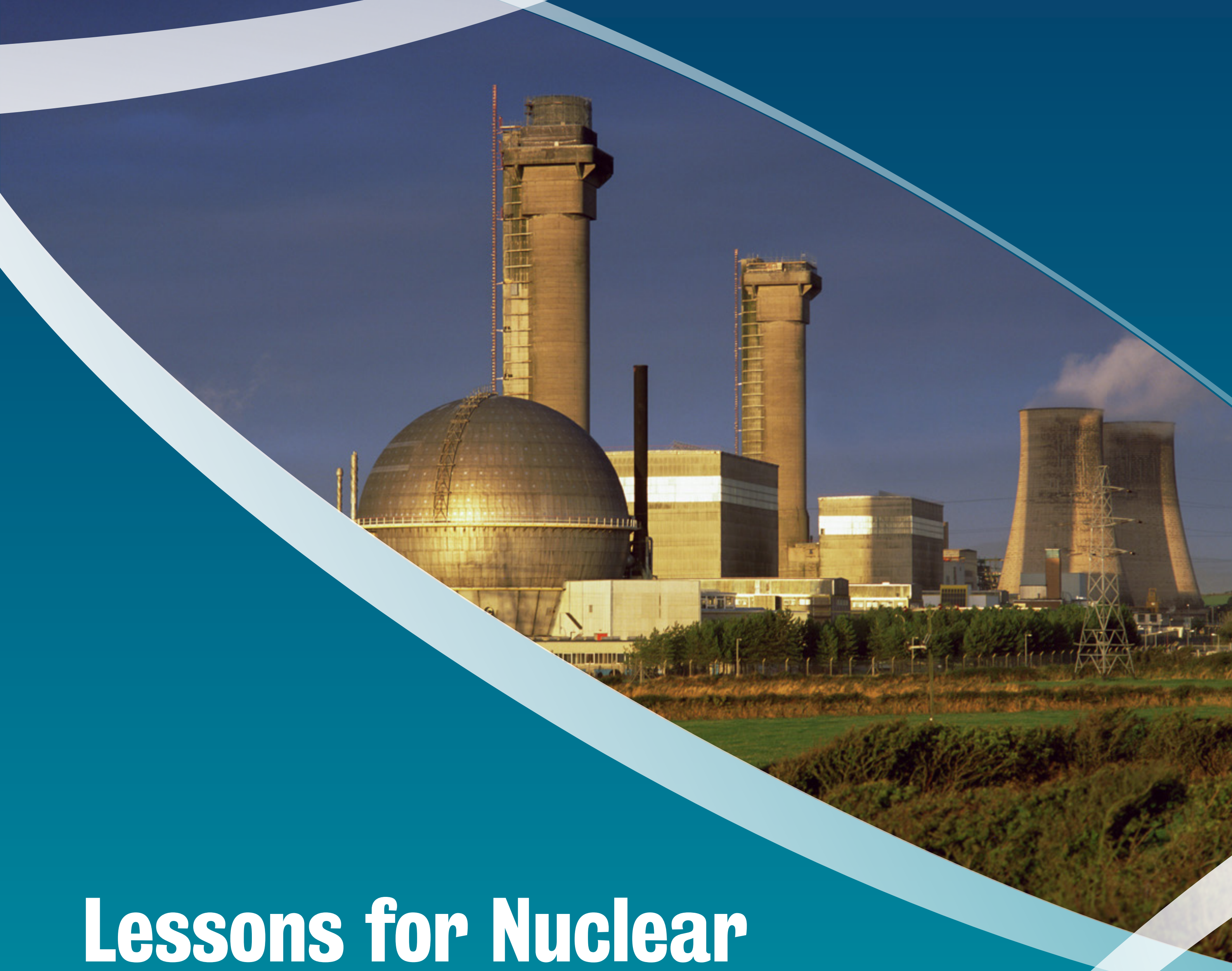
CENTRE FOR SCIENCE
& SECURITY STUDIES

KING'S College LONDON



Lessons for Nuclear Security from the UK's Response to Covid-19

Dr Sarah Tzinieris, George Foster (Amport Risk Limited)
and Professor Christopher Hobbs

2022

Contents

Commonly Used Abbreviations

BEIS	UK Department for Business, Energy and Industrial Strategy
CNC	Civil Nuclear Constabulary
Covid-19	Coronavirus Disease 2019
CPNI	UK Centre for the Protection of National Infrastructure
CPPNM	Convention on the Physical Protection of Nuclear Material
DBT	Design Basis Threat
EIMT	Examination, Inspection, Maintenance and Testing
IAEA	International Atomic Energy Agency
INTERPOL	International Criminal Police Organization
INFCIRC	Information Circular of the IAEA
NDA	Nuclear Decommissioning Authority
NHS	National Health Service
NIMCA	Nuclear Industries Malicious Capabilities (Planning) Assumptions
NSCP	Nuclear Security Culture Programme, led by King's College London
NSS	Nuclear Security Series of the IAEA
ONR	UK Office for Nuclear Regulation
PPE	Personal Protective Equipment
RAG	Red, Amber, Green
SSP	Site Security Plan
SyAPs	Security Assessment Principles
TSP	Temporary Security Plan

Acknowledgements

This policy brief was developed through the UK's Nuclear Security Culture Programme (NSCP), implemented by a King's College London academia-industry consortium and sponsored by the UK Department for Business, Energy and Industrial Strategy (BEIS). The authors are grateful for the support provided by BEIS under this programme and to the interviewees from UK government and industry, who included representatives from BEIS, the Office for Nuclear Regulation (ONR), the Nuclear Decommissioning Authority (NDA), the Civil Nuclear Constabulary (CNC), Nuclear Transport Solutions, and various nuclear operators. Thanks also to Madeleine Ryan, Sally Horspool and Amelie Stoetzel for their help in producing the brief.

Executive Summary

The Covid-19 pandemic has complicated nuclear operations around the world including the implementation of nuclear security. While the pandemic's impact and responses to it have varied from country to country, there exist common challenges faced by the nuclear sector. These include an increase in worker absenteeism due to infections and enforced isolation, restrictions on onsite numbers and the proximity of staff to minimise the risk of transmission, a large-scale transition to remote working and disruption to key supply chains. This policy brief seeks to explore the impact of these and other challenges faced by the UK nuclear sector, examining how they have affected the delivery of security and the efficacy of new measures put in place to mitigate potential risks.

It is also important to recognise that despite the unique nature of the Covid-19 pandemic – in terms of its global scale, extended duration and direct effect on humans – responses have nevertheless been informed and shaped by past events and systems for crisis management.[1] Governments and organisations have sought to develop strategies for both anticipating future crises and mitigating their impact. These broader approaches are also discussed in this brief as they provide a useful framework against which efforts to adapt nuclear security arrangements in response to Covid-19 should be considered.

Although countries deploy different national nuclear security systems, it is hoped that lessons learnt from the UK's experience in maintaining nuclear security following the onset of Covid-19 will be relevant for others in managing the impact of the pandemic, as well as preparing for future crises. To this end, efforts have been made to highlight key lessons that are likely to have broader applicability throughout an extreme event, as summarised below:

- Governments are likely to expand their information gathering requirements during a crisis, in an effort to understand its impact and assess emerging risks. In response to the onset of Covid-19, the Office for Nuclear Regulation (ONR) worked with operators to gather information across the UK's nuclear estate so that potentially concerning trends could be proactively identified and action taken, for example, any degradation of security. In conducting this type of effort, care should be taken to streamline information gathering exercises in order to reduce the burden on operators, by focusing on what data is most relevant for centralised decision-making.

- Organisational risk registers should be frequently reviewed to take into account emerging threats and vulnerabilities, and linked to national risk registers. In the context of Covid-19, relatively few UK nuclear operators had a pandemic scenario within their top-10 risks, despite its clear prominence as a high-probability high-consequence event in the UK's national risk register.

- Well-established risk management systems at the organisational level are essential for mitigating the effects of a range of crises. Although the UK nuclear industry had not developed or exercised an in-depth pandemic plan, decades of experience of broader contingency planning and consequence management was drawn upon following the onset of Covid-19. This approach enabled rapid and informed decision-making as organisations adjusted to the crisis.

- The UK nuclear regulator's outcomes-focused approach, which places the responsibility on the operator to design security solutions to manage risks, provided what was deemed a helpful level of autonomy and flexibility to modify arrangements at sites to meet their specific operational requirements, at a time when decisive action was essential.

- A considerable portion of planned regulatory inspections by ONR were moved online to reduce Covid-19 transmission. Greater

emphasis was placed on desk-based assessments, utilising data gathered from organisations' internal assurance processes and online engagement. This was observed to provide useful efficiencies and consequently, even as the effects of the pandemic decrease, a significant proportion of security assessment work will likely continue to take place online, with site visits focused on organisations which require more intervention and where ONR can add greatest value.

- Challenges have been encountered in ensuring the security of sensitive nuclear information across the supply chain. Here, physical access to suppliers has been limited by Covid-19 restrictions, making it difficult for operators to fulfil their legal obligation to provide independent assurance that security expectations for the protection of sensitive nuclear information are being met.
- A large proportion of the UK nuclear workforce has worked from home to reduce disease transmission, which involved transitioning employees to remote working arrangements at very short notice. While this initially placed a significant burden on nuclear organisations, once this process was consolidated operators reported significant efficiencies in the widespread use of digital platforms for routine activities, such as training, vetting and meetings.
- With large numbers of employees working remotely, greater emphasis has been placed on cyber security measures during the pandemic and heightening awareness among staff of potential security risks in relation to information management and digital communications.
- The pandemic and the experience of lockdowns have affected morale across all workforces, and not just in the nuclear industry. With large numbers of staff based at home, nuclear employers have needed to develop new approaches to protect the wellbeing of staff. A greater focus on staff wellbeing may also have helped mitigate against the insider threat.
- The significant reduction in workers at nuclear sites has mitigated some aspects of physical protection risks owing to reduced footfall, particularly those related to an active insider. However, as staff return to site, their understanding of these risks may have lessened – and it is important for operators to raise awareness among the broader workforce, not just those with direct responsibility for nuclear security.

