets/nsbb.pdf
268 'Strengthening of Japan's Nuclear Security Measures', Advisory Committee on Nuclear Security, Japan Atomic Energy Commission, 9 March 2012. http://www.aec.go.jp/jicst/NC/senmon/bougo/kettei120309.pdf
269 'IAEA Completes Nuclear Security Review Mission in Japan', IAEA News, 27 February 2015. https://www.iaea.org/newscenter/pressreleases/iaea-completes-nuclear-security-review-mission-japan
270 Ibid.
271 'IAEA Completes Nuclear Security Advisory Mission in Japan, IAEA News, 7 December 2018.
272 'Japanese regulators say TEPCO nuclear plant prone to attack', The Independent, 18 March 2021. https://www.independent.co.uk/news/japanese-regulators-say-tepco-nuclear-plant-prone-to-attack-fukushima-japanese-tokyo-north-korea-b1818821.html
273 Ibid.

from the technical failures. And within this context, it is entirely plausible that a serious nuclear security incident could be triggered by an adversary exploiting these weaknesses, including in the aftermath of a disaster. The analysis below considers aspects of the disaster in more detail from the perspective of nuclear security.

Design Basis for Nuclear Safety

The actual mechanics of the disaster involved tsunami waves breaching a protective seawall at the Fukushima Daiichi plant. This breach was caused by a 'beyond design basis event', meaning the protections in place were not appropriately or adequately designed. The original design basis for nuclear safety at Fukushima was developed in 1966 and only allowed for a tsunami of 3.3 metres above sea level. Although the seawall was rebuilt in 2002 to a height up to 5.7 metres above sea level, following a new model produced by Japan's Society of Civil Engineers,[274] the locations of many of the emergency back-up generators remained at basement level and were vulnerable to flooding. In 2008, TEPCO produced an in-house probabilistic risk assessment (PRA) that calculated hypothetical risk for a 15.7 metre-tsunami. Given that the seawall outside Fukushima was only 5.7 metres above sea level, this scenario would indicate that urgent site adjustments were required. However, the modelling work appeared to have been considered only as an indication of possibilities, rather than as a serious warning.[275]

This aspect of the Fukushima disaster highlights that without comprehensive data and regular updating, planning assumptions cease to serve as a meaningful anchoring point for the wider protection apparatus. Just as for nuclear security, a design basis for safety can only be effective if it can be shown to withstand the range of possible threats, even including those that are low probability-high consequence events as in the Fukushima disaster. Moreover, the disaster highlighted that design criteria and interpretation of data are inherently subjective. As will be discussed in more detail, there was also an absence of regulatory oversight as the then-regulator NISA allegedly failed to review TEPCO's PRA modelling.[276] Ensuring shared understandings across all stakeholders is essential in formulating the DBT and dealing with it appropriately.

Vulnerability Assessment

Concerns about a potential terrorist or sabotage attack at nuclear power plants have tended to focus on adversaries targeting the site's reactor or nuclear fuel.[277] With nuclear security prioritised in Japan following Fukushima, there was a recognition that loss of power supply through both regular and back-up power sources was a potential security issue. These functions could potentially be targeted by an adversary – most likely an insider – to trigger a nuclear meltdown. They could also become vulnerable during a crisis due to security staff being deployed elsewhere on the site. Related to this, there was now a greater recognition of the security aspects of the plutonium 'trilemma' facing Japan, referring to concerns about the direct disposal of spent fuel and recovering plutonium from reprocessing.[278] Indeed, spent fuel and plutonium recovery remain a still unresolved political issue

274 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/
275 Scott Sagan and Edward Blandford (eds.) Learning from a Disaster: Improving Nuclear Safety and Security after Fukushima, Stanford: Stanford University Press, 2016.
276 James M. Acton and Mark Hibbs, 'Why Fukushima was Preventable', Carnegie Endowment for International Peace, 6 March 2012. https://carnegieendowment.org/2012/03/06/why-fukushima-was-preventable-pub-47361
277 For example, training utilising the IAEA's fictional nuclear facility 'Shapash' often focuses on the Protective Areas of the site, housing the nuclear reactor and nuclear fuel.
278 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/

for the Japanese government, and this only increases the risk of theft and sabotage of these materials, for instance by groups with a political agenda.

