CENTRE FOR SCIENCE & SECURITY STUDIES

KING'S College LONDON

Nuclear Security within Academic and Research Organisations:

A Handbook of Global Case Studies

Jinho Chung, Karl Dewey, Professor Christopher Hobbs, Dr Zenobia Homan, EunBee Park, Dr Ross Peel, Emma Scott and Dr Sarah Tzinieris

2022

Contents

**Note that this case study was completed in January 2022*

Glossary

APPRE	Act on Physical Protection and Radiological Emergency (in South Korea)
ATAS	Academic Technology Approval System (in UK)
AURPO	Association of University Radiation Protection Officers (in UK)
BEIS	Department for Business, Energy and Industrial Strategy (in UK)
CoE	Centre of Excellence
CPNI	Centre for the Protection of National Infrastructure (in UK)
CPPNM/A	Amendment to the Convention on the Physical Protection of Nuclear Materials
CTSA	Counter Terrorism Security Adviser (in UK)
DoE	Department of Energy (in US)
DSECU	State Service of Export Control of Ukraine
ECG	Export Controls Group
HASS	High-activity sealed source
HEU	Highly enriched uranium
HSE	Health and Safety Executive (in UK)
IAEA	International Atomic Energy Agency
ICP	Internal compliance programme
IND	Improvised nuclear device
INR	Institute for Nuclear Research (in Ukraine)
INSA	International Nuclear Nonproliferation and Security Academy (in South Korea)
IPPAS	International Physical Protection Advisory Service
ITC	International Training Course (in South Korea)
ISO	International Organization for Standardization
ITAR	International Traffic in Arms Regulation (in US)
KEPCO	Korea Electric Power Corporation
KINAC	Korean Institute of Nuclear Nonproliferation and Control
LEU	Low enriched uranium
MECR	Multilateral Export Control Regime
MTCR	Missile Technology Control Regime
NAS	National Academy of Sciences of Ukraine
Necsa	South African Nuclear Energy Corporation
NRC	Nuclear Regulatory Commission (in US)
NRE	Georgia Tech School for Nuclear and Radiological Engineering
NSCP	Nuclear Security Culture Programme (in UK)
NSG	Nuclear Suppliers Group
NSS	Nuclear Security Series
NSSC	Nuclear Safety and Security Commission (in South Korea)
NTP	Nuclear Technology Products (radioisotope distributer)
ORIA	Office of Research Integrity Assurance (in US)
ORNL	Oak Ridge National Laboratory
OSPS	Purdue University Office for Sponsored Programmes Services
PI	Principal Investigator
PITA	Act on Prevention of Divulgence and Protection of Industrial Technology (in South Korea)
REM	Purdue University Radiological Environmental Management Group
TCP	Technology Control Plan
UK	United Kingdom
UNSCR	United Nations Security Council Resolution
US	United States
UUK	Universities UK
WINS	World Institute for Nuclear Security
WMD	Weapon of mass destruction
9/11	Terrorist attacks of 11 September 2001

Acknowledgements

This handbook was developed through the UK's Nuclear Security Culture Programme (NSCP), implemented by a King's College London-led, academia-industry consortium and sponsored by the Department for Business, Energy and Industrial Strategy (BEIS). Other consortium members include Nuclear Transport Solutions – a specialist nuclear transport company; and Amport Risk – a nuclear security and resilience consultancy. The authors are grateful for the support provided by UK government under this programme and to the interviewees from the six organisations under study: Georgia Institute of Technology; the South African Nuclear Energy Corporation (Necsa); Purdue University (PU); the Korea Institute of Nuclear Nonproliferation and Control (KINAC); the National Academy of Sciences of Ukraine (NAS) and King's College London. Thanks also to Madeleine Ryan, Sally Horspool and Amelie Stötzel for their help in producing the handbook.

Executive Summary

This handbook explores, through a series of case studies, how security systems have been developed within universities and research institutes to protect (from both state and non-state actor threats) nuclear and radiological materials, as well as related sensitive information, knowledge and technologies. It seeks to examine the challenges in implementing different security measures in these environments and how these can be overcome, identifying where possible transferable good practices, with a focus on organisational level initiatives.

Given the diversity of academic and research institutions worldwide, the case studies presented here should not be considered as comprehensive; instead analysis of these cases seeks to provide deeper practical insights into this relatively unexplored area of nuclear security. Key lessons from these case studies are summarised below:

- Organisations may benefit from the establishment of dedicated units to oversee and promote compliance with export controls and other security areas. Working across different departments, this can provide a useful single point of contact for enquiries, while functioning as a central hub for advice and training. In staffing these units it may be beneficial to bring in not just security specialists but also those with research experience. The Georgia Institute of Technology in the US, as discussed in the case study below, has established an Export Control Coordinator Initiative, through which academics and researchers are seconded to their Office of Research Integrity Assurance and tasked with reviewing new projects. This approach was deemed to be vital in assessing the security risks posed by new research, while also beneficial in helping bridge the gap between the academic and security communities.

- When an organisation lacks an existing export control system and wishes to implement measures to address risks, it may be counterproductive to introduce a complete suite of measures simultaneously. Indeed, trying to do too much is liable to create an excessive burden on staff. Small but effective measures that can be taken include visible commitments from senior leaders to compliance, raising of awareness within the organisation, and hiring and/or training a suitable number of export controls advisors. These measures can then be grown over time to ensure greater compliance.

- Sensitive information can be protected by putting in place procedural steps such as checklists and control plans to protect export-controlled items and technology, sensitive materials, and intellectual property, as well as information sharing practices, all of which should typically be reviewed on an annual basis. Researchers may initial view security controls as a burden to their work, or even contrary to academic freedoms and the spirit of research, and may choose to avoid compliance measures rather than engaging with them. As such it is vital that institutional compliance practices are presented appropriately, and that a culture is fostered which encourages compliance through awareness raising and other measures.

- Beyond training on export control laws and regulations, a robust compliance programme involves personal outreach and proactive initiatives by the export control team to researchers, including direct collaboration aimed at identifying likely issues and developing solutions which will enable their work. Organisations should also work closely with their national competent authorities when designing and implementing internal compliance programmes to help ensure these meet all required standards and best practice.

- It can be useful for academic and research organisations to share with their staff information on past security-related incidents. This will serve to ground security-related threats and responses, helping individuals to contextualise such incidents in their own working environments. In order to avoid revealing sensitive personal information, cases will have to be carefully anonymised, while at the same time ensuring they are sufficiently detailed so useful lessons can be learnt.

- Universities' fundamental operating principles of open campus and academic freedom can create challenges when implementing certain security measures, particularly those that relate to limiting physical access and the exchange of information. These must be carefully managed, with the importance of security promoted by university leadership, and facilitated through organisational structures, but also grown from the bottom-up. As demonstrated by the case study on King's College London, this can be achieved through informal initiatives aimed at engaging academics and researchers on security issues and providing them with opportunity to shape new controls and ways of working.

- Challenges can often occur when users are working with controlled information relating to radioactive materials, since data is sometimes perceived (erroneously) as a lesser security risk as compared to the physical risks of radioactive materials going out of regulatory control. Although the institution will need to ensure that the cumulative security of its radioactive materials is not compromised, licensees may have to devise a more flexible security arrangement and mitigate risks by scaling up other security measures.

- Developing a broader organisational culture of security is key to combating nuclear security risks in universities, research institutes and indeed other organisations. Here it is common for security to lag behind safety in terms of prominence and staff engagement, with safety culture a more well-established concept. Consequently, organisations should work to promote that security and safety go hand in hand, through joint awareness raising and training activities and the potential extension of existing safety-related systems to include security.