Research Approach

This study provides new empirical research on how key UK civil nuclear stakeholders have responded to the challenges posed by Covid-19, with a focus on the organisational level. Insights were gleaned from semi-structured interviews with practitioners from eight different UK nuclear organisations spanning government, the regulator, transport, nuclear research and energy production, all with direct responsibility for nuclear security. The interviews were conducted over a period of six months from early- to mid-2021, with interviewees asked about both their organisation's initial response to the pandemic and how this has evolved over time. Analysis is supported by a review of crisis preparation and management practices, drawing on the academic literature on resilience and crisis management. Reference is also made to key international nuclear security treaties and guidance documents, such as the International Atomic Energy Agency's (IAEA) Nuclear Security Series.[2]

Part I of this brief discusses in a general sense how to prepare for and manage crises through building resilience in nuclear organisations. It provides information on national and regulatory approaches, risk management and contingency planning, stakeholder engagement and security culture.

Part II then considers these and other approaches in the context of the Covid-19 pandemic, examining the UK's response. The findings of this research are not intended to be exhaustive. They may also not apply in all contexts, given how nuclear security remains the responsibility of states, which often take different approaches to its implementation at the national level. Nevertheless, given the overarching international legal requirements and common operating principles that serve to inform and shape the design of nuclear security systems, we anticipate many of the lessons identified in the brief will be relevant for others.

Part I
Nuclear Security Considerations in Preparing for and Managing Crises

1.1 Crises and Organisational Resilience

A crisis is commonly defined as an event which threatens high priority values of an organisation, presents a restricted amount of time in which a response can be made, and is unexpected or unanticipated.[3] Crises tend to destabilise a system as a whole and threaten basic assumptions, creating challenges that may not be alleviated by prescriptive or pre-planned responses.[4] They also tend to be complex and inherently uncertain, but require quick decision-making based on often incomplete or ambiguous information.[5] Crises can present a challenge to nuclear security, safety and broader operations as they may necessitate, at the site level, changes to standard operating protocols at short notice. This is without the necessary time, for example, to fully evaluate how these adaptions may impact on the delivery of security.

In combating crises, organisations are increasingly focused on the concept of 'resilience' – the ability to withstand adversity and bounce back quickly from either an internal or external shock.[6] To achieve resilience, organisations have developed a range of approaches aimed at preparing for and responding to crises. These include assessing changing threats and vulnerabilities, contingency planning and consequence management, strategies for engagement and communication, and organisational culture. Such approaches are typically underpinned by risk-informed decision-making where the likelihood and consequence of different scenarios are carefully evaluated.[7] The following sub-sections discuss these key methods in relation to nuclear security.

1.2 Evolving Threats and Vulnerabilities during a Crisis

Physical protection should be based on a state's current evaluation of the threat [Fundamental Principle G of INFCIRC/225/Rev.5][8]. In the predictive, or consequential, light of a crisis, national and local governments may decide to make alterations to overarching policies. For example, revised intelligence on threats to nuclear facilities and their assets can prompt a change in the National Nuclear Security Threat Assessment or Design Basis Threat (DBT). Conversely, it may be determined that that the crisis has not triggered a significant change to the threat profile and current security arrangements remain appropriate. If it is determined that changes should be made, typically these will be applied through state-level regulatory frameworks for nuclear security. In extreme circumstances, such as 'beyond DBT' scenarios such as state-on-state hostile activity or serious social and political disorder, existing security arrangements may break down and governments may need to intervene.

Nevertheless, in most crises the national competent authority will be expected to continue its mission to regulate [Fundamental Principle D of INFCIRC/225/Rev.5][9] and assure the security of nuclear and radioactive materials and assets, though how it implements its roles and responsibilities may change. For example, if its visibility of nuclear security delivery is restricted, an adjustment to the way in which regulation is exercised may be necessary. In these circumstances it will be the responsibility of the regulator to determine methods and mechanisms which allow for an adequate assessment of nuclear security. Indeed, during a crisis the characteristics of a site may change, and at short notice – with consequential impacts on the ability of regulators to access site security arrangements. For example, a severe weather event or seismic activity may restrict mobility on a site, although this is likely to be temporary. Similarly, a pandemic may restrict access but potentially for a prolonged duration. This may require a modified methodology for regulation; the regulator might rely more on remote and alternative assurance through the provision of information-driven evidence of a licensee's claims or the use of modelling and simulation rather than more conventional exercising and testing. Naturally, rapid modifications to the regulatory process pose potential risks and, as such, these should be carefully considered with close coordination between the regulator and the operator.

Equally, the nature of a crisis means that an unexpected and sudden turn of events might occur before a state authority is able to revise the DBT, placing the onus on nuclear organisations to adjust their own threat assessments under time pressure. While a crisis is more likely to lead to an increase – rather than a decrease – in the threats posed to nuclear assets, this is not always the case. During the Covid-19 pandemic, reduced mobility across state borders and within states, together with fewer staff working on nuclear sites, has conceivably reduced the probability of a transnational terrorist attack occurring.

However, the situation tends to be more complex than a simple evaluation of the threat being increased or decreased. Even if the underlying threat is judged to be unchanged, the crisis may still have served to alter risks due to changes in operational norms and ways of working.[10] For instance, while lower footfall on nuclear sites may reduce the risk of an active insider, the transition in large numbers of staff to remote working may at the same time increase the risk of a cyber or information security compromise. With large numbers of staff working remotely, vulnerabilities may also be more diffuse and difficult to identify – and thus protect against. In this context, the management of remote employees is significantly more complicated and may only extend to monitoring their digital activity. As such, nuclear organisations must consider all aspects of the threat environment when making an assessment during a crisis.[11]

In some cases, remote working may lead to irregular working hours and staff accessing systems via non-approved devices.[12] Furthermore, reduced in-person interaction between workers can serve to undermine observational systems in place that help identify potential insider threats. This risk may be compounded by the potential adverse impacts of self-isolation or health and wellbeing issues associated with a prolonged crisis. Vulnerabilities may also occur due to changes in the maintenance and testing of physical security systems. For example, fewer onsite workers as a result of Covid-19 might mean that maintenance and testing activities have to be scaled back. While alternative measures or even postponement may provide adequate assurance temporarily, the efficacy of these arrangements may be called into question in the longer term.

1.3 Risk-Informed Approaches

A Hypothetical Example of a Security Risk Register

Date Entered/ Reference Number	Risk Description	Security Categorisation	Existing Controls	Impact	Probability	Mitigation	Priority (PRI)	Cost (approx)	Treatment
30 Aug 21 R-S-00313	Compromise of site access control measures	Physical Security – Automated access control system	Existing site access chip and PIN readers do not have multi factor authentication and are subject to an unacceptably high false alarm rate (FAR)	Possible unauthorised entry by a malicious intruder	Possible 60%	Determine reasons for high FAR	1/5	£10,000	Action by 31 December 21 security contingency fund
						Renegotiate contract delivery to rectify possible installation faults	1/5	Nil Work/time costs only	Action with FAR study
						Engage alternative solution	3/5	£20,000	Budget for next financial year. Carry into security improvement schedule

Source: George Foster, Amport Risk Ltd

In evaluating the impact of changes to threats and vulnerabilities that may be precipitated by a crisis and developing security solutions, the same risk-informed approach applicable in normal operations should be followed. In simple terms, a risk-informed approach is concerned with the optimisation of resources in the implementation and delivery of nuclear security, based on continuous assessment of the risk environment. Adopting such an approach is likely to be essential in a crisis when an organisation faces an extreme event and is required to respond decisively and often with limited information. As observed by the IAEA, a risk-informed approach can ‘help a State to allocate its resources more effectively and efficiently by systematically considering the threats and risks’.[13] Outlined below is a brief description of some of the key components of this approach to nuclear security.

i. **Risk Management** is a business process that involves the identification, evaluation, analysis, treatment and monitoring of risk. If overall risk is evaluated to be too high, it must be mitigated by introducing countermeasures. Risk management in nuclear security involves processes such as critical asset and Vital Area Identification, Threat Assessment, risk reduction treatment and risk audits.[14] These are utilised to ensure that security arrangements on nuclear sites are proportionate, appropriate and affordable. Here it is unreasonable to expect to achieve a risk level equal to zero and therefore nuclear organisations need to define which level of risk they consider acceptable – their ‘risk appetite’. Nuclear organisations are encouraged to develop and apply risk management frameworks specific to their site(s), supply chain and broader operations.

ii. **Risk Registers** perform a key role in preparing for crises, through recording the details of potential future risks and associated mitigating measures and budgeting. A risk register is not designed to contain an exhaustive list of risks, but instead identifies the most important ones based on their probability of occurring and expected severity. Alongside each risk contained in the register, there is analysis of what the risk means for an organisation’s nuclear assets, alongside detailed plans for how those risks will be treated and mitigated. However, it is intrinsically challenging to assess the probability of risks occurring or identify all possible risks. Here it is essential that nuclear organisations avoid the tendency to populate risk registers with only conventional scenarios. This was demonstrated by the Fukushima Daiichi disaster, where the failure to consider the risks of disruption to both regular and back-up cooling systems was partly to blame for the crisis that enveloped the plant in March 2011.[15] While no risk register will ever capture the full range of possible risks, nuclear organisations should reappraise their registers regularly to ensure they reflect the evolving threat environment.

iii. **Quality assurance** involves the examination, inspection, maintenance and testing of security systems to gain confidence in their effectiveness reviewed against the threat, while meeting national regulations [Fundamental Principle J of INFCIRC/225/Rev.5][16]. It can be argued that 'assuring quality' is the most valuable aspect of risk management as it offers confidence that physical protection requirements are being implemented correctly – and consequently failures, mistakes and deficiencies will be avoided. As stated in the Convention of the Physical Protection of Nuclear Material (CPPNM), 'a quality assurance policy and quality assurance programmes should be established and implemented with a view to providing confidence that specified requirements for all activities important to physical protection are satisfied.'[17] Here there is emphasis on the importance of rigorous inspection and testing of physical protection systems, which can support the development of resilience in advance of a crisis.

iv. **Minimum thresholds** are essential for sustaining security operations. It is important to evaluate minimum thresholds so that security measures and resources can be appropriately allocated across the business. Typically, during normal operations security will be implemented at higher levels than these thresholds, thereby reducing risk levels. However, during times of crisis, a prior, agreed, minimal operational security threshold can be useful as organisations may wish to 'flex' their response. Here security assets may be prioritised to areas of greatest vulnerability – allocating resources from elsewhere but ensuring that minimum thresholds are maintained.