The events of Fukushima also shed light on a new security vulnerability concerning three interrelated safety functions: the loss of all forms of power supply (i.e. both regular power and back-up generators and batteries), the loss of cooling function for the nuclear reactor facility, and the loss of cooling function of spent fuel pools.[279] The locations of the spent fuel pools in the reactors' basements were also identified as a particular vulnerability. In fact, the acceptance of this vulnerability led to a reformulation of Japan's spent fuel management policy.[280] It also led to changes in the design of nuclear security systems in other countries. For example, the US National Academy of Sciences report recommended that, in the event of an attack on a nuclear plant, operators should 'measure real-time conditions in spent fuel ponds' and 'maintain adequate cooling of stored fuel'; such improvements might include 'hardened and redundant physical surveillance systems, radiation monitors, pool temperature monitors, pool water-level monitors…' etc.[281]

Vetting and Trustworthiness Checks

One of the recommendations contained in the 2012 ACNS report was establishing personnel vetting programmes in Japan.[282] Despite Japan's large civil nuclear sector, at the time of the disaster there was not yet an established vetting or trustworthiness checking system for personnel working in the nuclear sector. In fact, Japan was ranked 30th out of 32 countries with weapons-usable nuclear materials for the 'security personnel measures' category in the 2012 Nuclear Security Index, published by the Nuclear Threat Initiative (NTI).[283] Prior to Fukushima, the issue had allegedly been deliberated by NISA but no further action taken.

The ACNS report advocated implementing immediate measures to mitigate against the insider threat, including the 'two-person rule' and more thorough ID checks on personnel and their belongings. Also recommended was the introduction of a vetting system for those workers accessing strategic facilities and equipment on nuclear sites, with reference to the IAEA's INFCIRC/225 publication. However, it is reported that the Japan Federation of Bar Associations opposed the creation of any personnel reliability system amid concerns about individual privacy and human rights.[284] As a result, key tenets of best practice vetting procedures such as staff background checks were not widely implemented following the disaster, though progress has reportedly been made in recent years.

Regulatory Capture

The 2012 National Diet's report was particularly scathing about the role of the regulator in the disaster. The report lay the blame squarely on unhealthy relations between the key nuclear stakeholders in Japan, concluding: 'The TEPCO Fukushima Nuclear Power Plant accident was the result of collusion between the government, the regulators and TEPCO, and the lack of governance by said parties….We believe that the root causes were the organizational and regulatory systems that

279 'Strengthening of Japan's Nuclear Security Measures', Japan Atomic Energy Commission, Advisory Committee on Nuclear Security, 9 March 2012. http://www.aec.go.jp/jicst/NC/senmon/bougo/kettei120309.pdf
280 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/
281 '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
282 'Strengthening of Japan's Nuclear Security Measures', Advisory Committee on Nuclear Security, Japan Atomic Energy Commission, 9 March 2012. http://www.aec.go.jp/jicst/NC/senmon/bougo/kettei120309.pdf
283 2012 Nuclear Security Index, Nuclear Threat Initiative (NTI), January 2012. https://www.ntiindex.org/archive
284 Scott Sagan and Edward Blandford (eds.) Learning from a Disaster: Improving Nuclear Safety and Security after Fukushima, Stanford: Stanford University Press, 2016

supported faulty rationales for decisions and actions'.[285] This situation is often labelled 'regulatory capture', referring to the corruption of authority when regulating agencies are co-opted to serve the interests of a minority constituency – in this case the powerful nuclear power industry.[286]

Avoiding regulatory capture in the nuclear industry is a perennial problem across the world. Nuclear regulators require staff to possess specialised knowledge of nuclear technology and equipment, which tends to be gained from first-hand practical experience working in industry. The consequence of this specialisation prerequisite is a narrow pool of appropriately trained workers to draw from, often leading to staff switching between employment at nuclear facilities and the relevant regulator in the same country. In their critique of Japan's regulatory system, Charles Ferguson and Mark Jansson refer to Japan's 'nuclear village'.[287] They draw attention in particular to the role of the Ministry of Economy, Trade and Industry (METI), which at the time of the disaster was responsible for advancing nuclear power in Japan. The authors observe that the main regulating body NISA was under the authority of the Agency for Natural Resources and Energy (ANRE), which itself was based in METI. The strict and traditional organisational hierarchy within METI meant there was a conflict of interest when senior officials interacted with NISA further down the hierarchy.[288]