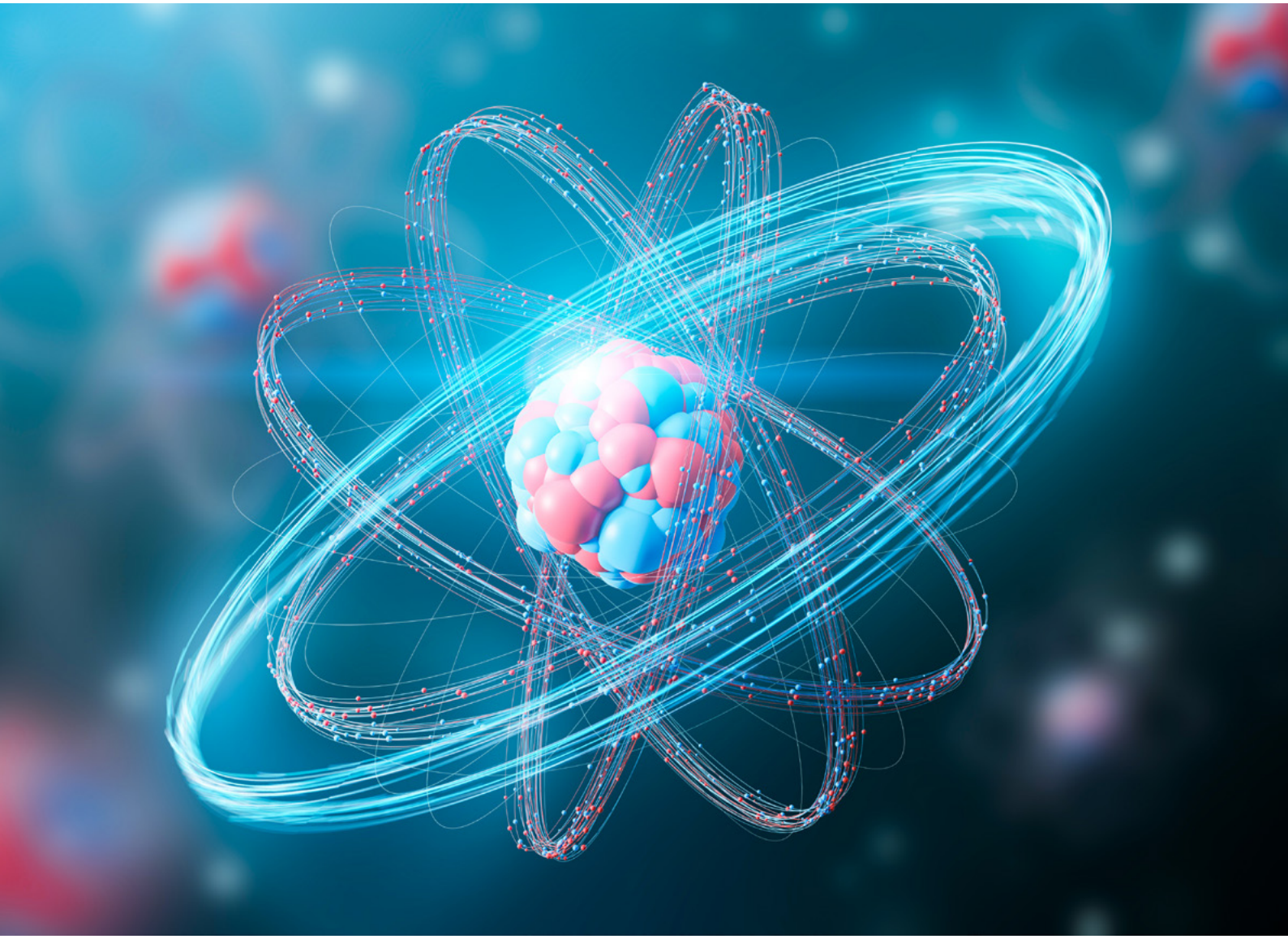
- Regular self-assessment is an essential component of security culture programmes, as this enables areas of strength and weakness to be identified so good practices can be shared and resources concentrated on elements that need additional support. However, in academic and research organisations security culture is a relatively new concept and there have been only a limited efforts to carry out assessments. Consequently, this is an area to which organisations should consider devoting additional focus, drawing on international and national guidance and best practice to inform new initiatives.

- Although states cannot compel organisations to foster an effective nuclear security culture, national implementation guides on nuclear security culture nonetheless provide a useful focal point of standards and normative expectations. Indeed, as the case study on the Korea Institute of Nuclear Nonproliferation and Control (KINAC) shows, government authorities can actively support organisations in their development of effective nuclear security culture. After establishing expectations, the state can continue to encourage organisations to foster effective nuclear security cultures by engaging with stakeholders to comply with guidelines, while also emphasising the impact of poor culture during routine regulatory activity. Engagement efforts can be further supported through the provision of education and training programmes. These may be done within organisations, or centrally through the establishment of national training academies.

Research Approach

This handbook presents new empirical research on how nuclear security programmes have been developed by universities and research institutes. It draws on semi-structured interviews, conducted in 2020 and 2021, with a number of professional services and academic staff at six different institutions involved in the implementation and review of security programmes. The interviewees were asked about their organisation's approach to security, how this has evolved over time, the challenges encountered and what initiatives have been successful.

The handbook continues by introducing nuclear-related risks, examining briefly how, why and the different ways that malicious actors may seek to gain access to materials, systems, technologies and information. The potential consequences of these actions are also discussed, with a focus on the individuals and organisations involved. Attention then turns to how security measures can be enacted to mitigate against these risks, examining key international initiatives, national levels efforts and the implementation of security at the organisation level. Key concepts from these introductory sections are then utilised to analyse the six case studies contained in this handbook.



Nuclear Security-Related Risks

Historically, concerns around the security of nuclear assets have been framed in terms of countering state-level proliferation. Indeed, analysis of past cases demonstrating that nuclear weapons programmes are rarely indigenous and typically draw on a range of actors in order to acquire relevant materials, technologies and know-how.[1] Support may be explicit, for example, in the Soviet Union's provision of scientific and technical assistance support for China's nuclear weapons development, from 1954 to 1960, or concealed, with organisations unwitting parties to proliferation activities.[2] For example, the AQ Khan illicit proliferation network, which operated from the 1980s to the early 2000s, involved a number of commercial manufacturers and suppliers that may have been unaware that the dual-use and nuclear equipment they developed and transported were destined for nuclear weapons programmes.[3]

Assistance can also be indirect, for example, scientists and engineers studying or working abroad in an effort to acquire fundamental nuclear knowledge and skills for later redirection to nuclear weapons development. This has been well-documented in the cases of Libya and Iraq, where nationals purposely undertook advanced nuclear-related degrees at universities in the UK and the US in the 1970s and 1980s, before entering weapons programmes upon their return.[4]

More recently, concerns have extended to include the possibility of nuclear terrorism, through the acquisition of a crude nuclear capability by non-state actors.

Here attention has focused predominantly on securing key nuclear materials, in particular highly enriched uranium (HEU) and plutonium, whose production is widely believed to be beyond the capability of non-state actors.[5] Although acquisition of sufficient quantities of HEU or plutonium would be a highly significant step towards the development by terrorists of what is commonly referred to as an improvised nuclear device (IND), specialist equipment, knowledge and skills would also be needed to weaponise this material.[6] Beyond the development of an IND, the concept of nuclear terrorism encompasses other potential scenarios including the attacks on nuclear facilities in an effort to trigger a radioactive release, as well as the acquisition of non-nuclear radioactive materials for use in so called radiological weapons, commonly referred to as 'dirty bombs'.[7] Relevant radioactive materials are far more widespread than nuclear materials and can be found in industry, hospitals, universities and research institutions.

It should also be stressed that not all non-state actor threats are proliferation-driven. There exists numerous examples where nuclear materials, technologies and sensitive information has been stolen and systems sabotaged, by individuals motivated by financial gain, disgruntlement, ideological reasons and psychological issues.[8] Many of these attacks have been carried out by 'insiders' – employees of organisations with authorised access to nuclear or radiological assets.[9]

1 Leonard S. Spector and Egle Murauskaite, 'Introduction and Overview', *Countering Nuclear Commodity Smuggling: A System of Systems*, James Martin Center for Nonproliferation Studies (CNS), 2014. http://www.jstor.org/stable/resrep09900.8

2 Ibid.; and Zhihua Shen and Yafeng Xia, 'Between Aid and Restriction: The Soviet Union's Changing Policies on China's Nuclear Weapons Program, 1954-1960'. *Asian Perspective*, vol. 36, no. 1, Proquest, 2012, pp. 95-122. https://www.proquest.com/scholarly-journals/between-aid-restriction-soviet-unions-changing/docview/1010324050/se-2?accountid=11862

3 David Albright and Corey Hinderstein, 'The A. Q. Khan Illicit Nuclear Trade Network and Implications for Nonproliferation Efforts, *Strategic Insights*, vol. V, no. 6, July 2006.

4 Wyn Q. Bowen, 'Chapter two: Proliferation Pathways', *The Adelphi Papers*, vol. 46, no. 380, pp. 25-46; Barbara Crossette, 'Expert Says Iraq Got Bomb Data from U.S.' *New York Times*, 23 March 2000.

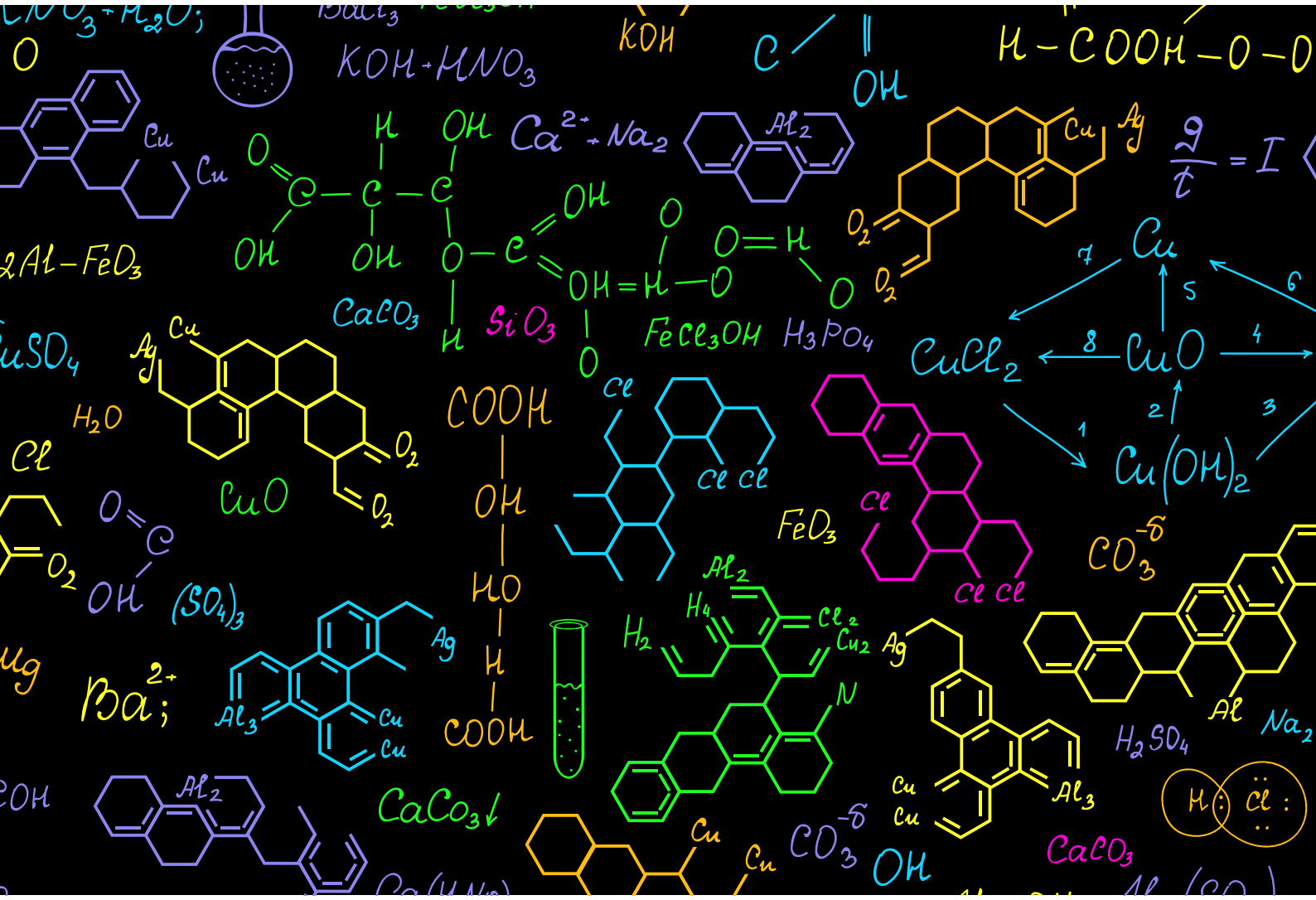
5 Jeffrey Boutwell (ed.), 'Nuclear Terrorism: The Danger of Highly Enriched Uranium (HEU)', Pugwash Conferences on Science and World Affairs, vol. 2, no. 1, September 2002. https://pugwashconferences.files.wordpress.com/2018/02/200209_issuebrief_nuclearterrorheu.pdf