1.4 Operational Management of Crises

Despite efforts to manage risk through the aforementioned approaches, crises and other significant events will require nuclear organisations to rapidly respond and consequently it's also essential for organisations to develop plans to this end. Typically, focus will be placed on the following key stages:

i. **Contingency planning** is how organisations prepare to respond to an unexpected or sudden event which may trigger a crisis [Fundamental Principle K of INFCIRC/225/Rev.5].[18] The nature of the contingency plan will be influenced by the determination of risk, the consequences of the risk, the risk appetite of an organisation and a cost-benefit analysis. Contingency planning can range from a very basic approach involving a 'skeleton' plan based upon planning assumptions and established organisational structures, to more comprehensive and detailed preparation, with specific objectives, tasks, roles and responsibilities which are tested, exercised and validated. Here emphasis and the approach taken will be based upon an assessment of the likelihood of different risks and their potential impact.

ii. **Consequence management** involves the enaction of specific measures to mitigate the key impacts of an evolving crisis.[19] Due to the difficulties in planning for all the consequences of a crisis, nuclear organisations can utilise existing plans and adapt these either predictively or in response to events as they unfold. This may, for instance, require modifications to aspects of its design and the implementation of new ad-hoc structures, resources, roles and responsibilities. Effective management of the crisis will be aided where an organisation prioritises its ability to maintain essential outputs and create the conditions for a timely and efficient return to normal operations.

iii. **Recovery** is the phase of a crisis where a nuclear organisation returns to business as usual, with operations potentially revised in the light of the crisis experience.[20] This might mean concurrent planning during the consequence management phase, to ensure a smooth transition from management of the crisis back to normal operations. For example, there may be a gradual reduction of risk-managed temporary security plans that were put in place during the crisis and a return to normal regulatory scrutiny involving the revival of inspection activity that was postponed or cancelled. Here the nuclear operator and regulator will need to agree prioritised requirements, objectives, deliverables and scheduling. In addition, attention should be given to identifying key lessons from the crisis response, including what approaches worked well and which were less effective, and any potential efficiencies or process improvements identified through adopting new ways of working that should be maintained. This will inform responses to future crises, and may also result in the modification of previous business-as-usual working practices.

1.5 Stakeholder Engagement and Communication

At the onset of a crisis, there are likely to be high levels of uncertainty and ambiguity, which will only reduce with more accurate information and assessment as this emerges over time. While confronting the crisis will be their top priority, nuclear operators also need to maintain communication with key stakeholders external to their organisation and provide regular updates.[21] It is a common feature of crises of any nature that the volume and frequency of the reporting of the nuclear organisation's data, statistics and analysis will be increased – often at the request of government agencies, the regulator and the organisation's senior leadership and board.[22] Furthermore, meetings and general communications are likely to expand between the organisation and these key stakeholder groups. This will significantly add volume and complexity to information management and exchange, at least in the early period of a crisis.

Nuclear organisations may also face conflicting requirements for information gathering and reporting from different stakeholder groups. Management of this reporting and communications activity requires careful coordination to ensure coherence and accuracy in the data, while also maintaining a manageable schedule, and this may necessitate the deployment of additional resources to the activity. Prior recognition of the additional reporting and communication demands triggered by a crisis can enable nuclear organisations to plan for, and accommodate, external demands. As discussed previously, the recovery phase of a crisis will lead to some response-driven activities being concluded as the organisation moves from the initial response phase back to business as usual. It is important for both the nuclear organisations and senior stakeholder groups to recognise when additional reporting and communication activities no longer serve their purpose and can be safely ended.

1.6 Security Culture

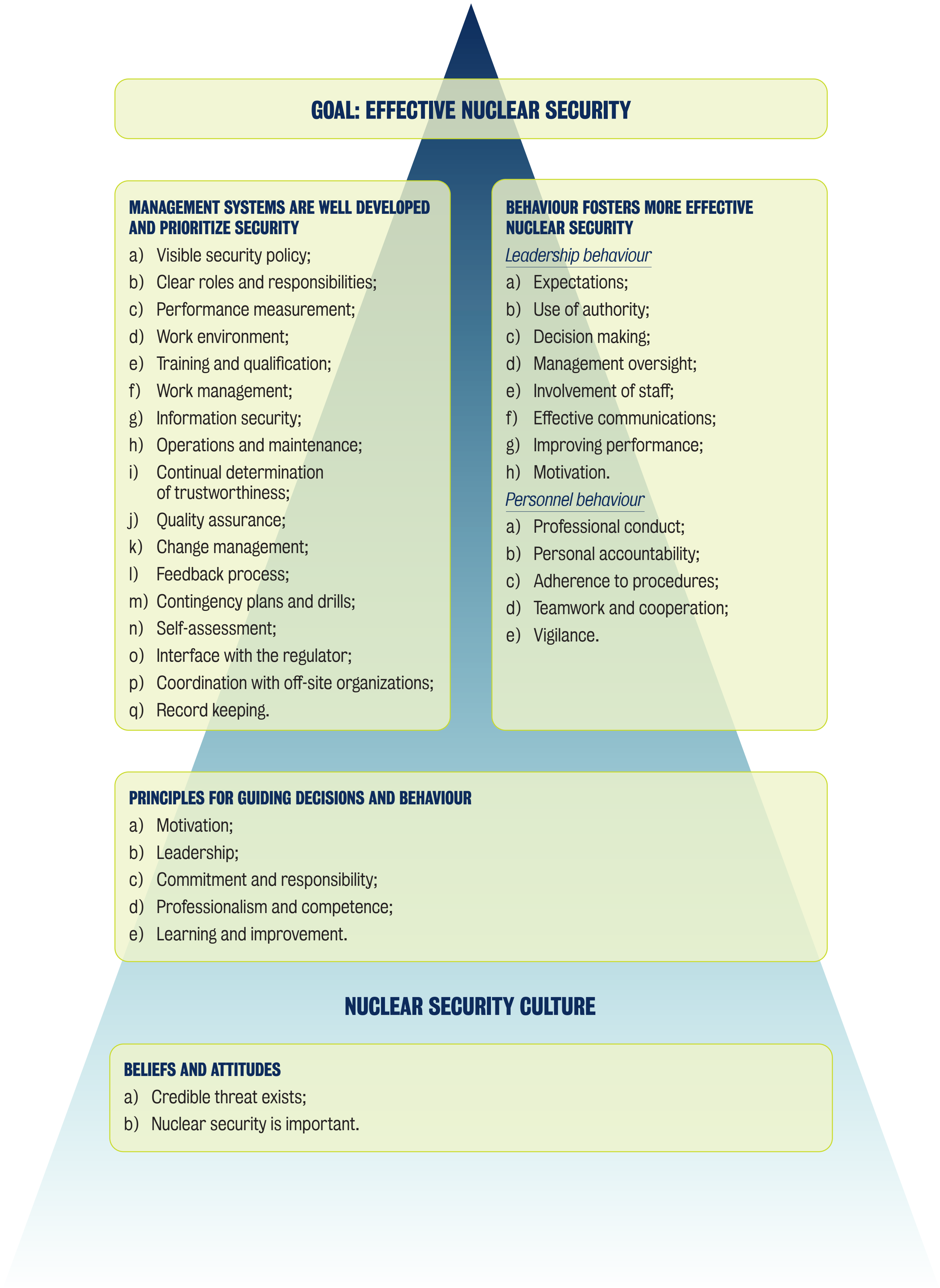
All organisations involved in the protection of nuclear materials should give due priority to security culture [Fundamental Principle F of INFCIRC/225/Rev.5][23]. While the proximate causes of crises may be technical malfunctions or natural phenomena such as earthquakes and wildfires, it is *human factors* that underpin the security of nuclear and radiological materials. During a crisis, the strength of an organisation's security culture will be an important factor in how effectively it is able to mitigate the impacts of an extreme event, as well as the success of the recovery process. Often with very short lead-in times and lacking accurate information, workers will need to respond to dramatic events that fundamentally change working conditions and organisational structures, while sustaining a robust security regime.

Crises also require staff to maintain productivity and professionalism during what can be an extremely challenging period, where both work and home life may be affected. Drawing on the IAEA's model for security culture, emphasis should be placed on the continued importance of the fundamental building blocks – the belief that a 'credible threat exists' and 'nuclear security is important'.[24] Maintaining organisational focus on routine security risks can be challenging when a large proportion of staff are focused on the crisis itself. Consequently, nuclear organisations may need to increase internal communication about nuclear security – even where inherent security risks are not actually elevated – to maintain awareness and alertness among all staff.[25] Awareness-raising about nuclear security is also a key component of the post-crisis phase when staff return to routine working arrangements, for instance following an extended period when they may have worked from home, such as during a pandemic.

The IAEA's model for security culture also emphasises the importance of 'principles for guiding decisions and behaviours.'[26] These principles include characteristics such as 'professionalism and competence', 'commitment and responsibility' and 'learning and improvement'. Many staff can find responding to a crisis challenging due to, for example, difficulties in human interaction, cuts to staff numbers or reduced oversight. Consequently, developing the model characteristics within a nuclear workforce is crucial to protecting operations, particularly where fellow colleagues or managers cannot be present to assist individuals.

The IAEA's model also notes the essential role of leadership and management systems. As highlighted by previous crises afflicting the nuclear industry such as the 2011 Fukushima Daiichi disaster, effective decision-making can be crucial in preventing a situation from escalating.[27] This involves senior leadership teams taking a visible and outwards-facing role, and acting decisively.[28] At the same time, nuclear security functions benefit from senior decision-makers enabling appropriate levels of flexibility during a crisis. For instance, it may be helpful to overcome bureaucratic obstacles in the early phase of a crisis where senior managers take a pragmatic approach, empowering staff to make independent decisions as a crisis rapidly evolves.

The security culture model of the International Atomic Energy Agency



GOAL: EFFECTIVE NUCLEAR SECURITY

MANAGEMENT SYSTEMS ARE WELL DEVELOPED AND PRIORITIZE SECURITY

a) Visible security policy;
b) Clear roles and responsibilities;
c) Performance measurement;
d) Work environment;
e) Training and qualification;
f) Work management;
g) Information security;
h) Operations and maintenance;
i) Continual determination of trustworthiness;
j) Quality assurance;
k) Change management;
l) Feedback process;
m) Contingency plans and drills;
n) Self-assessment;
o) Interface with the regulator;
p) Coordination with off-site organizations;
q) Record keeping.