Another weakness that contributed to the disaster was the overlapping structures within Japan's regulatory system. The Nuclear Safety Commission (NSC), largely responsible for developing new safety regulations, had been established only as an advisory body and lacked the authority to ensure that NISA implemented new regulations. In parallel, the NSC supported NISA in investigating safety incidents and breaches. Faced with a mounting backlog of investigations, both agencies were unable to devote resources to preventative activities, such as promoting new regulations or engaging with emerging best practices from other parts of the world.[289]

The defanging of Japan's regulating agencies ultimately resulted in sub-standard and weakly-enforced rules on nuclear safety and security at the time of the disaster. Lack of independence also resulted in regulatory system being ineffective. For example, revised information about tsunamis exceeding previous assumptions and about risks from the destruction of a seawater cooling system had apparently been shared between regulatory and TEPCO officials, but not acted upon.[290] In essence, Japan's regulatory authorities suffered from impotence on two fronts: being overruled by powerful industry interests in terms of improvements in safety and security standards; and being overwhelmed by safety incidents and non-compliance, which fed into a vicious cycle of focusing on past events. Ultimately this prevented the regulatory authorities from developing structural and regulatory changes that might improve industry-wide standards and adherence.[291]

Creating Redundancy and Flexibility in Protection Strategies

One of the recommendations contained in the US National Academy Report was the expansion of the nuclear industry's 'diverse and flexible coping strategies (FLEX) capability' in order to respond

285 National Diet of Japan, The Official Report of The Fukushima Nuclear Accident Independent Investigation Commission, 2012. https://www.nirs.org/wp-content/uploads/fukushima/naiic_report.pdf
286 For example, see Charles D. Ferguson and Mark Jansson, 'Regulating Japanese Nuclear Power in the Wake of the Fukushima Daiichi Accident', Federation of American Scientists, FAS Issue Brief, May 2013. https://fas.org/wp-content/uploads/2013/05/Regulating_Japanese_Nuclear_13May131.pdf
287 Ibid.
288 Ibid.
289 Ibid.
290 Scott Sagan and Edward Blandford (eds.) Learning from a Disaster: Improving Nuclear Safety and Security after Fukushima, Stanford: Stanford University Press, 2016
291 Ibid.

effectively to a crisis.[292] The report advocated both the upgrading of security infrastructure and systems and the training of security personnel to cope with extreme external events. This emphasised creating 'redundancy' in physical protection systems, such as independent and protected electric power sources. The report also recommended developing 'diverse and flexible approaches' in terms of how a plant might reconstitute security infrastructure and staffing during and following the acute phase of a crisis.[293] Embedding redundancy and flexibility in security systems ultimately helps develop the resilience of an organisation to deal with any eventuality.

Lessons can also be gleaned from the cases of Onagawa and Daini. First, having a well-trained and effective senior leadership team at a nuclear plant can mean the difference between, on the one hand, a natural disaster being contained and, on the other, a catastrophe arising. At Onagawa, despite the absence of the site superintendent, the workforce responded effectively due to emergency exercises being conducted regularly in the past.[294] Second, establishing and maintaining communications were central to the responses at both the Daini and Onagawa facilities. For example, resilient back-up communication systems like non-digital communications equipment helped prevent lapses in reliable information-sharing. This saved the operators time and effort in delivering messages between response centres and sites when regular communication systems such as mobile phones were out of action (in contrast to the events at Fukushima Daiichi). Third, incorporating additional access control support into emergency response plans was crucial because the recovery after the crisis involved unfamiliar workers, including contractors, some of whom lacked the regular authorisation to enter a facility.