6 Peter D. Zimmerman and Jeffrey G. Lewis, 'The bomb in the backyard', *Foreign Policy*, vol. 157, 2006, p. 33.

7 William C. Potter, Charles D. Ferguson and Leonard S. Spector, 'The Four Faces of Nuclear Terror: And the Need for a Prioritized Response', *Foreign Affairs*, vol. 83, no. 3, 2004, pp. 130-132. https://doi.org/10.2307/20033982

8 For case studies on insider threats see: Christopher Hobbs and Matthew Moran, 'Insider Threats: An Educational Handbook of Nuclear and Non-Nuclear Case Studies', *King's College London*, 2015, pp. 1-40.

9 Matthew Bunn and Scott D. Sagan (eds.) *Insider threats*, Cornell University Press, 2017.



Acts may also be driven by industrial espionage where organisations seek to acquire trade secrets and proprietary information in order to gain a commercial advantage.[10]

The consequences of successful state-level proliferation, the detonation of an IND by a terrorist group or the purposeful spreading of radioactive materials over a highly populated area are potentially devastating. However, even if these events do not ultimately occur there can nevertheless be a significant negative impact on organisations and individuals that fail to protect sensitive nuclear assets.

For example, in the US researchers and academics have been prosecuted and, in some cases, imprisoned for transferring sensitive dual-use technologies and information to other states.[11] Meanwhile, organisations can suffer financial and operational costs, as well as broader reputational damage. Here there exist numerous examples of research institutions and universities where the loss of nuclear and radiological materials has been subsequently reported by the mainstream media.[12] National regulators also typically have the power to fine organisations that fail to protect nuclear and radiological materials and in extreme some cases revoke licences.[13]

10 Noelle Camp and Adam David Williams, 'A New Approach to Insider Threat Mitigation: Lessons Learned from Counterintelligence Theory, Department of Energy Office of Scientific and Technical Information (OSTI), 1 June 2020. https://www.osti.gov/biblio/1798557

11 See, for example: The United States Department of Justice, 'Retired University Professor Sentenced for Four Years in Prison for Arms Export Violations Involving Citizen of China', *Justice News*, 1 July 2009. https://www.justice.gov/opa/pr/retired-university-professor-sentenced-four-years-prison-arms-export-violations-involving; Sara Coble, 'Raytheon Employee Jailed for Exporting Missile Data to China', *Info Security,* 19 November 2020. https://www.infosecurity-magazine.com/news/wei-sun-jailed-for-exporting

12 See, for example: *BBC News*, 'Idaho State University faces fine for losing plutonium,' 4 May 2018. https://www.bbc.co.uk/news/world-us-canada-44007709

13 International Atomic Energy Agency, 'Combating illicit Trafficking in Nuclear and other Radioactive Material,' IAEA Nuclear Security Series, No.6, Vienna, 2007, p. 95. https://www-pub.iaea.org/mtcd/publications/pdf/pub1309_web.pdf

Securing Nuclear Assets in Academic and Research Environments

A wide range of initiatives have been developed over time in an effort to combat the risks outlined in the last section. At the international level there exists a complex web of tens of multilateral and bilateral treaties, United Nations Security Council Resolutions (UNSCR), international governmental organisations, regional institutions and political commitments.[14] One of the most central and wide-ranging of these is UNSCR 1540, passed in 2004 in an effort to prevent the terrorist acquisition of weapons of mass destruction (WMD).[15] This dictates that states: refrain from providing support to non-state actors – including education and know-how; construct systems for the physical protection and accounting of sensitive materials; establish border and export controls on technologies – both tangibles and intangibles; and put in place criminal or civil penalties for violating the aforementioned measures.[16]

At the national level, international treaties, informal initiatives and guidance are translated into legislative and regulatory systems focused on protecting nuclear and radiological materials, facilities, technologies and information. For example, states may pass and enforce laws that criminalise the unauthorised possession of nuclear materials and trespass on nuclear sites, in an effort to deter such actions.[17] States will also empower regulatory bodies to ensure that holders of nuclear and radiological assets have developed and tested security plans and measures capable of withstanding a wide range of different attacks.

The types of measures implemented will vary across countries and organisations but will typically include limiting access to sensitive areas and systems and establishing physical protection, information and cyber security systems so that the actions of adversaries are detected, delayed and appropriately responded to.

As part of these national efforts, states may operate vetting systems aimed at excluding potentially untrustworthy individuals with certain high-risk characteristics. For example, in the UK the Academic Technology Approval System (ATAS) has operated since 2007 in an effort to prevent the dissemination of knowledge and skills that could be used to build advanced conventional military technologies or WMD.[18] Under this system students and academic researchers from particular countries seeking to pursue certain advanced scientific and technical degrees or conduct research in sensitive areas at UK universities and research institutes are required to undergo screening aimed at validating their reason for studying or working in the UK.

Recognising ever-increasing international collaboration in science and technology, in both the public and private sectors, states have sought to develop controls on strategic goods and technologies (collectively referred to as 'export controls').[19] Such efforts are aimed to prevent transfers that could, in the context of this report, support foreign states and non-state actors from developing nuclear or radiological weapons. Export controls apply to both tangible and intangible items including physical goods but also software, data and know-how.

14 Benjamin Kienzle, 'Atoms untangled: Examining the implications of 'regime complexity' in the fight against the proliferation of nuclear weapons', 2017 International Studies Association Annual Convention, Baltimore, 24 February 2017.

15 Benjamin Kienzle, 'Effective Orchestration? The 1540 Committee and the WMD Terrorism Regime Complex,' *Global Policy*, vol. 10, no. 4, November 2019, pp. 486-496.

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

17 See, for example: United Kingdom, Terrorism Act 2006, section 9-12, 13 April 2006. https://www.legislation.gov.uk/ukpga/2006/11/part/1/crossheading/offences-involving-radioactive-devices-and-materials-and-nuclear-facilities-and-sites/scotland/2006-03-30?view=plain

18 Government of the United Kingdom, 'Guidance: Academic Technology Approval Scheme (ATAS)', Foreign, Commonwealth & Development Office, 25 March 2013. https://www.gov.uk/guidance/academic-technology-approval-scheme

19 John Helferich, *Arms Export Controls under Siege of Globalisation: Defeated Nation States or Voluntary Surrender?* Tectum, Baden-Baden, 2020, p. 1.

Under these systems, organisations and individuals are required to apply for and obtain a licence before, for example, shipping a physical item to an entity in another country or transferring research data to a collaborator at a foreign university or research institute.

Detailed controlled item lists have been developed by international organisations and national governments to support individuals and organisations in determining whether or not they should apply for an export control licence.[20] These are supplemented by end-use controls which can be invoked on any item, even if it does not appear on control lists.[21] Here a more complex determination must be made as to whether the item might nevertheless be utilised in a weapons programme.

The above measures apply to all organisations, although are arguably most challenging to effectively implement in academic and research institutions. These challenges stem from both the nature of the work undertaken and several competing pressures that may serve to undermine security efforts. For example, many universities promote an 'open campus' model where sites are treated as public spaces within which individuals can come and go freely and within which physical security measures are necessarily limited.[22] In addition, a core principle of working at a university or research institute is that of 'academic freedom', based on open inquiry and the exchange of ideas and information.[23] This can serve to create tensions with efforts to restrict both access and exchange of information on security or other grounds.

Given these challenges, it is essential that universities and research institutes carefully assess and manage risk in this area so that they can effectively protect not just their sensitive assets, but also their broader values, international partnerships and ways of working. In the context of the UK, Universities UK (UUK) has produced guidelines to support this process, which provide both a framework and different hypothetical scenarios for organisations looking to develop resilience in this area.[24] This is complemented by the Trusted Research Guidance for Academia, developed by the UK's Centre for the Protection of National Infrastructure (CPNI), which seeks to support organisations in protecting their intellectual property, sensitive research and personal information while undertaking international scientific collaboration.[25] To be effective, the principles and recommendations enshrined within these documents need to be considered within and tailored to different organisational contexts. It is hoped that the case studies presented within this handbook provide useful practical examples of how this may be achieved.