BEHAVIOUR FOSTERS MORE EFFECTIVE NUCLEAR SECURITY

Leadership behaviour

a) Expectations;
b) Use of authority;
c) Decision making;
d) Management oversight;
e) Involvement of staff;
f) Effective communications;
g) Improving performance;
h) Motivation.

Personnel behaviour

a) Professional conduct;
b) Personal accountability;
c) Adherence to procedures;
d) Teamwork and cooperation;
e) Vigilance.

PRINCIPLES FOR GUIDING DECISIONS AND BEHAVIOUR

a) Motivation;
b) Leadership;
c) Commitment and responsibility;
d) Professionalism and competence;
e) Learning and improvement.

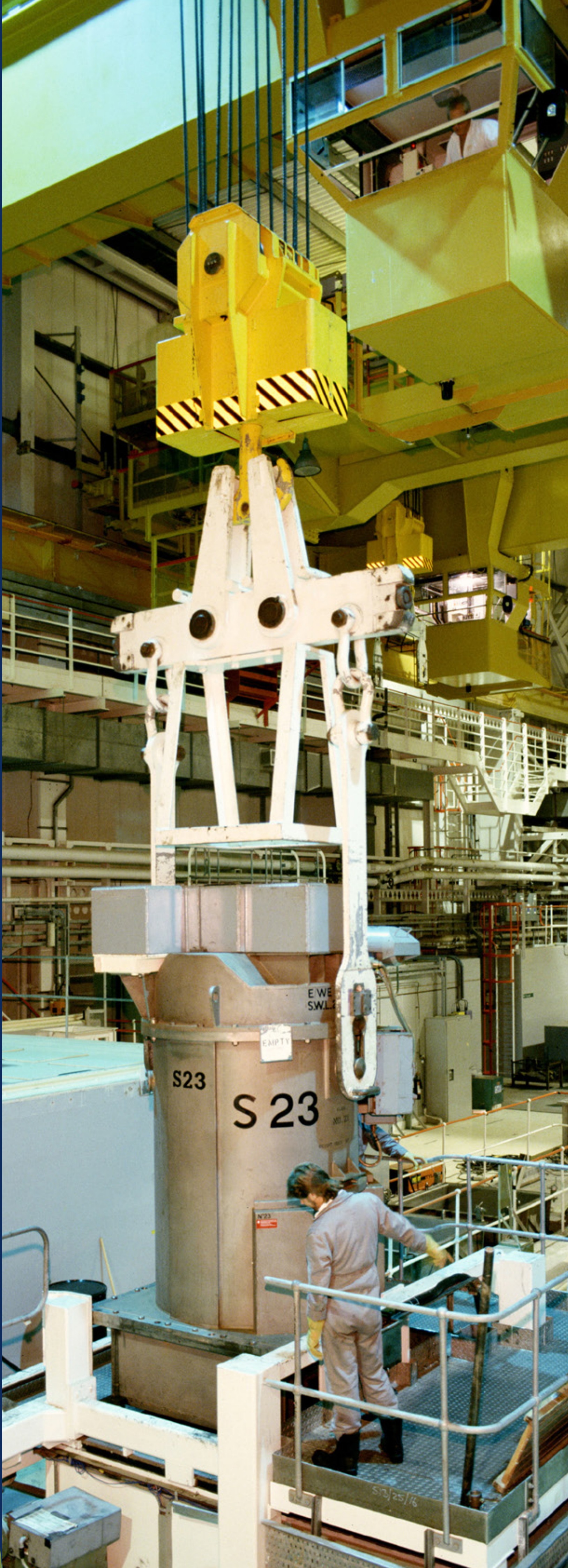
NUCLEAR SECURITY CULTURE

BELIEFS AND ATTITUDES

a) Credible threat exists;
b) Nuclear security is important.

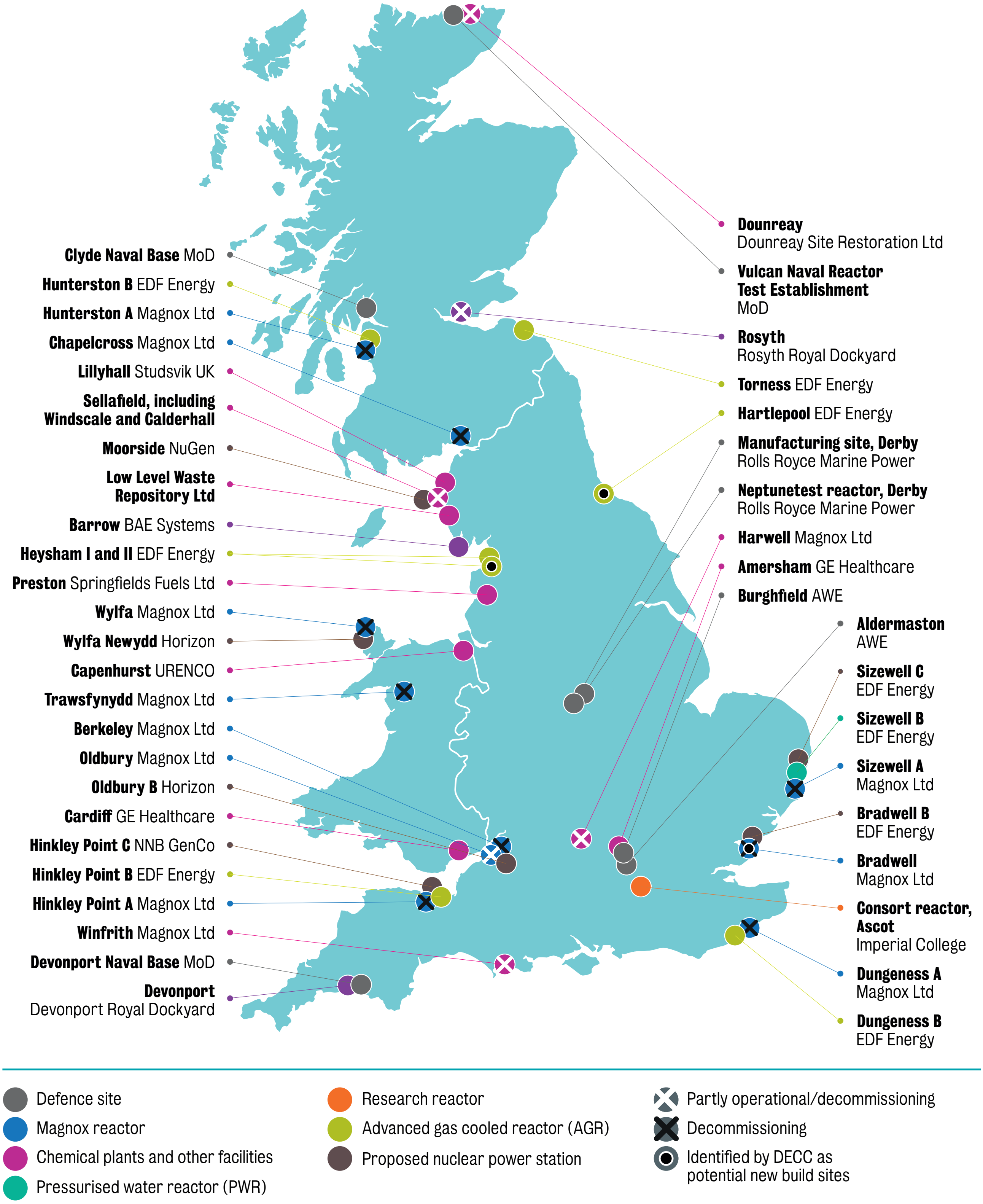
Source: Nuclear Security Series of the IAEA

Part II
The UK's Experience of Delivering Nuclear Security during Covid-19



This section of the policy brief explores how the UK delivered nuclear security following the onset of the Covid-19 pandemic, discussing the challenges encountered and the modification of key measures. It starts by outlining government policy and the regulatory response to the pandemic before discussing operational level changes. Here focus is placed on how operations were secured at the onset of the pandemic, its impacts on supply chains, modifications to physical protection systems, and the transition to remote working.

Nuclear sites in the UK regulated by the Office for Nuclear Regulation


Clyde Naval Base MoD
Hunterston B EDF Energy
Hunterston A Magnox Ltd
Chapelcross Magnox Ltd
Lillyhall Studsvik UK
Sellafield, including Windscale and Calderhall
Moorside NuGen
Low Level Waste Repository Ltd
Barrow BAE Systems
Heysham I and II EDF Energy
Preston Springfields Fuels Ltd
Wylfa Magnox Ltd
Wylfa Newydd Horizon
Capenhurst URENCO
Trawsfynydd Magnox Ltd
Berkeley Magnox Ltd
Oldbury Magnox Ltd
Oldbury B Horizon
Cardiff GE Healthcare
Hinkley Point C NNB GenCo
Hinkley Point B EDF Energy
Hinkley Point A Magnox Ltd
Winfrith Magnox Ltd
Devonport Naval Base MoD
Devonport Devonport Royal Dockyard
Dounreay Dounreay Site Restoration Ltd
Vulcan Naval Reactor Test Establishment MoD
Rosyth Rosyth Royal Dockyard
Torness EDF Energy
Hartlepool EDF Energy
Manufacturing site, Derby Rolls Royce Marine Power
Neptunetest reactor, Derby Rolls Royce Marine Power
Harwell Magnox Ltd
Amersham GE Healthcare
Burghfield AWE
Aldermaston AWE
Sizewell C EDF Energy
Sizewell B EDF Energy
Sizewell A Magnox Ltd
Bradwell B EDF Energy
Bradwell Magnox Ltd
Consort reactor, Ascot Imperial College
Dungeness A Magnox Ltd
Dungeness B EDF Energy
Defence site
Magnox reactor
Chemical plants and other facilities
Pressurised water reactor (PWR)
Research reactor
Advanced gas cooled reactor (AGR)
Proposed nuclear power station
Partly operational/decommissioning
Decommissioning
Identified by DECC as potential new build sites

Source: Guide to Nuclear Regulation in the UK, Office for Nuclear Regulation (ONR)

2.1 Government Direction – Lockdowns, DBT and Reporting

The UK government's response has evolved during the pandemic but broadly it has sought to contain, delay and mitigate the spread of Covid-19 among the general population. At various times, mandatory or advisory measures have been applied to restrict social mobility and proximity, whilst testing and contact tracing regimes have facilitated containment measures. During periods of elevated disease transmission (so-called 'waves' of the virus), government policy has mandated people to work from home, where applicable. This has resulted in a wholesale reduction of the national workforce attending their place of work, other than in critical sectors such as health, government, energy, transport and education.