Cultivating an Effective Nuclear Security Culture

While the Fukushima disaster was inherently a safety incident, the crisis revealed broader weaknesses in organisational culture endemic across the Japanese nuclear industry, from which lessons can be extrapolated for nuclear security. In particular, the crisis highlighted the importance of effective communication, leadership and governance when organisations face an extreme event. As discussed in the introduction to this handbook, these qualities are fundamental to building resilience within nuclear organisations, which in turn enhances their ability to respond and adapt to extreme and unexpected events. The way that the Fukushima disaster unfolded highlights how technical failures can be rooted in human factors, in terms of organisational resistance in anticipating a crisis – or even accepting a threat exists – and in terms of an inadequate crisis management response that enables a disaster to spiral out of control.

It is useful to refer back to the IAEA's guidance on security and safety culture, derived from Edgar Schein's work on organisational culture.[295] At every stage of the Fukushima disaster, these fundamental building blocks for organisational culture appear to have been absent or degraded. Most notably, the belief that a credible threat exists – a sub-conscious and intangible characteristic in the IAEA's security culture model[296] – was not widely recognised across Japan's nuclear village. Stakeholders tended to avoid acknowledging the safety risks associated with nuclear power, to the extent that a 'myth of absolute safety' prevailed.[297] It can be argued that there was equally a 'myth of

292 '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
293 Ibid.
294 'Responses to the Tohoku-Pacific Ocean Earthquake and Tsunami at the Onagawa Nuclear Power Station and Tokai No.2 Power Station', Japan Nuclear Safety Institute, August 2013. http://www.genanshin.jp/english/archive/disastersitereaction/data/report_OnTk.pdf
295 Edgar Schein, Organisational Culture and Leadership 4th ed. (2010, Jossey-Bass), p.18
296 Nuclear Security Culture: Implementing Guide, International Atomic Energy Agency, IAEA Nuclear Security Series, No.7, 2008. https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1347_web.pdf
297 Scott Sagan and Edward Blandford (eds.) Learning from a Disaster: Improving Nuclear Safety and Security after Fukushima, Stanford: Stanford University Press, 2016

absolute security' at the time of the Fukushima disaster, underscored by the lack of efforts made to secure nuclear materials or monitor site access as the crisis unfolded, the inadequacy of pre-existing vetting procedures, an absence of back-up communication systems, and so on.

These beliefs ultimately led to a failure to challenge basic assumptions around threats, design basis and vulnerabilities. Powerful vested interests, in the form of energy companies, were strongly influential in shaping regulation, not least as these organisations often possessed more technical knowledge than their counterparts at the main regulating body NISA. Hindsight cannot say with certainty that the accident would have been averted, but alleged reluctance in considering new counter-measures against tsunamis highlights how human factors contributed to the crisis. One academic study of the Fukushima disaster uses a groupthink model to explain the underestimation of the tsunami risk despite obvious risks being known, which led to a 'procrastination of problem solving'.[298] Likewise, groupthink helps explain the lack of progress during this period in progressing the implementation of nuclear security across Japan's nuclear estate, despite the Japanese government actively participating in global fora such as the Nuclear Security Summits and being a signatory of the CPPNM.

The mid-level of the IAEA's pyramid model contains 'principles for guiding decisions and behaviours'. Here again, the Fukushima disaster highlighted an absence of key IAEA characteristics: 'professionalism and competence', 'commitment and responsibility' and 'learning and improvement'. Despite nuclear disasters in other parts of the word acting as precursors, the Japanese nuclear complex had not implemented lessons learnt from these incidents, notwithstanding urging from the IAEA and World Association of Nuclear Operators (WANO). The Independent Investigation Commission, one of the four key reports of the Fukushima disaster, labelled the lack of interest in absorbing historical lessons as 'Galapagos syndrome' to convey the isolation of Japan's regulatory regime.[299] Without the opportunity for self-reflection, for instance by engaging with the international nuclear community, Japanese duty-holders and regulatory authorities failed to develop essential behaviours for improvement amongst the workforce such as learning, professionalism, motivation and responsibility, which ultimately led to a lack of resilience when faced with a similar scaled crisis.