20 See, for example: Government of the United Kingdom, 'Guidance: UK Strategic Export Control Lists', Department for International Trade, 3 August 2012. https://www.gov.uk/guidance/uk-strategic-export-control-lists-the-consolidated-list-of-strategic-military-and-dual-use-items#where-do-the-control-lists-originate; Nuclear Suppliers Group, Annex of the 'Guidelines for Transfers of Nuclear-related Dual-use Equipment, Materials, Software, and Related Technology', June 2019. http://nuclearsuppliersgroup.org/images//2019NSG_Part_2.pdf

21 Government of the United Kingdom, 'Guidance: Export controls: dual-use items, software and technology, goods for torture and radioactive sources', Export Control Joint Unit, 24 September 2019. https://www.gov.uk/guidance/export-controls-dual-use-items-software-and-technology-goods-for-torture-and-radioactive-sources

22 Richard Calvert, 'Open to all? Using our physical and digital spaces to better engage local communities' *THE Campus*, 28 June 2021. https://www.timeshighereducation.com/campus/open-all-using-our-physical-and-digital-spaces-better-engage-local-communities

23 Liviu Andreescu, 'Individual academic freedom and aprofessional acts', *Educational Theory*, no. 59, 2010, p. 2.

24 Universities UK (UUK), 'Managing Risks in Internationalisation: Security related issues', website of UUK, 11 August 2021. https://www.universitiesuk.ac.uk/what-we-do/policy-and-research/publications/managing-risks-internationalisation

25 Centre for the Protection of National Infrastructure (CPNI), 'Trusted Research Guidance for Academia', website of the CPNI, 4 January 2022. https://www.cpni.gov.uk/trusted-research-guidance-academia

Case Study 1 – Georgia Institute of Technology: Security Culture Leadership and Reinforcement

Organisation Overview

The Georgia Institute of Technology, commonly referred to as Georgia Tech, is a public research university and institute of technology in Atlanta in the state of Georgia, United States (US). Founded in 1885, Georgia Tech first opened its doors to students in 1888. Initially focused on supporting the adoption of industrial trades in the Southern US, it expanded its scope during its first 50 years to include advanced technological and scientific research. Georgia Tech also supported the US efforts in World Wars One and Two, during which time it saw a dramatic increase of sponsored classified research, both from industry and federal government.[26] More recently Georgia Tech has sought to expand from its core national security work into broader academic research. Thus, since its early days, security issues have been embedded in research conducted by the Institute.[27]

Georgia Tech conducts a wide range of technology-focused research and teaching, offering degrees in computing, the natural sciences and engineering. This includes nuclear-related work, within its College of Engineering's School for Nuclear & Radiological Engineering (NRE).[28] NRE has undergraduate students, graduate students and faculty members involved in its teaching and research programmes. It has both experimental as well as computational facilities with activities that cover everything from advanced reactor designs to nuclear non-proliferation to the study of forensic signatures as part of the nuclear fuel cycle to medical physics.[29] Members of NRE work closely with a number of US national laboratories and government agencies and lead a consortium which explores how advanced technologies affect nuclear non-proliferation.[30]

Export Controls' Awareness Raising and Training

Given that classified research has been undertaken at Georgia Tech for a long time, it is not surprising that Georgia Tech has a robust export control compliance programme in place. This is delivered through the Office of Research Integrity Assurance (ORIA) and encompasses all activities within the Institute. The approach taken by the ORIA is personal, proactive and collaborative, when it comes to sensitising academics and researchers to potential security risks.[31] For example, when new researchers join Georgia Tech, the export control team within ORIA reach out to them individually to introduce themselves and the function of their office, while also sending across dedicated educational and training resources.[32] The export control team also tries to work with researchers to help facilitate their work by identifying and seeking to develop solutions to potential issues, as opposed to implementing a prescriptive framework of what individuals should or should not do.[33]

As part of this engagement, new researchers receive training and mentorship from ORIA, with the export control programme offering a training course twice a month.[34] This provides a high-level overview of federal laws governing export control as they relate to Georgia Tech, detailing how to contain an uncontrolled research programme within the 'Fundamental Research' exemption, and how to protect research programmes that fall outside of this with a 'Technology Control Plan' (TCP).[35] This two-hour training makes use of real export control violation cases available via the Department of Justice website as well as internally developed hypothetical examples.[36]

26 'History of Georgia Tech', WikiMili, 7 April 2019. https://wikimili.com/en/History_of_Georgia_Tech

27 Director of Research Integrity in discussion with the author, July 2020.

28 Georgia Tech, 'Schools of the College of Engineering', website of *Georgia Tech*. https://coe.gatech.edu/schools-college-engineering

29 Chair of Nuclear and Radiological Engineering and Medical Physics Programme in discussion with the author, December 2020.

30 Georgia Tech, 'Kickoff Meeting Launches Consortium for Enabling Technologies and Innovation', website of Georgia Tech, 2012. https://web.archive.org/web/20210124210208/https://www.me.gatech.edu/etikickoff

31 Ibid.

32 Ibid.

33 Ibid.

34 Ibid.

35 Georgia Tech, 'Export Control: Education and Training', website of Georgia Tech. https://researchintegrity.gatech.edu/export-control/education-and-training

36 Director of Research Integrity in discussion with the author, July 2020.

Every relevant team member in a sensitive research area, such as aerospace engineering or nuclear engineering, must complete export control training shortly after joining Georgia Tech. Tailored export control classes are also available for certain laboratories working on sensitive topic areas, and supervisors are asked to encourage their staff to go on this training. The training also addresses penalties for violations of export control regulations with a focus on institutional error versus the individual intent of the researcher (i.e., was it the intention of the researcher to go against the Institute's policies and procedures?). Finally, the training encourages researchers to approach the ORIA with any questions should they have any as they progress their research.[37]

In an effort to further bridge the gap between the compliance and research teams, Georgia Tech has established an Export Control Coordinator Initiative. This initiative covers 50% of an academic or researcher's time to take on a facilitation role between the two groups. Staff employed through this initiative have understanding of both the technical and export control issues, and therefore are extremely well-placed to assess the security risks posed by new research. They also assist with both reviewing research projects for export control issues, and with talking to other academics to spread the message of the need for compliance with export controls. At the time of writing, there were six Export Control Coordinators in place at Georgia Tech.[38] The work of these coordinators is supported by dedicated export control officers, who receive considerable training in this area, including by the Society for International Affairs and the Export Control Compliance Training Institute – a world leader in US export control compliance, which offers dedicated export control training for universities.[39]

Protecting Sensitive Information

Georgia Tech assesses every sponsored research project from the proposal stage onwards for export controls matters and other intellectual property concerns. As part of the proposal submission process, a checklist covering everything from export controls to intellectual property, to use of nuclear radiological materials and other technologies, as well as research involving human subjects must be completed.[40] If the project proposal is successfully funded, an additional follow-on step occurs where the same questions are asked again. In cases where answers to any of those questions are yes or flagged as problematic, the researcher, scientist or engineer will be required to work with the export control team to identify what is potentially sensitive and how it can be managed.[41] Export control measures are established through the development of a TCP; this serves to define and limit access, addressing how the data should be used and handled, and where it should be stored. Everyone involved in the research project must sign the TCP before formally joining the project.[42]

In cases where external partners are involved in the research project, the ORIA checks that collaborators are not on the denied parties list nor a foreign military or defence entity. In the case that the external partner is a denied entity, the project process would be stopped.[43] If not, interaction across multiple institutions is managed by asking questions such as what are the best ways to communicate information? What are the right ways to share information in a protected manner? The answers to those questions are continually evolving and hence the processes in place must be revisited on an annual basis.[44]

37 Ibid.
38 Ibid.
39 Ibid.
40 Interviewee in discussion with the author, December 2020
41 Ibid.
42 Ibid.
43 Director of Research Integrity in discussion with the author, July 2020.
44 Chair of Nuclear and Radiological Engineering and Medical Physics Programme in discussion with the author, December 2020.

Security Vetting, Screening and Human Reliability

Not only is there a thorough review process for research projects, particularly for applied research projects, but there is also screening process in place for all individuals that apply to work at Georgia Tech. All applicants are screened against the denied parties' lists, and if any applicant features on such a list, they are of course not hired.[45] That said, certain foreign nationals can teach courses that are offered in the public domain and participate in 'Fundamental Research'. If the research conducted is not fundamental, Georgia Tech considers the individual's nationality, the technology being researched and, henceforth, the relevant export control regulations.[46] In particular, Georgia Tech must carefully manage all students within sensitive programmes which utilise export-controlled software. Here, there is a need to ensure the students are cleared for access when utilising these goods and understand how they should be used responsibly.[47]

Developing a Broader Security Culture

Like in many US institutions, efforts to grow a broader culture of security amongst the workforce at Georgia Tech have taken place over decades.[48] In this regard, Georgia Tech is perceived to have benefited from a strong historical leadership on security matters because many of its senior members have served in the military and spent their careers working in sensitive areas. Here security culture has been driven by the upper leadership at Georgia Tech, who have outlined and articulated clear expectations regarding export controls and the protection of sensitive information.[49] These messages have been cascaded through the organisation with junior staff expected to work closely with more senior team members on security issues, who in turn are required to ensure people are working in line with expectations.[50]

High-level messaging and direction are complemented by the aforementioned awareness raising and training, which is continually reinforced by presentations, lectures, seminars and other opportunities offered throughout the year. For example, staff at Georgia Tech have conducted visits to national laboratories, where they were given the opportunity to observe and discuss how they implement security.[51] There is also a range of well-established management and reporting systems which help facilitate correct actions and behaviours with respect to security. This includes regular audits of export and physical controls, aimed at ensuring that individuals are following proscribed rules and procedures such as those in place for handling and managing data.[52]

Georgia Tech also aims to instil the mindset of leading by example, and views this as one of the most important things when reinforcing security culture and good practices. Such leadership is expected to come from every office and person, whether that be the president of the Institute, faculty or student members setting examples for others. The view is held that if one individual is not compliant, it affects the hiring prospects of others, with emphasis placed on the importance of everyone representing Georgia Tech well.[53]

Managing Mistakes

In the event that mistakes occur, the submission of a voluntary disclosure agreement is strongly encouraged. Additionally, there is a requirement to disclose the mistake to the sponsor. In such a scenario, Georgia Tech would also undertake an internal review to determine how the mistake occurred in the first place, and whether there was potential intent by the academic or researcher to circumvent controls. In the case of deliberate intent, Georgia Tech would convene a panel to determine whether there was a conflict with the Institute's procedures.