Most significantly, the scale of infection and transmission led to three national 'lockdowns' in the UK, all of which had a significant impact on economic activity, including in the nuclear sector which experienced a reduction in electricity demand.[29] The prevailing characteristic of lockdowns is to restrict social proximity and mobility in order to prevent the virus from spreading uncontrolled through the population. Fortunately, the rollout of vaccinations in the UK since December 2020 and regular Covid-19 testing have made a significant impact on reducing both the spread and severity of infection.

Throughout the pandemic, the UK government has not made significant changes to nuclear security policies at the national level. At the onset of the crisis, there was some expectation on the part of the nuclear industry that central government would provide additional guidance and potentially policy changes due to the impact on operations.[30] However, no specific direction was initially forthcoming from central government, albeit generic guidance was issued for industry in general, with an emphasis on enabling staff to work remotely.[31] Instead, the Department for Business, Energy and Industrial Strategy (BEIS) – the government ministry responsible for the UK's civil nuclear industry – placed reliance on the judgement of its national competent nuclear authority, the Office for Nuclear Regulation (ONR).

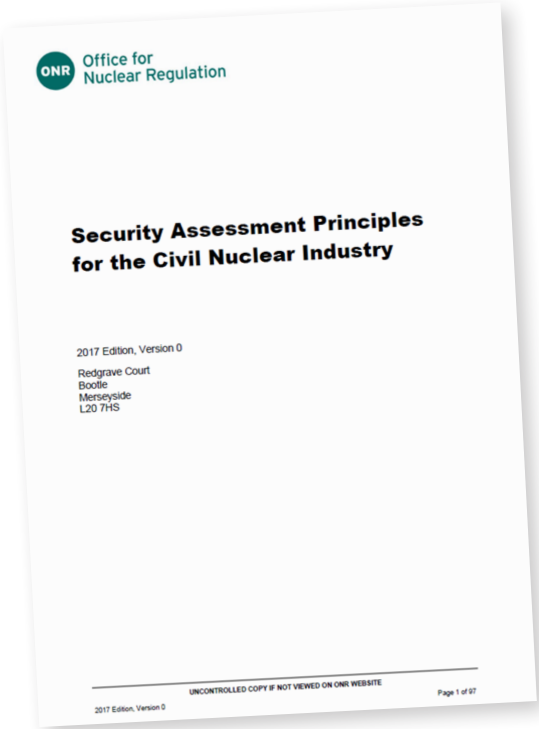
This approach arguably contributed towards a period of turbulence in the early weeks of the Covid-19 pandemic, when the impacts of absenteeism and remote working created high levels of uncertainty across the UK nuclear sector.[32] However, despite this initial period of ambiguity, nuclear operators were aware of what was expected of them and remained focused on their ongoing requirement to secure nuclear assets from malicious adversaries. Meanwhile, BEIS took proactive steps to ensure the continued viability of the UK's Design Basis Threat (DBT), known in the UK as the Nuclear Industries Malicious Capabilities (Planning) Assumptions (NIMCA). This was brought to ministerial level for consideration, with the conclusion that no adjustments were required as there was insufficient intelligence to suggest the threat had changed substantively.[33]

BEIS also expanded its reporting channels for the nuclear industry, coordinating closely with ONR.[34] Every nuclear licensee in the UK was obliged to provide data to BEIS and ONR regarding its site status. Using a RAG (red, amber, green) model, the reporting provided data on absenteeism rates, number of Covid cases, cyber security controls, remote working arrangements, security assurance and other relevant information.[35] Each categorisation was also accompanied by a more detailed statement about the RAG rating, its impact on security, and, where necessary, mitigation measures for any identified shortfalls.

In pre-pandemic times, government was routinely advised on the status of nuclear security by the regulator. However, during periods of lockdowns in the UK, a significant reduction of in-person site inspections reduced the regulator's visibility of security arrangements. A key objective of this information gathering exercise by the regulator and central government was, therefore, to ascertain the levels of operational sustainability across the UK nuclear estate. This would enable the identification of potentially concerning trends so that interventions could be made proactively in order, for example, to maintain the continuous supply of electricity across the UK or avert the potential degradation of safety or security systems.[36]

In effect, the ONR established an information collation operation for the entire civil nuclear sector in collaboration with operators, underpinned by a strong pre-existing regime of stakeholder communication. Initially this posed a challenge for some nuclear organisations that were not yet prepared for the significantly increased demand for data gathering. However, the frequency of data reporting, as of late-2021, has been scaled back somewhat since the initial crisis phase, with a greater focus on data most relevant for centralised decision-making. Nuclear organisations have also sought to further develop their internal data gathering mechanisms, helping strengthen their resilience against future crises. These developments represent an example of how the pandemic has arguably triggered a positive change in the UK's approach to nuclear security.

2.2 Regulatory Approach – Online Engagement and Internal Assurance



ONR Office for Nuclear Regulation

Security Assessment Principles for the Civil Nuclear Industry

2017 Edition, Version 0

Redgrave Court
Bootle
Merseyside
L20 7HS

UNCONTROLLED COPY IF NOT VIEWED ON ONR WEBSITE

2017 Edition, Version 0

Page 1 of 97

Source: Office for Nuclear Regulation (ONR) 2017

The UK has a relatively unique approach to the regulation of nuclear security in the civil nuclear sector, having transitioned over the past two decades from a prescriptive rules-based system to an outcome-focused system. The new regulatory regime is built on high-level security requirements known as Security Assessment Principles (SyAPs), with responsibility for security risk management to achieve these outcomes placed on the operator and a framework for validation by the regulator.[37] This provides operators with flexibility in their development and deployment of security arrangements, the effectiveness of which they must determine and validate through the provision of evidence which is assessed by ONR through routine onsite regulatory inspection and engagement.[38]

In response to the pandemic, nuclear security arrangements and assurance mechanisms have been modified with ONR adapting its approach to industry engagement. At the onset of the crisis, in line with the UK's outcomes-focused regulatory approach, nuclear operators led the modification of their security arrangements, as opposed to these being directed by ONR. This approach was perceived to be beneficial with operators noting the useful flexibility that this conferred in enabling them to develop solutions that efficiently met the needs of individual sites at a critical time when speed was of the essence.[39] In particular, operators were able to ensure that nuclear security was maintained whilst also focusing on the new health responsibilities for their personnel, a complex endeavour that often-required bespoke solutions.[40] Meanwhile, ONR's annual test exercises were postponed along with other activities that did not carry a critical or urgent status.

Most significantly, the Covid-19 pandemic forced ONR to avoid in-person visits where routine business could be delayed or conducted via digital platforms. This resulted in significant revisions to ONR's 'Integrated Intervention Strategies' (ISS) – a procedure of identifying actions an operator needs to take to improve issues, following a site visit.[41] The interventions were scaled back according to an assessment based on sites' nuclear material holdings, other risks and past performance.[42] Although the security assurance process was now largely being conducted remotely, ONR maintained a 'trust and verify' approach, where operators were still expected to provide satisfactory evidence of the claims being made through frequent and routine digital reporting. This involved data collection and online engagement with regulatory inspectors, with greater emphasis placed on desk-based assessments and the internal assurance processes set up by individual operators.[43] As the effects of the pandemic abate, ONR has increased the proportion of its nuclear security assessment work remotely, due to the already observable efficiencies this offers. Onsite visits will still take place but will be focused on sites which require more intervention and where ONR can add greatest value.[44]

Regulating nuclear security in the UK during the Covid-19 pandemic has also demonstrated the importance of transparency and trust between stakeholders, given the increased physical separation. To maintain and foster this there has been an increase in the frequency of online meetings between regulators and operators to discuss issues, for example, the modification of nuclear security, absenteeism rates and the resilience of security arrangements. When lockdown restrictions were eased, regulatory intervention visits were resumed but on a lesser frequency – underpinned by the success of, and value placed upon, how this remote assurance activity had been conducted. In effect, the experience of the pandemic has placed an increased emphasis on operator's internal assurance mechanisms in order to satisfy ONR's requirements.

2.3 Risk Management – Flexibility and Resilience

As discussed previously, in the UK nuclear licensees have relatively broad authority to manage security risks as they consider appropriate. This responsibility, enshrined in regulation, generates different approaches to security risk management across the UK's nuclear sites, though all nuclear licensees are legally required to reduce risks where 'reasonably practicable' to 'an acceptable level'.[45] Accordingly, nuclear licensees have developed their own risk-informed management systems, which are regularly revised, tested, updated and reviewed by the regulator.[46]

When the pandemic unfolded in early 2020, the UK's nuclear organisations were prepared in varying degrees to manage the scale of impact and disruption through their risk management systems. A flu pandemic was listed in the National Risk Register and, as such, most nuclear operators included a pandemic scenario as one of the potential risks in their risk management assessments, with corresponding mitigation strategies set out.[47] Yet, while operators were aware that a pandemic represented a serious threat, most did not consider this to be sufficiently probable or damaging to warrant significant contingency planning. This is reflected by the lack of any sector-wide exercises addressing the impact of a pandemic, with this scenario typically ranked outside the top-10 risks in company risk registers. As such, pre-existing mitigation strategies for this specific risk and its consequences were relatively underdeveloped.

Like many industries around the world, the UK nuclear sector initially found itself 'on the back foot' facing the enveloping crisis in early 2020.[48] Here, three crucial factors enabled the UK nuclear industry to respond quickly and effectively at the onset of the pandemic. First, while risk management assessments for nuclear sites did not contain fully developed pandemic plans, the industry as a whole had considerable experience in enacting broader contingency and 'in-crisis' planning. For example, some operators already had nuclear security 'incident management' teams in place, who could develop response mechanisms across the business at speed, and crucially they often already reported directly to senior management.[49] Second, the experience of regular stress testing of nuclear security systems and an enabling security culture has served to create resilience within the broader workforce, with staff tending to observe protocol, which was particularly valuable as procedures were changed due to the pandemic. Third, the aforementioned skeletal risk management contingency plans acted as a vehicle for more detailed decision-making – and not as a constraint which might occur in overly-detailed, prescriptive response plans. Indeed, it would seem the adaptability and flexibility of these plans, facilitated by the UK's regulatory approach to nuclear security, proved beneficial at a time when events were moving fast and relatively little was known about the disease.