At the top of the IAEA's pyramid model are leadership and management systems. Ultimately these characteristics proved to be inadequate to contain the Fukushima disaster – both at the facility level and the government level. As discussed, the response from the nuclear operator was slow, there was a breakdown in incident command chain, personnel were inadequately trained for the crisis management tasks, and insufficient resources were deployed to the scene. As highlighted by the 2012 National Diet's report, poor decision-making was constantly re-validated by a reflexive deference to leadership and refusal to scrutinise past failures.[300] Closely related to leadership in the IAEA model is the role of communications. The weaknesses in the response to the Fukushima disaster were significantly worsened by the confusion around the chain of command. Once the magnitude of the disaster emerged, Japan's top political leadership became closely engaged but communication between the government and TEPCO had already fallen apart at a critical time.

298 Ryota Matsui, 'Groupthink Trap: A study on the essence of failure in the Fukushima nuclear accident', Transactions of the Academic Association for Organizational Science, 2017, Vo.6 Issue 2. https://www.jstage.jst.go.jp/article/taaos/6/2/6_14/_article/-char/en

299 Independent Investigation Commission on the Fukushima Daiichi Nuclear Accident, 28 February 2012. https://apinitiative.org/en/project/fukushima (also see Routledge edition in English published on 6 March 2014)

300 National Diet of Japan, The Official Report of The Fukushima Nuclear Accident Independent Investigation Commission, 2012. https://www.nirs.org/wp-content/uploads/fukushima/naiic_report.pdf

Concluding Thoughts

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. And this shift in attitudes enabled safety's close cousin, nuclear security, to gain more traction across the Japanese nuclear enterprise and beyond. 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.[301] 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.

The legacy of the Fukushima disaster therefore goes beyond nuclear safety and nuclear security to extend to other kinds of unconventional security challenges. The work of Scott Sagan and Edward Blandford on the Fukushima disaster has emphasised the importance of absorbing lessons learnt from previous incidents in order to avert future disasters.[302] They refer to this as 'vicarious learning', the process of learning through others' experiences without the opportunity costs involved. It appears that even today not all lessons from the Fukushima crisis, particularly in the area of nuclear security, have been adequately absorbed, although this is not a problem unique to Japan. Far too often security incidents are not disclosed to the IAEA and wider international community out of concerns about reputational damage to a country's nuclear industry.

301 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/

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

Conclusion

The Covid-19 pandemic has been a challenging time for the nuclear industry, as it has for practically every type of organisation. While significant steps have been taken to controlling the crisis – particularly through the deployment of vaccines – there still remains great uncertainty about its full impact and how long the situation will endure. This handbook has sought to consider nuclear security in times of crisis, exploring cases from the recent past in order to extract lessons for current and future crises. Employing a broad definition of a 'crisis' – high-stakes events presenting challenge urgency and surprise – has allowed a range of case studies to be included – featuring political, economic or societal turmoil, natural disasters or other major unforeseen events.

Although they rarely receive attention, crises are not unprecedented in nuclear operations. As shown by the case studies explored in this handbook, nuclear operators often have to adapt. This adaptation could be necessary in the face of natural disasters, whether the rapid onset of the Cerro Grande fire in New Mexico or the effects of the 2011 earthquake and tsunami in Japan. Political crises can also precipitate the need for adaptation, such as in the case of the dissolution of the Soviet Union, or the heightened concerns of terrorist attacks in Belgium. 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.

An adversary could take advantage of security weaknesses during a crisis or even initiate a crisis as part of a more elaborate attack. In each of the preceding case studies, operators, regulators, and governments faced crises that tested the resilience of their nuclear security systems. While many of these case studies contained stories of heroism in the face of existential threats, they also demonstrated how institutional decisions made years earlier can impact an organisation's ability to maintain strong and sustainable security. The crises explored above have yielded a number of lessons for nuclear security.

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.

Beyond the crisis generated by the Covid-19 pandemic, nuclear operators, regulators and government agencies need to prepare for future crises – whether these are political, social or economic in nature, or stem from future natural disasters. Given the locations of nuclear facilities around the world, climate change is likely to ensure that more such crises – whether natural or human resulting from secondary effects – emerge over the coming decades. The authors hope that the case studies explored here will be of use to operators, regulators and governments, and inspire more researchers to consider how nuclear security can be maintained during future crises.

Centre for Science and Security Studies
Department of War Studies
King's College London
Strand
London WC2R 2LS
United Kingdom

www.kcl.ac.uk/csss
@KCL_CSSS