45 Director of Research Integrity in discussion with the author, July 2020.
46 Ibid.
47 Chair of Nuclear and Radiological Engineering and Medical Physics Programme in discussion with the author, December 2020.
48 Ibid.
49 Director of Research Integrity in discussion with the author, July 2020.
50 Chair of Nuclear and Radiological Engineering and Medical Physics Program in discussion with the author, December 2020.
51 Ibid.
52 Ibid.
53 Ibid.

In worst-case scenarios, the individual's research activities could potentially be restricted, or the individual might even be fired.[54]

Summary and Conclusions

Georgia Tech has a well-established security culture developed over the course of a century. This culture although driven by a top-down approach depends on each individual assuming responsibility and setting the example for others. The support provided by ORIA to both incoming and established researchers is intrinsic to the success of the export control programme. Established processes and procedures for screening and protecting sensitive information have resulted in a research culture where all staff are aware of their obligations and the potential consequences should these advertently not be fulfilled.

To conclude, Georgia Tech is a leading example for institutes wanting to develop more robust security awareness and culture. It exemplifies the core components of an internal compliance programme for research involving sensitive items. These components include top level management and leadership; organisational structure, responsibility and the commitment of resources; training and awareness raising; export screening processes and procedures, performance reviews, audits and corrective action; and physical information and security.[55] In cases where mistakes are made, Georgia Tech can point to its significant efforts to comply, and that alone may result in limited admonition.

54 Director of Research Integrity in discussion with the author, July 2020.

55 European Union, 'COMMISSION RECOMMENDATION (EU) 2021/1700 of 15 September 2021 on internal compliance programmes for controls of research involving dual-use items under Regulation (EU) 2021/821 of the European Parliament and of the Council setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items', *Official Journal of the European Union*, L338/1, vol. 64, 23 September 2021. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L:2021:338:FULL

Case Study 2 – South African Nuclear Energy Corporation: Strengthening Organisational Culture

Organisation Overview

The South African Nuclear Energy Corporation (Necsa) is situated in the North West province of South Africa. Amongst its various responsibilities, the corporation runs SAFARI-1 ('Safari'), a light water-cooled, pool-type research reactor which first reached criticality in 1965. Initially fuelled by highly enriched uranium (HEU), the reactor was converted to low enriched uranium (LEU) in 2009. SAFARI-1 is used for research and the production of radioisotopes (specifically molybdenum-99). Originally part of the Pelindaba National Nuclear Research Centre, and later the Atomic Energy Corporation, SAFARI-1 was transferred to Necsa following the Corporation's creation in 1999.

Although this case study will focus primarily on the SAFARI-1 team and facility, Necsa's Pelindaba site is currently made up of a complex portfolio of subsidiaries including radioisotope distributer NTP ('Nuclear Technology Products'), fluorochemicals supplier Pelchem, and commercial division Pelindaba Enterprises – as well as departments for Research and Development, Operations, Nuclear Compliance and Services, Finance, Business and Development, and Corporate Services. The Pelindaba site, which lies in the middle of a nature reserve, covers 640 hectares of land inside its perimeter fence, which can be accessed via three separate gates. At the time of writing, the Necsa Group had around 2,200 employees, with around 2,000 people accessing the Pelindaba site on a daily basis.[56]

56 Necsa, 'Scaling down on number of Necsa staff on site due to the national disaster relating to Covid-19 virus', Necsa Coronavirus Statement, 23 March 2020. https://drive.google.com/file/d/1swjCbmo4G6VQxQp8-HNfkEWvlgnqvjG6/view

Over the last decade, Necsa has engaged with international partners such as Oak Ridge National Laboratory (ORNL) from the US and the UK's Nuclear Security Culture Programme (NSCP), with special attention paid to the fostering of effective nuclear security culture. Through this engagement and other initiatives, several interviewees noted how the organisation has "come to understand" that security and safety go hand in hand, whereas previously priority was given to safety, with security considerations given lesser attention.[57]

Incidents, Changing Threat Perceptions and New Security Approaches

The Necsa site has a long history relating to nuclear security and safety, which has attracted international attention from time to time.[58] Most prominently, in 2007, two armed incursions took place at Necsa.[59] Globally, this incident fuelled concern over Pelindaba because of its historical involvement in nuclear weapons-related work and use of HEU fuel in its reactor.[60] This incident prompted an internal review, with security measures subsequently upgraded to mitigate the risk of future breaches and to align with newly-introduced national regulations. For example, fences and physical barriers were strengthened and the emergency control centre at Necsa was upgraded to have a 24-hour presence.

Traditionally, emphasis at Necsa has been placed on upgrading physical security, aimed primarily at external adversaries, although 'insider threats' have also recently received increased attention. For instance, facility access procedures have been altered in an effort to reduce potential opportunities for employee thefts. Previously, once inside the Necsa site, it was possible to walk in and out of buildings without being challenged. Now, access to individual buildings requires passing through additional security checks such as bag scanners, metal detectors and turnstiles. Biometric scanners are also employed, along with cameras for continuous monitoring, and security guards are stationed at the entrances of all buildings.

In addition, there is a requirement that guests must be signed in and out and accompanied at all times.

Security Awareness Raising and Training

All new employees are required to complete an orientation session, as part of which they are introduced to the Safety, Health Environment and Quality (SHEQ-INS) system, which is included in Necsa's integrated management system. This includes the provision of several hundred documents that detail procedures and processes relating to a wide range of topics, such as security, conventional safety, emergency preparedness, electronics and housekeeping, and radiation protection. The broader Necsa Group has also established a 'Safety & Security Culture Forum', through which topics, relevant to safety and security are presented to staff. These presentations are then delivered at different organisations throughout the Necsa Group by safety and security culture 'ambassadors' within individual departments. For example, in response to the Covid-19 pandemic in 2020, sessions have been run on how this has changed the security risk landscape for Necsa. Presentations are prepared and sent out to the entire Necsa Group, with some departments make use of these as training material, adding supplementary questions in order to help ensure that the content is understood.

When people join the SAFARI-1 reactor team at Necsa, in addition to the company orientation programme, they also need to have an understanding of the different regulations and acts applicable to their work. These include the National Nuclear Regulations, the Occupational Safety and Health Act and the National Key Point Act.[61] As such, there are dedicated SAFARI-1 orientation sessions, specifically addressing SAFARI-1 documentation such as procedures, maintenance and policies. In addition to security exposure during orientation, the SAFARI-1 team runs regular awareness sessions twice a month, which last for 20 minutes at the start of the day.

57 Safety culture specialist in discussion with the authors, July 2020.

58 Micah Reddy, 'Another nuclear safety scare at Pelindaba as management fumbles', *news24*, 7 June 2018. https://www.news24.com/news24/southafrica/news/another-nuclear-safety-scare-at-pelindaba-as-management-fumbles-20180606

59 Noah Schachtman, 'Second Attack on South African Nuke Plant', *Wired*, 13 November 2007. https://www.wired.com/2007/11/second-attack-o; Douglas Birch and Jeffrey Smith, 'How intruders stormed their way into a South African nuclear plant', *The Washington Post*, 14 March 2015. https://www.washingtonpost.com/world/how-armed-intruders-stormed-their-way-into-a-south-african-nuclear-plant/2015/03/13/470fc8ba-579d-4dba-a0c0-f0a1ed332503_story.html

60 'Profile', website of Necsa, 2021. http://www.necsa.co.za/about-us/#:~:text=Nearly%20ten%20%20years%20later%2C%20in,to%%2020the%20then%20Pelindaba%20site

61 Applicable as SAFARI-1 has a Nuclear Installation Licence and is situated on a National Key Point site.

They also run separate stand-alone sessions throughout the year that address specific security issues of importance. Security training is compulsory and attendance is monitored. If employees consistently miss training, this can be escalated and result in disciplinary action being taken – unless satisfactory reasons for absence can be provided. A considerable benefit for the SAFARI-1 team within Necsa is that it has its own training facility. Safari security officers and other personnel have access to awareness raising material, security documents and training files. This kind of direct access has proven to be beneficial in helping the SAFRAI-1 team to develop its security culture, with several interviewees emphasising the benefits of a dedicated security department and training facility.[62]

The move to working from home, precipitated by Covid-19, revealed remote access inequalities. Necsa has needed to ensure reliable and secure digital access and connectivity across the organisation. However, within the SAFARI-1 team, connectivity issues are less acute and most staff do have computer and internet access. Here, the move to remote working has actually had a positive effect on attendance by SAFARI-1 staff at security training, which has risen from around 70% to 90%.[63] Now that onsite work has been reduced or adapted, staff have more flexibility to attend security training, which has circumvented a major obstacle – namely that staff members found it difficult to leave their posts and offices. This has been particularly impactful for shift workers and security officers, who had previously been amongst the most difficult to reach.