As part of the risk management process, most nuclear operators set up their own Covid-19 response units which worked across the business and, importantly, often reported directly to the senior leadership team. Approaches to delivering nuclear security inevitably differed across organisations, but common principles included securing operations, strengthening contingency planning and protecting supply chains. Here models deemed particularly effective employed transitional phases, comprising: horizon scanning; early contingency planning; enacting and planning; implementation; and recovery. Although these phases were essentially linear, the model was sufficiently flexible to allow the organisation to revert to an earlier phase, when appropriate.

2.4 Overcoming Absenteeism – Redundancy, Worker Status and Testing

One of the most significant challenges for the UK nuclear industry has been managing the impacts of high levels of absenteeism during the pandemic. A Covid-19 outbreak concentrated at a nuclear plant could potentially result in entire shifts being unable to work, affecting operations and potentially degrading security if this occurred within the guarding and responses forces. Of particular concern would be an outbreak within the Civil Nuclear Constabulary (CNC), who provide armed response at UK nuclear sites and whose work necessarily involves physical patrolling and coming into close contact with colleagues.

Absenteeism within the UK nuclear industry has been mostly due to staff needing to self-isolate at various times owing to national travel restrictions, being a close contact of a positive Covid-19 case or, to a lesser extent, being stricken by the illness itself. In spring 2020, there was a short period when the absenteeism rate was very high across the UK nuclear industry; this was at a critical point when operators were in the initial process of responding to the pandemic and securing operations. Although concerns were raised at the time to the regulator, additional staff capacity and prioritisation of human resources ensured sufficient resilience in the system and at no point was there any threat of a UK reactor being shut down or kept offline.[50]

Absenteeism was also an issue that impacted the supply chain. At an early stage of the crisis, operators recognised that protecting the supply chain and networks of local contractors was vital. The turbulence in the supply chain was felt through a significant reduction in the numbers of suppliers achieving routine access to sites. In some cases, this required the reorganisation of existing contractual frameworks, to reflect this and to ensure onsite access for the provision of essential and operationally critical services from the supply chain. One such example was the preventive maintenance of critical security technologies.[51] At the same time, it has been necessary to ensure the health and welfare of contractors in the same way that staff have been protected.

In order to mitigate the risk of absenteeism, many staff working in the civil nuclear industry were classified as 'key workers' and, later when the designation changed, as 'critical workers'.[52] This worker status was extremely useful for maintaining productivity as, among other assistance, staff were able to access childcare during lockdowns. From December 2020, the National Health Service (NHS) began its successful rollout of vaccinations across the UK, helping to reduce levels of absenteeism across all sectors. From March 2021, the government made lateral flow tests – which can help detect asymptomatic cases – available free of charge to all businesses and later on to the wider population.[53] And since July 2021, workers in the civil nuclear sector have been exempt from isolation in the event they come into close contact with a positive case, on the proviso they take part in daily swab testing.[54] The combination of these measures has helped maintain business continuity in the UK nuclear sector, especially during periods of high disease transmission.

Even in pre-pandemic times, nuclear facilities allowed for some limited additional redundancy in the system to safeguard against any potential threats such as unexpected levels of absenteeism. The Covid-19 pandemic has highlighted how the UK nuclear industry tends to build in more contingencies than might be borne out during a crisis – in other words, a 'belt and braces' approach. Thus, the experience of the pandemic has generally affirmed the benefits of a conservative approach to risk management and the importance of operating above minimum security thresholds.

2.5 Physical Protection – Consolidation, Social Distancing and Innovation

Despite the pandemic's disruptive impacts, sustaining onsite physical security generally required only minor modifications, with fundamental principles of protection still being applied. Here a major difference was the significantly reduced numbers of onsite staff, although the overall numbers of onsite security personnel remained similar to pre-pandemic levels.[55] At the onset of the pandemic, nuclear operators followed through on crisis management protocols by re-assessing the design basis planning and vulnerability assessments for their nuclear assets. The most significant change to the risk landscape was the reduction in onsite staff, either because they were self-isolating, already working remotely, or unable to travel to the site owing to travel restrictions. Here nuclear organisations were aware that this new working environment impacted risk profiles within their site, which were continuously assessed.

On the one hand, the reduction in onsite staffing levels arguably served to lower the physical 'insider' threat to nuclear materials. Furthermore, fewer onsite staff simplified the patrolling, surveillance and access control aspects of nuclear security as vulnerabilities were more visible and there was less congestion from vehicles and operations in vital areas.[56] On the other hand, there were fewer people around to notice anomalies or potential security vulnerabilities.[57] A more complex consideration for nuclear organisations was whether the Covid-19 pandemic might change the planning assumptions of malicious actors. While the motivations, intentions and capabilities of malicious actors can be expected to be enduring, the potential perception that during a crisis the ability of security forces to adequately protect their target is weakened – whether valid or not – might act as a catalyst for adversaries to launch an attack.

Early on in the crisis, it became clear that a key priority was protecting facilities and offices from disease transmission, and inevitably safety and security counterparts needed to work closely to solve the practical challenges.[58] With significantly fewer staff onsite, operators were able to consolidate some aspects of physical protection, such as reducing the number of entry points, suspending some staff checks and closing onsite car parks.[59] While operators did not tend to make substantial alterations to the shifts worked, onsite staff were sometimes placed into 'bubbles' to ensure any potential Covid-19 outbreak could be contained to a single shift; for the same reasons, staff might be rotated less frequently between work stations.[60] Meanwhile, there were reductions in the frequency of routine maintenance for some security systems; where maintenance was necessary, this was again often conducted in a 'bubble' structure but only for critical security systems, structures and components. Training was another area significantly undermined by the pandemic. In many cases training had to be delayed or its delivery transitioned to digital platforms. Nevertheless, the use of digital platforms for training has since been recognised as beneficial by nuclear organisations, with some aspects of nuclear security training set to continue being delivered via digital platforms in the longer term.[61]

The nuclear industry has some of the strictest safety and security protocols of any sector, and there is an expectation of strict adherence. During the pandemic, this strong culture of compliance helped personnel to adapt to the new operating environment with its emphasis on social distancing, enhanced hygiene and personal protective equipment (PPE). Staff were used to working in a highly disciplined and compliant environment, ensuring that PPE and other Covid-19 protocols were complied with.[62] The requirement for enhanced hygiene also meant that cleaning became a new focus of nuclear security, with extra cleaning staff being brought onsite to sterilise sensitive items such as security access control touch pads and turnstiles.[63]

The requirement for social distancing created some logistical difficulties for physical protection. In particular, operators needed to find alternative ways to deliver security controls that require proximity between people, such as bag searches and 'pat-down' body searches.[64] The guard force – which in the UK comprises an unarmed Civilian Guard Force (contracted) and the Armed Response Force of the Civil Nuclear Constabulary (CNC) – has encountered more challenges than most in delivering security during the pandemic, as guarding by its nature, for the most part, cannot be conducted remotely. Meanwhile, there were challenges for nuclear organisations reliant on travel due to the inevitably close proximity between people, especially in the case of car sharing or bus transportation of staff.[65]

In terms of the evaluation of physical protection systems, a reduction of onsite staff and contractors due to Covid-19 resulted in necessary changes to routine examination, inspection, maintenance and testing (EIMT). Overall, this was reduced according to a risk-based approach with operators identifying the critical elements of systems where EIMT must be maintained, while significantly lowering EIMT for less critical components except in cases where performance assessment could be conducted remotely on digital platforms. Large-scale security exercises involving multiple departments were also postponed during periods of national and local lockdowns. With the agreement of the regulator, such exercises were postponed and then rescheduled for periods when lockdowns were lifted. This is another example of collaboration between operators and the regulator where solutions could be achieved through a risk management approach.

The pandemic also saw an increase in both the number of 'temporary security plans' (TSPs) and the duration over which these extend. Typically, TSPs are used for temporary and short periods of increased risk such as barrier repairs and new build construction. However, during the pandemic, operators applied TSPs to a greater variety of situations, including those that were not strictly temporary in nature such as vehicle searching. This more flexible approach was facilitated by ONR implementing an overarching 'variation policy' that allowed a broader operator interpretation of security 'variations' and a greater degree of operator autonomy to use TSPs. Nevertheless, ONR still required visibility of TSP maintenance throughout this period, based on a 'trust and verify' approach to regulation. This meant that operators could apply greater autonomy in the use of TSPs but each decision still formed part of a risk-managed approach, where operators would be expected to provide evidence to the regulator for claims being made.[66]

Despite the aforementioned challenges, the pandemic has also served to trigger improved efficiencies in some aspects of physical protection.[67] Historically, the development of nuclear security in the UK came many decades after the industry itself was established, meaning that physical protection has tended to be based on a plant's existing operations. But with fewer staff onsite, operators have been able to reassess and streamline a number of nuclear security processes. While the increasing return of onsite staff means some measures will only be temporary, the situation has triggered internal reviews of such matters on the basis of the benefits identified.[68] With security, safety and human health issues now at the vanguard of operators' concerns, it has more generally proved easier for teams responsible for nuclear security to push through changes. In the longer term, the UK nuclear industry is likely to adopt some of these new ways of working where they can be demonstrated to strengthen nuclear security.

2.6 Remote Working – Transition Process and Cyber Security

The large-scale transition to remote working during the Covid-19 pandemic was one of the most significant operational changes for the UK's nuclear industry. In early 2020, organisations faced very short lead-in times and minimal preparation to shift large numbers of staff from nuclear facilities and offices to remote working arrangements. This transition was unprecedented for an industry in which staff were, prior to the pandemic, overwhelmingly based in nuclear facilities or shared offices. Almost overnight, nuclear organisations needed to set up new remote networks with rigorous security controls while also managing a significant cultural shift with many of their workers being entrusted to work securely and alone for the first time.