Security Vetting, Screening and Human Reliability

Like in other organisations, personnel security at Necsa begins with a security clearance process, including a criminal record check. This is administered utilising a graded approach, where the number of checks and clearances before starting work will increase in line with the staff member's level of responsibility and access to sensitive information and facilities. In addition to these initial checks, Necsa maintains mechanisms aimed at monitoring staff behaviour and flagging potential safety and security concerns.

Staff are encouraged to report poor behaviour through a Behavioural Based Safety (BBS) programme and an Event Management Programme (EMP). Analysing trends for individuals on both programmes helps ensure that concerning behaviours are identified and prioritised for action. In relation to security, this might include refusing to be searched at a checkpoint, or not wanting to make use of a turnstile, when accessing a sensitive part of the facility. Initially the staff member will receive a warning, although following repeated infringements this will result in a disciplinary process managed by Human Resources, through which more formal sanctions can be applied.

In an effort to further strengthen its human reliability programme, Necsa offers mental health services to its staff members, employing a company psychologist as well as an Employee Assistance Practitioner to help resolve any issues. NTP Radioisotopes has as psychologist with an 'open door' policy, where staff are free to book a consultation. This service also offers other routes through which to assess whether an individual is experiencing difficulties. In addition to supporting staff welfare, Necsa EAPs have an important security function to play. They identify if and when someone is potential threat to themselves or others. In these circumstances the EAP and NTP psychologist have the obligation to report the individual to their manager and the security team. Individuals are notified of this escalation, although care is taken to frame actions as a step in aiding that individual, removing negative or punitive connotations. EAP and NTP psychologists also seek to identify cases of broader work-related stresses, so that staff can be given time off when necessary. This is reflected in Necsa's official policy for staff in technical and hazardous roles – such as working with isotopes in NTP. According to this process, staff should be sent home when they are unwell and suffering from stress, rather than being pressured into fulfilling shift work.

In addition to formal procedures, Necsa staff make use of informal communication methods such as WhatsApp and text message groups to discuss staff welfare. The EAP and NTP psychologist are usually members of these groups and use them to stay in touch with everyone to make sure "no one falls through the cracks".[64]

62 Safari training and support team in discussion with the authors, October 2020.

63 Ibid.

64 Company psychologist in discussion with the authors, September 2020.

There are WhatsApp groups for both regular staff and managers. These groups contribute to an "unwritten buddy system", in which colleagues watch out for one another and report to either the team of psychologist or a manager when they are concerned about someone's behaviour.[65] It has also proven to be a useful way of identifying other potential signs of poor mental health, for example, when individuals are taking an excessive number of sick days. Maintaining contact has been more challenging during the Covid-19 pandemic, because, at its peak, only between one-third and half of personnel had been on site every day.[66] However, a combination of WhatsApp, Zoom and Microsoft Teams has been used to mitigate this. Seeing people on video calls or hearing their voice has been found to be particularly helpful.

Protecting Sensitive Information

When joining Necsa, all staff sign a confidentiality agreement. As part of their employment contract, staff also agree never to share any secret information. In addition, Necsa operates a digital information system, where access to certain documents will be restricted based on their level of confidentiality. These are stored on a protected server where access is limited based on factors such as job responsibilities and levels of security clearance. Additional restrictions around the use of intellectual property policies are also put in place when relevant. This is especially applicable to the research and development group, which does confidential commercial work, as well as staff working for NTP on isotope production. Necsa has also sought to develop a culture of sharing experiences, in order to help staff members visualise and learn from past mistakes. For example, in the (infrequent) event that sensitive information has been stolen or leaked, procedures require this incident to be included in quarterly presentation by the relevant senior manager in order to bring it to everyone's attention. This helps to remind people of the rules and regulations and prevent further infractions.

Necsa staff are also prohibited from using any 'outside' devices on their computers. For instance, all USB ports on computers and laptops provided by NTP are blocked. This has proven to be especially important during the shift to working from home due to Covid-19.

Basic cyber awareness sessions are also run for all staff, which cover different threats and key security principles. For example, how phishing can manifest in the work environment and the importance of regularly changing passwords. Similar to other office environments, access to sites via the internet is restricted and screened, with permission required to access webpages outside of those deemed relevant to everyday work.

Safety and Security Culture-Related Efforts

Safety culture at Necsa is relatively well-established and it is seen as the common basis through which security culture can be integrated. Since 2004, Necsa has run an 'Active Safety Culture Programme' including a 'Behaviour Based Safety Programme Initiative' aimed at lowering the overall injury rate of the company. This includes one in-person employee observation per month, in an effort to identify high risk behaviours – which are corrected as soon as possible. Since 2018, Necsa has also tried to include security in this programme, extending its observations to encompass security-related behaviours. Safety training now encompasses security issues, with compulsory site inductions also covering both. Although the programme has run since 2004, the programme is not universally popular. Some have called for review, suggesting that the programme be offered on an electronic platform.

Necsa already seeks to visibly incorporate safety culture into everyday processes and is using some of those tools to increase awareness of good security practice. For example, every meeting at Necsa begins with a 'safety and security moment', where relevant information is shared. Necsa also has an electronic event management system, in which staff can anonymously report any observed safety or security concerns. As an alternative, staff also have the option to call the relevant department to directly report concerns – which is the method used most frequently. Anecdotal evidence suggests this is an effective system, which is well-embedded for safety and it is increasingly being used to report security issues. For example, one interviewee described how another employee had observed an occasion where the gate to a sensitive facility had inadvertently been left open.[67] This was reported with the security weakness then immediately rectified.

65 Ibid.

66 Ibid.

67 Safety culture specialist in discussion with the authors, July 2020.

As previously noted, Necsa also seeks to share experiences as a sensitisation tool, and if anything suspicious is noted, it will be shared on the company intranet and also printed out and put on notice boards. This could be something such as an IT incident, or a person entering a building without the correct access authority. For example, interviewees recalled that in 2018, cleaners noticed someone in the NTP bathroom, who should not have been there. The person said they simply needed to use the bathroom. The cleaners wrote a letter to complain, and management re-affirmed that staff should not use facilities they are not assigned to. The reporting process worked well in this case: the cleaners felt responsible and the incident was followed up on and stopped immediately. Other examples of good safety and security culture awareness include people being called out when they try to take pictures on their phone, or if they are not wearing a face covering.

In an effort to further gauge its organisational culture with respect to safety and security, Necsa has conducted surveys, albeit, to date, focused largely on safety issues. Safety culture forms part of the internal Necsa audit process as well as inspections by the regulator, although these have been halted during the Covid-19 pandemic.[68] Currently, there is no regulatory requirement in South Africa for nuclear security culture. Nevertheless, increasing interest by the regulator in this area will help consolidate progress made at Necsa.

Challenges Encountered and Lessons Learnt

Necsa's move to promote a culture of security across its entire workforce is relatively new and here it is recognised that attitudes and behaviours cannot change overnight. Consequently, it is not surprising that security culture-related initiatives have encountered several challenges. These include securing greater management buy-in, so that the senior leadership – and the Board especially – can use their authority to drive change across the whole organisation. Interview data suggests that it has been challenging to incite enthusiasm for active participation at this level.

For example, as Necsa introduced new security measures and procedures after the 2007 incursion, it took time for senior staff members to become accustomed to these changes – which arguably slowed down adoption by the broader workforce.[69] However, following a concerted awareness raising and training campaign by the security team, staff have come to appreciate the new rules and measures in relation to security which were once seen as an inconvenience.[70]

In an effort to promote high-level engagement with, and support for, safety and security Necsa has sought to improve senior managers' technical understanding of these issues. Gaps there were brought to light following an independent International Atomic Energy Agency (IAEA) Safety Culture Audit, during August 2018, which revealed that the senior management level had only a general understanding of key procedures. As a result, a programme has been developed to enhance executive level knowledge of safety and security issues. Efforts have also been supported by external engagement, for example, participation by senior managers in workshops on nuclear security culture delivered by outside organisations. Senior staff are also invited to take part in in workshops on safety and security issues abroad, for example at the IAEA. In addition, managers are encouraged to participate in elements of Necsa's security culture programme, such as engaging with security-related observations. The engagement of management is seen as vital in providing support for the safety and security teams and driving greater collaboration across the organisation.

Challenges have also been encountered when it comes to sustaining staff engagement on security issues. As noted, when staff join the organisation, they must all complete a standard induction, which includes information on subjects such as site emergency preparedness arrangements and security. However, follow-up training typically does not vary significantly from what is received during induction. In general, training material is only altered when something changes in the facility. This has led to concerns being raised that material is repetitive and does not address "training fatigue".[71]

68 The South African nuclear regulator conducted a security culture survey at the end of 2019.

69 Safety culture specialist in discussion with the authors, July 2020.

70 Ibid.

71 Safari training and support team in discussion with the authors, October 2020.

To counter this, Necsa has sought to anticipate changes in the safety and security environment. For example, prior to South Africa's 2020 lockdown, the safety culture team organised a presentation on the likely impact of Covid-19 which was compulsory for everyone to attend. Typically, there are four presentations delivered like this per month on site on safety and security issues, which are adapted to what is happening at the time. For instance, during the aforementioned course, a focus was placed on presentations that deal with stress and mental health-related issues. The meetings are generally well-attended (around 70%-80% of personnel) and they are recorded on 'company score cards'. These are tabulated and staff must attend 75% of all presentations per year. Such fora are deemed to provide a good platform for continuous security awareness training and provide a natural pathway for Necsa to further embed security within its pre-existing safety and security culture.