UK nuclear organisations are highly cognisant of the risk of cyber-attacks and there are stringent controls in place to protect computer and information management systems and the data they hold. However, one of the most significant changes in the threat environment during the pandemic was a surge in cyber-attacks around the world. In a report released in March 2021, the UK's Department for Digital, Culture, Media and Sport (DCMS) found that 39% of businesses had experienced a cyber security breach in the previous 12 months.[69] Cyber criminals increased both the frequency and severity of cyber-attacks on companies, taking advantage of the large numbers of staff transitioning to working remotely.

Notably, Interpol observed a shift in cyber-attacks against individuals and small businesses towards these targeting major corporations, governments and critical infrastructure.[70] Nuclear organisations in the UK have not reported any major targeted cyber-attacks against the sector, but incidents in other industries – especially health – have exposed the vulnerability of organisations to cyber-attacks and online scams during Covid-19. Noteworthy incidents during the pandemic include cyber-attacks on two French hospitals in February 2021, Ireland's Health Service Executive in May 2021 and a Japanese shipping company in March and July 2021.

In general, a transition to remote working is likely to increase the risk of a cyber compromise, if this outpaces a worker's familiarity with changing cyber security requirements. To mitigate this, UK nuclear organisations have scaled up their security controls and increased internal communications about mitigating the risks of, for example, the loss of the site security plan (SSP) held in digital format. This has also required the provision of additional training for staff on best practice approaches to cyber security. In particular, staff have been reminded about changing passwords regularly, avoiding insecure video conferencing platforms and restricting business-related email messages to work accounts. Nevertheless, as in other industries, there were some 'teething problems' with a small minority of staff initially not complying with the new computer security protocols. Fortunately, most such irregularities could be automatically detected by network computer security tracking controls.[71]

Despite the upheaval, the transition to remote working has proved to be a broadly positive experience for the UK nuclear industry. Many of the paper-based processes in the nuclear industry were substituted through the use of electronic systems, while working from home has provided extra flexibility for staff. Notably, many organisations have signalled plans to maintain a hybrid model of combining onsite and remote working, even when the pandemic abates.[72] Meanwhile, certain aspects of staff training are expected to continue being delivered by digital platforms. Some of the assurance and assessment work by the regulator may also continue to be conducted remotely via digital platforms.[73] Nuclear organisations have observed greater awareness at all levels of security risks related to information management and of the vital importance of data.[74] Indeed, the nuclear industry's increased dependency on technology was not perhaps fully appreciated in the past.

The experience of remote working has also meant that digital communications, information management, cyber security and internet connectivity are now more fully embedded in organisations' risk assessments and business continuity models.[75] The way that the nuclear industry has embraced remote working highlights the transformational impact of a major crisis on organisations – and not only in the nuclear sector – by driving forward changes to working arrangements that may otherwise have taken much longer without such a catalyst. In this respect, crises, although often detrimental to organisations, can at the same time force innovation and strategic change through a shift in risk perceptions and risk appetite.

2.7 Insider Threats – Human Reliability Programmes and Staff Wellbeing

All staff in the UK nuclear industry undergo security checks as part of routine employment vetting controls. While levels of new recruitment dipped at the onset of the crisis, especially for contracting staff, there were inevitably additions and changes to the workforce throughout the pandemic – and this still required vetting and personnel screening. Even in pre-pandemic times many aspects of vetting and personnel screening were conducted electronically, but now almost all checks are conducted via digital platforms and remote face-to-face engagement; overall it was deemed that this has made the process more efficient.[76] However, a particular challenge facing the industry at the onset of the crisis was that existing staff had undergone screening premised on them being based in onsite facilities or offices. In consultation with the regulator, nuclear operators were able to extend vetting arrangements for various categories of staff to enable the rapid transition to remote working (with additional cyber security controls in place, as previously discussed).[77]

For most industries, the risk of the insider threat has increased as a result of the Covid-19 pandemic, due to a combination of vast numbers of people working remotely and the domestic, financial and emotional pressures that can lead to worker disgruntlement. The global nuclear industry has been better protected from the global economic downturn, with no reports to date of plant closures stemming from financial causes; equally, the pandemic has not led to electricity supply interruptions in countries monitored by the World Nuclear Industry Status Report.[78] Nevertheless, external Covid-19 related pressures are likely to have impacted the morale of some staff working in the nuclear sector both globally and in the UK. Disgruntlement, financial worries, ill health and dissatisfaction are known contributing factors for insider actions.[79] While nuclear organisations increasingly recognise the vital importance of staff wellbeing as part of their duty of care, the pandemic has highlighted the centrality of this area for mitigating against the insider threat too.

In the UK, mitigation of the insider threat has been further complicated by the sizeable proportion of the nuclear workforce working from home. This poses inherent challenges in maintaining oversight of staff with a more dispersed workforce. A combination of isolation and reduced oversight increases both the probably of and opportunity for insider actions relating to cyber-attacks. While the industry has implemented rigorous technical controls on its remote networks, a major challenge remains the retention of a robust security culture in a remote working environment that both recognises and responds to the insider threat. The UK's Centre for the Protection of National Infrastructure (CPNI) is working with industry to develop training and monitoring in this area, including for when staff return to the workplace after the pandemic abates.[80] In particular, the CPNI has highlighted the importance of providing a duty of care to staff through investing in their wellbeing and professional development, which in turn mitigates against the insider threat.[81]

Recognising the evolving challenges, nuclear organisations in the UK have stepped up awareness-raising of the insider threat through the different elements of their human reliability programmes.[82] The monitoring of the use of devices by staff is routinely deployed within the UK nuclear industry, in an effort to both identify malicious activity and correct inadvertent actions that my undermine security. This has increased during Covid-19 with monitored devices now being deployed in greater numbers and more heavily away from nuclear sites. The use of monitoring tools must be balanced with issues of confidentiality and the UK's Data Protection Act (in force since 2018), in order to ensure that their deployment is proportional to the perceived risks. This was case even during the crisis phase of the pandemic where the benefits and drawbacks of increased monitoring were debated at the organisational level.

Disclaimer

The authors of this report invite liberal use of the information provided in it for educational purposes, requiring only that the reproduced material clearly cite the source, with the following elements to be included (in any reasonable referencing format): 'Lessons for Nuclear Security from the UK's Response to Covid-19', by Dr Sarah Tzinieris, George Foster (Amport Risk Limited) and Professor Christopher Hobbs, King's College London CSSS Occasional Paper Series, January 2022. The material in this document should not be used in other contexts without seeking explicit permission from the authors.

References

1 For a detailed discussion of past crises and their impact on nuclear security, please see Geoffrey Chapman, Rebecca Earnhardt, Christopher Hobbs, Nickolas Roth, Daniel Salisbury, Amelie Stoetzel and Sarah Tzinieris. 2021. 'Nuclear Security in Times of Crisis', CSSS Occasional Paper Series. https://www.kcl.ac.uk/csss/assets/nuclear-security-in-times-of-crisis-handbook.pdf

2 See the 'Nuclear Security Series' guidance and implementation documents of the International Atomic Energy Agency (IAEA). Vienna. https://www.iaea.org/resources/nuclear-security-series

3 Hermann, Charles F. 1963. 'Some Consequences of Crisis Which Limit the Viability of Organisations'. Administrative Science Quarterly, pp. 61-82; Chapman, Geoffrey, Rebecca Earnhardt, Christopher Hobbs, Nickolas Roth, Daniel Salisbury, Amelie Stoetzel and Sarah Tzinieris. June 2021. 'Nuclear Security in Times of Crisis Handbook'. London: King's College London. https://www.kcl.ac.uk/csss/assets/nuclear-security-in-times-of-crisis-handbook.pdf

4 Pauchant, Thierry C. and Ian Mitroff. 1992. Transforming the Crisis-Prone Organization: Preventing Individual, Organizational and Environmental Tragedie. Jossey Bass Business & Management Series; British Standards Institution (BSI). 31 May 2014. British Standard 11200:2014. Crisis Management: Guidance and Good Practice. https://shop.bsigroup.com/products/crisis-management-guidance-and-good-practice-1?pid=000000000030274343

5 British Standards Institution (BSI). 31 May 2014. British Standard 11200:2014. Crisis Management: Guidance and Good Practice. https://shop.bsigroup.com/products/crisis-management-guidance-and-good-practice-1?pid=000000000030274343

6 Comfort, Louise K., Arjen Boin and Chris C. Demchak (eds.). 2010. Designing Resilience: Preparing for Extreme Events. Pittsburgh: University of Pittsburgh Press.

7 Comfort, Louise K., Arjen Boin and Chris C. Demchak (eds.). 2010. Designing Resilience: Preparing for Extreme Events. Pittsburgh: University of Pittsburgh Press, p. 9; Langeland, Krista, David Manheim, Gary McLeod and George Nacouzi. 2016. 'How Civil Institutions Build Resilience: Organizational Practices Derived from Academic Literature and Case Studies'. RAND Corporation, pp. 35-36. https://www.rand.org/pubs/research_reports/RR1246.html

8 International Atomic Energy Agency (IAEA). 2011. 'Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities', Nuclear Security Series: Recommendations. No. 13. INFCIRC/225/Revision 5. Vienna. https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1481_web.pdf

9 International Atomic Energy Agency (IAEA). 2011. 'Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities', Nuclear Security Series: Recommendations. No. 13. INFCIRC/225/Revision 5. Vienna. https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1481_web.pdf

10 In considering what a risk means for nuclear security, there are three major components to consider: threat, vulnerability and consequence.

11 International Atomic Energy Agency (IAEA). 2015. 'Risk Informed Approach for Nuclear Security Measures for Nuclear and Other Radioactive Material out of Regulatory Control'. Nuclear Security Series (NSS): Implementing Guide. No.24-G, p. 2. https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1678_web.pdf

12 Hobbs, Christopher, Nickolas Roth and Daniel Salisbury. 28 June 2021. 'Security under Strain? Protecting Nuclear Materials during the Coronavirus Pandemic'. The RUSI Journal. Vol. 166, no. 1. https://www.tandfonline.com/doi/full/10.1080/03071847.2021.1937302; Findings from author interview with UK nuclear operator. January 2021.