A further challenge is reaching certain individuals, particularly those who do not have access to computer workstations. As safety and security presentations are distributed electronically, not all staff can access these. This particularly affects staff such as cleaners. Onsite computers have been made available for them, although it is difficult to control and monitor engagement. To address this, the most important safety and security presentations have been printed, laminated and put up onsite. In addition, broader efforts to share staff experiences in relation to security, including in-person observations, have also helped in socialising issues and increasing understanding amongst different teams.

As touched on earlier, for staff with good computer connectivity increased working from home has had mixed security benefits. On one hand, increased flexibility has improved staff availability for meetings, where security issues are discussed – including staff who work shifts or may otherwise be unavailable due to being sick or on leave. On the other hand, assessing learning uptake in a virtual setting has been problematic. Some of these safety- and security-related presentations are assessed (training), but others are not (awareness raising). It is possible to run an awareness raising presentation 'in the background' on a computer at home without fully engaging.

To compensate, training presentations are accompanied by questions that must be answered – and when answered incorrectly access to the Necsa site and buildings is restricted. For those who cannot take a test online, it is possible to take these in person onsite.

Necsa is still in the process of establishing a 'Challenge Culture' where staff adopt a questioning approach to any perceived security violations. Here, interviews suggested that while some people are vigilant and questioning, others do not feel the same level of responsibility to participate, and some lack the confidence to directly challenge others.[72] In some cases, it is apparent that incidents have not been reported because staff did not want to 'rock the boat' and be dragged into a subsequent investigation. Related to this, there is perceived concern that reporting is not completely anonymous – for example, as a result of the fact that many people work in small teams.

Summary and Conclusions

While it is an ongoing process at Necsa to reach all levels of staff, ever increasing numbers are becoming aware of the relevant security policies and documents. In the absence of a concerted 'top-down' effort, a 'bottom-up' approach has deemed to be relatively effective. This has strengthened compliance with security procedures, where staff are encouraged to respond to security at an individual level and every person feels like they can make a difference and to take responsibility. Organising training with other sites, facilities, countries and experts was deemed by interviewees to create positive energy and inspiration.[73] For example, interaction with ORNL and the UK's Nuclear Security Culture Programme drove the integration of safety and security, establishing a more holistic view of culture as a whole and not singling out safety or security by itself. Greater leadership support would likely further accelerate these efforts.

72 Safety culture specialist in discussion with the authors, July 2020.

73 Safari training and support team in discussion with the authors, October 2020.

Case Study 3 – Purdue University: Changing Threat Perceptions and Increased Focus on Security

Organisation Overview

Purdue University ('Purdue') is a public research university situated in the state of Indiana in the United States (US). The university was founded in the second half of the 19th century and has traditionally focused on disciplines relating to science, technology and agriculture. Located near Lafayette and West Lafayette, Purdue is a relatively rural university, with the local population making up most of Purdue's circa 46,000 students and 3,500 academic staff.[74] In addition, many local businesses are dedicated to the university's operation and thus the local population has a vested interest in its performance.

Uniquely, Purdue currently operates the only nuclear reactor (PUR-1) in Indiana. PUR-1 is an underground pool-type research reactor, which first reached criticality in 1962.[75] The PUR-1 research reactor is used for teaching and training related to reactor physics, and as a source for neutrons for research in nuclear engineering, chemistry and health sciences. Accordingly, the reactor has a relatively low power range and is licenced to operate only up to 12 kilowatts (thermal).[76] PUR-1 is also the first and only US Nuclear Regulatory Commission (NRC) facility to be licenced for a fully digital safety control system.

74 Data up to 2020.

75 'PUR-1 goals fully digital', *Nuclear Engineering International*, 14 November 2019. https://www.neimagazine.com/features/featurepur-1-goes-fully-digital-7507939

76 'Safety Evaluation Report – Renewal of the Facility Operating License for the Purdue University Research Reactor, PUR-1', Office of Nuclear Reactor Regulation, US Nuclear Regulatory Commission, October 2016. https://www.nrc.gov/docs/ML1626/ML16267A000.pdf

Largely due to Purdue's non-urban setting, security was historically not posited as a serious concern. However, in recent years, several security-related factors have converged to necessitate the development of stricter protocols and procedures. These are aimed at protecting both nuclear assets and sensitive research materials from misuse. Major drivers include the 9/11 terrorist attacks and increasing concern that non-state actors may seek weapons of mass destruction (WMD). As part of a nationwide effort, the federal government and the Department of Energy (DoE) introduced new measures universities should take to reduce risks and increase security. In the case of Purdue, this translated to the upgrading of physical protection systems, and in 2005 the university's reactor was converted from using highly enriched uranium (HEU) to low enriched uranium (LEU).

More recently – particularly over the past five years – civil and political unrest in the US, as well as an increasing number of incidents relating to radicalisation, have further elevated security issues within the local community. Purdue has consequently increased awareness raising on potential threats and the importance of nuclear security, integrating these topics into educational programmes and launching efforts to gauge and enhance security culture.[77]

Security Awareness Raising and Training

Although the Radiological Environmental Management Group (REM)[78] has sought to raise general awareness of nuclear and radiological threats across the entire campus, it has proven to be a challenging exercise. This stems from the breadth of activities of conducted by Purdue, the majority of which do not involve nuclear or radiological materials. As such, people on campus are generally unaware that the radiological and nuclear materials present can be used for malicious purposes, and do not understand what the potential threats arising from their presence are.[79] While the users of these materials have traditionally focused their attention on risks in relation to safety rather than security.[80]

Specific nuclear security-related training offered to academics, researchers and professional service staff at Purdue depends on their role and responsibilities. However, all personnel engaged in activities with hazards (i.e., using biological, chemical or radioactive materials) are required to undergo training. At the time of writing, there were approximately 400 people at Purdue who worked with radioactive materials on campus. While the majority of those materials are very low category materials (mainly category five), these users must nevertheless go through REM training. However, the security aspects of REM training are relatively limited for most users. For example, these include emphasising the importance of keeping stores and rooms locked and identifying and reporting suspicious behaviours. In addition, anybody who conducts related research also has to take responsible conduct and research training which covers the related areas of ethical behaviour and research integrity.

Security-related engagements for higher category radioactive material is more in-depth. Anyone on a control plan (see below) is required to participate in a series of trainings including data security training (valid for one year) and export control training (valid for five years). Here individuals must show mastery of these materials through extensive documented use and testing. For those new to Purdue, individuals must either take an additional course given by REM (40 hours, which includes safety and security concepts) or enrol in a comparable course offered, for example by the US NRC or by one of the US National Nuclear Laboratories. The university's Radiation Safety Committee (RSC) reviews all applications for authorised user status and can also recommend additional training. The highest level of security training is reserved for a handful of individuals responsible for working on the reactor and associated irradiation laboratories. This training also covers requirements for protecting sensitive information, human reliability vetting and drug testing.

77 Associate Dean and Professor in discussion with the authors, June 2020.

78 Under the Board of Trustees and the President of Purdue University, there are a number of Executive Vice-President (EVP) offices and under those, Vice President (VP) offices. REM falls under the EVP for Business and Finance (Treasurer) and then VP for Physical Facilities. Many US universities choose to have research and facilities (covering safety and security) separate so there are no conflicts of interest. This is Purdue's approach. Being under the Treasurer also ensures greater awareness and visibility for meeting financial obligations needed for safety and security.

79 Data from multiple interviews, June-September 2020.

80 Max Boholm, Niklas Möller and Sven Ove Hansson, 'The concepts of risk, safety, and security: applications in everyday language', *Risk analysis* vol. 36, no. 2, 2016, pp. 320-338.

Security Vetting, Screening and Human Reliability

Users of radioactive materials are also subject to regular vetting, which serves to further raise awareness and understanding of security issues. Vetting is handled by the university working with the NRC and the country's Federal Bureau of Investigation (FBI). Individuals passing through vetting will typically complete a security-related questionnaire and may be asked to participate in interviews aimed at further assessing their suitability for working with sensitive assets. This is conducted based on a graded approach, where the sensitivity of an individual's work is assessed and then associated with a commensurate level of vetting. Vetting requirements at Purdue apply to both staff and students, the latter of whom must be appointed to work on sponsored research projects related to nuclear and radiological materials. As such, they are considered employees and bound by contract conditions. Non-contracted volunteers do not have to pass through vetting and are consequently prohibited from working on such projects. More broadly, all new members of staff must also undergo a basic Human Resources background check.

Any new research project that is funded through external (non-Purdue) funds goes through a checklist (Sponsored Programs Services Proposal Worksheet). A number of screening questions are asked and an appropriate office (such as REM) may investigate these further depending on the responses. This process includes a background check against 'restricted party lists' from the US and several other countries such as Australia and Japan. The aim of this process is to understand why a proposed project partner may be on a list, so that this can be addressed with the researcher in a conversation. For example, a specific international institute may have been on a foreign list for several years, but only recently featured on the US Entities of Concern list. This could be due to a direct violation of US export control laws – for instance, an association between the institute and a newly banned organisation, rather than the institute having committed any violations itself. As such, it will be made clear to any faculty members working with this third party that risks may exist due to that organisation's ties with a sanctioned entity.