13 International Atomic Energy Agency (IAEA). 2015. 'Risk Informed Approach for Nuclear Security Measures for Nuclear and Other Radioactive Material out of Regulatory Control'. Nuclear Security Series: Implementing Guide. No.24-G. Vienna. https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1678_web.pdf

14 International Atomic Energy Agency (IAEA). 2015. 'Risk Informed Approach for Nuclear Security Measures for Nuclear and Other Radioactive Material out of Regulatory Control'. Nuclear Security Series: Implementing Guide. No.24-G. Vienna. https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1678_web.pdf

15 The National Diet of Japan. July 2012. 'The Fukushima Nuclear Accident Independent Investigation Commission'. Tokyo. http://large.stanford.edu/courses/2013/ph241/mori1/docs/NAIIC_report_hi_res10.pdf

16 International Atomic Energy Agency (IAEA). 2011. 'Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities', Nuclear Security Series: Recommendations. No. 13. INFCIRC/225/Revision 5. Vienna. https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1481_web.pdf

17 International Atomic Energy Agency (IAEA). 3 March 1980. Convention on the Physical Protection of Nuclear Material. Information Circular. INFCIRC/274/Rev.1. Vienna. https://www.iaea.org/sites/default/files/infcirc274r1.pdf

18 International Atomic Energy Agency (IAEA). 2011. 'Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities', Nuclear Security Series: Recommendations. No. 13. INFCIRC/225/Revision 5. Vienna. https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1481_web.pdf

19 'CT Measures, Emergency Preparedness and Response Planning', Office for Nuclear Regulation (ONR). October 2020. https://www.onr.org.uk/operational/tech_asst_guides/cns-tast-gd-10.1.pdf

20 'CT Measures, Emergency Preparedness and Response Planning', Office for Nuclear Regulation (ONR). October 2020. https://www.onr.org.uk/operational/tech_asst_guides/cns-tast-gd-10.1.pdf

21 Macnamara, Jim. 10 April 2021. 'New Insights into Crisis Communication from an "inside" emic perspective during COVID-19', Public Relations Inquiry. pp.237-262.

22 'Recommendations for Crisis Management'. April 2017. 2016 Additional Global Security Programme. https://uic.org/IMG/pdf/crisis_management_report.pdf

23 International Atomic Energy Agency (IAEA). 2011. 'Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities', Nuclear Security Series: Recommendations. No. 13. INFCIRC/225/Revision 5. Vienna. https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1481_web.pdf

24 International Atomic Energy Agency (IAEA). 2008. 'Nuclear Security Culture: Implementing Guide'. Nuclear Security Series. No. 7. Vienna. https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1347_web.pdf

25 Findings from author interview with UK nuclear operator. March 2021.

26 International Atomic Energy Agency (IAEA). 2008. 'Nuclear Security Culture: Implementing Guide'. IAEA Nuclear Security Series. No. 7. Vienna. https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1347_web.pdf

27 Chapman, Geoffrey, Rebecca Earnhardt, Christopher Hobbs, Nickolas Roth, Daniel Salisbury, Amelie Stoetzel and Sarah Tzinieris. June 2021. 'Nuclear Security in Times of Crisis Handbook'. London: King's College London. https://www.kcl.ac.uk/csss/assets/nuclear-security-in-times-of-crisis-handbook.pdf

28 Macnamara, Jim. 10 April 2021. 'New Insights into Crisis Communication from an "inside" emic perspective during COVID-19', Public Relations Inquiry. pp.237-262.

29 Mehlig, Daniel, Helen ApSimon and Iain Staffell, 'The impact of the UK's COVID-19 lockdowns on energy demand and emissions', Environmental Research Letters, Vol.16, No.5. 30 April 2021.

30 Findings from author interviews with various UK nuclear operators. January-March 2021.

31 United Kingdom Parliament. 26 March 2020. 2020 No.350, The Health Protection (Coronavirus, Restrictions) (England) Regulations 2020. https://www.legislation.gov.uk/uksi/2020/350/pdfs/uksi_20200350_en.pdf; also see United Kingdom Government. 23 November 2020. 'Guidance overview: COVID-19 Winter Plan'. https://www.gov.uk/government/publications/covid-19-winter-plan#history

32 Findings from author interviews with various UK nuclear operators. January-March 2021.

33 Findings from author interview with UK national authority. January 2021.

34 Findings from author interview with UK national authority. February 2021.

35 Findings from author interview with UK national authority. January 2021.

36 Findings from author interview with UK national authority. February 2021.

37 Office for Nuclear Regulation (ONR). 'Security Assessment Principles (SyAPS)'. Website of ONR. https://www.onr.org.uk/syaps

38 For a summary of the UK's nuclear security regulatory transition, see Sims, Matthew. March 2020. 'UK Experiences of Implementing an Outcome Focused Security Regulation'. International Conference on Nuclear Security (ICONS). Conference proceedings. Vienna. https://conferences.iaea.org/event/181/contributions/15682/

39 Findings from author interview with various UK nuclear operators. January-February 2021.

40 Findings from author interviews with various UK nuclear operators. January-March 2021.

41 Office for Nuclear Regulation (ONR). October 2020. 'Guidance for Strategy Inspection Planning and Recording'. ONR Compliance Inspection Guide. https://www.onr.org.uk/operational/tech_insp_guides/onr-insp-gd-059.pdf

42 Findings from author interview with UK national authority. February 2021.

43 Findings from author interview with UK national authority. February 2021.

44 Findings from author interview with UK national authority. February 2021.

45 Office for Nuclear Regulation (ONR). 2017. 'Security Assessment Principles for the Civil Nuclear Industry'. https://www.onr.org.uk/syaps/security-assessment-principles-2017.pdf

46 Office for Nuclear Regulation (ONR). June 2017. 'Risk informed regulatory decision making'. https://www.onr.org.uk/documents/2017/risk-informed-regulatory-decision-making.pdf

47 Findings from author interviews with various UK nuclear industry stakeholders. January-March 2021; House of Lords Library. 28 May 2020. The National Risk Register: Preparing for national emergencies. UK Parliament. https://lordslibrary.parliament.uk/the-national-risk-register-preparing-for-national-emergencies/.

48 Findings from author interview with UK nuclear operator. March 2021.

49 Findings from author interview with UK nuclear operator. January 2021.

50 Findings from author interview with UK nuclear operator. March 2021.

51 Findings from author interview with UK nuclear operator. January 2021.

52 For a list of critical workers, see 'Guidance: Children of critical workers and vulnerable children who can access schools or educational settings'. 9 March 2021. Website of UK government. https://www.gov.uk/government/publications/coronavirus-covid-19-maintaining-educational-provision/guidance-for-schools-colleges-and-local-authorities-on-maintaining-educational-provision#critical-workers

53 'Press release: Free rapid tests for all businesses for regular workplace testing'. 6 March 2021. Website of UK government. https://www.gov.uk/government/news/free-rapid-tests-for-all-businesses-for-regular-workplace-testing; 'Order coronavirus (COVID-19) rapid lateral flow tests'. Website of UK government. https://www.gov.uk/order-coronavirus-rapid-lateral-flow-tests

54 UK Government. 27 May 2020 (updated on 13 August 2021). 'Guidance: NHS Test and Trace in the workplace'. https://www.gov.uk/guidance/nhs-test-and-trace-workplace-guidance

55 Findings from author interviews with various UK nuclear operators. January-March 2021.

56 Findings from author interview with UK nuclear operator. February 2021.

57 Centre for the Protection of National Infrastructure (CPNI). August 2020. 'Insider Threats in a Pandemic' and 'Return to the Workplace' in 'COVID-19 and security'. https://www.cpni.gov.uk/covid-19-easing-lockdown

58 Findings from author interviews with various UK nuclear operators. January-March 2021.

59 Findings from author interview with UK nuclear operator. March 2021.

60 Findings from author interview with UK national authority. February 2021.

61 Findings from author interview with UK nuclear operator. March 2021.

62 Centre for the Protection of National Infrastructure (CPNI). August 2020. 'Insider Threats in a Pandemic' and 'Return to the Workplace' in 'COVID-19 and security'. https://www.cpni.gov.uk/covid-19-easing-lockdown

63 Findings from author interview with UK nuclear operator. January 2021.

64 Findings from author interview with UK nuclear operator. January 2021.

65 Findings from author interview with UK nuclear operator. March 2021.

66 Findings from author interview with UK nuclear operator. February 2021.

67 Findings from author interviews with various UK nuclear operators. January-March 2021.

68 Findings from author interviews with various UK nuclear operators. January-March 2021.

69 Department for Digital, Culture, Media and Sport (DCMS). 24 March 2021. 'Businesses urged to act as two in five UK firms experience cyber attacks in the last year'. https://www.gov.uk/government/news/businesses-urged-to-act-as-two-in-five-uk-firms-experience-cyber-attacks-in-the-last-year

70 Interpol. August 2020. 'Cybercrime: Covid-19 Impact', p. 4. https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19

71 Findings from author interviews with various UK nuclear operators. January-March 2021.

72 Findings from author interviews with various UK nuclear operators. January-March 2021.

73 Findings from author interview with UK national authority. February 2021.

74 Findings from author interviews with various UK nuclear operators. January-March 2021.

75 Findings from author interviews with various UK nuclear operators. January-March 2021.

76 Findings from author interview with UK nuclear operator. March 2021.

77 Findings from author interview with UK nuclear operator. March 2021.

78 Schneider, Mycle et al. September 2021. 'The World Nuclear Industry Status Report 2021'. Paris. https://www.worldnuclearreport.org/-World-Nuclear-Industry-Status-Report-2021-.html

79 Hobbs, Christopher, Nickolas Roth and Daniel Salisbury. 28 June 2021. 'Security under Strain? Protecting Nuclear Materials during the Coronavirus Pandemic'. The RUSI Journal. Vol. 166, no. 1. https://www.tandfonline.com/doi/full/10.1080/03071847.2021.1937302

80 See resources provided by the Centre for the Protection of National Infrastructure (CPNI), 'COVID-19 and security'. 9 June 2001. https://www.cpni.gov.uk/covid-19-easing-lockdown

81 Centre for the Protection of National Infrastructure (CPNI). August 2020. 'Insider Threats in a Pandemic' and 'Return to the Workplace' in 'COVID-19 and security'. https://www.cpni.gov.uk/covid-19-easing-lockdown

82 Findings from author interviews with various UK nuclear operators. January-March 2021.

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