As per the US International Traffic in Arms Regulations (ITAR), Purdue limits access to sensitive programmes for students from ITAR restricted countries.[81] Students from these countries may study at Purdue, but not all disciplines. Indeed, during the Obama administration several countries were restricted from studying (nuclear) energy-related courses. In early 2021, the US specifically had sanctions on four 'State Sponsors of Terrorism': Iran, Cuba, Syria and North Korea, with corresponding strict export control and immigration restrictions in place.

Export Controls

Purdue formally introduced its export control programme in 2005, with controls put in place at the contract stage before any work begins.[82] A programme has existed prior to this, although it was formalised due to heightened security concerns post-9/11, which also coincided with growing international engagement by the university. Within Purdue, the Office for Sponsored Programmes Services (OSPS)[83], which sits at the university level, handles proposal submissions as well as contract negotiations. As part of their role, the eight-person OSPS team considers factors such as: whether the proposal sponsor has publication approval from their industry partners; whether US national legislation restricts participation based on citizenship; and whether there are further dissemination limits on how the researcher can publish the work. After their review – which all proposals must go through – the OSPS works with individual faculties to put in place any necessary 'Technology Control Plans' (TCP). They also investigate all aspects of research information assurance. As projects undergo screening, each Principal Investigator (PI) is made aware of any issues and requirements.[84] In the US, contracts usually determine what 'Fundamental Research' entails and whether it is subject to any publication restrictions. If researchers receive controlled information, this is often managed under a non-disclosure or other confidentiality agreement.

81 As of 2020, these include Afghanistan, Belarus, Cuba, Iran, Iraq, Libya, North Korea, Syria, Vietnam, Myanmar, China, Haiti, Liberia, Rwanda, Somalia, Sudan, or Democratic Republic of the Congo and any UN Security Council arms embargoed country.

82 Director of Research Compliance in discussion with the authors, September 2020.

83 OSPS falls under the Office of the Executive VP of Research and Partnerships (EVPRP).

84 Director of Research Compliance in discussion with the authors, September 2020.

Where a contract requires a TCP, this identifies which personnel are authorised to fulfil contract work, dissemination and publication restrictions, and physical and information technology security (including where information can be stored on the university network, how information may be shared with the sponsor, and other controls of unclassified information). This is signed by the Principal Investigator (PI) of the project, the head of IT, the head of department, the laboratory leader and all project personnel.

Part of the OSPS remit includes reviewing agreements with foreign sponsors to ensure they are not a 'designated entity', and whether the research or research materials require a licence. This investigation includes jurisdictional review, to determine which regulations the contract falls under (e.g., commerce rule, the export administration regulations, or State Department rules). It further includes lab review, to prevent the risk of deemed export[85] occurring due to a significant number of foreign persons on campus. They also consider whether physical shipments require any licence and, if so, which. Concerns could arise with regards to partnerships with US businesses which have foreign partners when goods are shipped abroad.

The OSPS recognises that it is crucial for staff to understand what the regulations say, without overstating what is legal or not. Staff should feel empowered to communicate with one another on potential risks and threats. Significantly, Purdue has unofficially observed that if they conduct outreach to a particular department, then the export control office will subsequently receive more questions from that department. Recognising the benefit of additional outreach and peer-to-peer engagement, more experienced faculties are now mentoring other faculties and departments and encouraging them to think about these issues.

Protecting Sensitive Information

The OSPS review includes identification of the types of information or material that should be controlled, and whether and how this may be published or otherwise communicated. As per the ITAR exemption to 'Fundamental Research', if research is free from publication restrictions, it requires publication approval by the sponsor. Any results of the research that include technology or technical data resulting from the regulation is not subject to the export control regulations. Therefore, it can be submitted to a journal legally without any requirement for a licence. Purdue also recognises critical and sensitive technologies, and it is trying to educate its staff to determine when a research project or result might require further due diligence. This is a matter of security culture, awareness and ethics. Furthermore, departmental leaders, the Executive Vice President for Research and the President of the university have been open to communication with government agencies in terms of sharing information about risks and threats.

However, Purdue does not have a 'Central Risk Committee' which considers sensitive research such as non-peer reviewed output. Individual academics police themselves and their own research students. Some outputs may be limited when it comes to security, but mostly publications would only be restricted if the research was classified or sensitive. For example, if anyone is working on something related to reactor security such as risk analysis or adversary pathway analysis, details about the reactor facility (e.g., placement and number of cameras) cannot be provided. While in certain publications, the university's name may also be omitted.

Physical and Information Security Measures

As a whole, Purdue contains numerous laboratory and research environments that contain hazardous materials and sensitive information. To ensure information security, each lab containing hazardous radioactive materials has a dedicated computer which is locked, containing files and folders that are separately password protected.[86]

85 "Deemed" exports are described in 734.13(b) of the Export Administration Regulations (EAR). The Regulation imposes an obligation to obtain an export licence before "releasing" controlled technology to a foreign person. Releases of controlled technology to foreign persons in the US are "deemed" to be an export to the person's country or countries of nationality. Those organisations having persons with permanent residence status, US citizenship, and persons granted status as "protected individuals" are exempt from the "deemed" export rule. 'Fundamental Research' – defined as "basic and applied research in science and engineering where the resulting information is ordinarily published and shared broadly within the scientific community" – is exempt from EAR licencing requirements. See: Bureau of Industry and Security, 'Scope of the Export Administration Regulations', Government of the United States, 5 October 2021. https://www.bis.doc.gov/index.php/documents/regulation-docs/412-part-734-scope-of-the-export-administration-regulations/file

86 Research Associate in discussion with the authors, September 2020.

Only the lab members are provided with the passwords, which are changed regularly. Purdue also works with password protected flash drives. For people outside the project entering the lab there is a two-person rule or 'buddy system' in place, with their access continually monitored.[87]

From its workplace observations, Purdue has been able to establish that staff in general maintain excellent adherence to procedures; doors are not held open, badges are checked and rooms are locked.[88] Communication between staff is also deemed to be good, with individuals aware of what is meant to be happening and noticing when something unusual is going on. Notably, there is no reward scheme aimed at encouraging these behaviours. Instead, staff take an intrinsic pride in adhering to security-related procedures. If issues occur, staff usually address these between one another rather than escalating to management.

Regarding its research reactor, Purdue must balance security concerns with its core mission of teaching and public engagement. One example of this is its reactor tours. These cater to the general public, including potential students. In order to be confident that they can be conducted safely and securely, Purdue has performed a risk assessment of the PUR-1 facility including the creation of a 'Potential Facility Risk Index' (PFRI).[89] This includes analysis of potential threat groups and adversary sequence models to better understand possible risks and consequences.

Indeed, although public access via tours may allow greater insight into the reactor building's layout, the risk level posed by the LEU-powered, pool-type reactor is considered low. This is because of the nature of the hazard and mitigating measures that have been put in place. As such, foreign nationals are allowed in without vetting.

Members of the public must show ID however, copies of which are retained. People are not allowed to take backpacks or bags into the reactor building. There are also cameras in place which continually monitor individuals participating in the tours. Visitors are allowed to take photos in permitted areas, but not videos. Purdue continuously evaluates these policies, as well as potential incident scenarios. In assessing risks, potential reputational issues are also considered. Should a security event occur, the subsequent media coverage could well prove more detrimental than the physical effects of the incident itself.[90]

Security Culture Assessment

Upon arrival at Purdue, students may not be aware of the security environment straight away – particularly if they do not work in a big or busy lab with sensitive materials or information. They become familiar with their lab culture and necessarily the broader security culture at Purdue. In addition, an internal review conducted by Purdue suggested that there is a generational divide amongst staff in terms of attitudes and behaviours with respect to security.[91] According to this research, it was observed that long-term faculty members tended to prioritise safety over security, or that they struggled to determine the difference.[92]

Significantly, researchers from Purdue have recently developed a risk model in which they have tried to quantify the human aspect of security through assessing organisational culture. Here they have attempted to extract lessons from global best practice within the nuclear sector, utilising guidance published by the International Atomic Energy Agency (IAEA) and the World Institute for Nuclear Security (WINS). Building on this, Purdue have sent out surveys and conducted interviews, looking at general awareness and asking about people's understanding of procedures, leadership and management in relation to security.

87 Ibid.

88 Shraddha Rane, Jason T. Harris, Eric K. Foss and Courtney Sheffield, 'Nuclear and Radiological Source Security Culture Assessment of Radioactive Material Users at a University', *Health Physics,* vol. 115, no. 5, 2018, pp. 637-645.

89 Jason T. Harris, Shraddha Rane, Emily Bragers and Destiny White, 'Nuclear Security Risk Analysis of a Higher Education Institution Research Reactor', International Conference on Nuclear Security, International Atomic Energy Agency, Vienna, 10-14 February 2020. https://conferences.iaea.org/event/181/contributions/15755/attachments/8454/11739/IAEA-CN-278-361-ORA.pdf

90 Data from multiple interviews, June-September 2020.

91 Shraddha Rane, Jason T. Harris, Eric K. Foss and Courtney Sheffield, 'Nuclear and Radiological Source Security Culture Assessment of Radioactive Material Users at a University', *Health Physics*, vol. 115, no. 5, 2018, pp. 637-645.

92 Shraddha Rane, Jason T. Harris, Eric K. Foss and Courtney Sheffield, 'Nuclear and Radiological Source Security Culture Assessment of Radioactive Material Users at a University', *Health Physics*, vol. 115, no. 5, 2018, pp. 637-645.

Initially this study focused on users of radiological materials, but a broader follow-up included the entire campus (both students and staff) with surveys distributed to around 30,000 people. It looked at differences between and across key demographics such as age and ethnicity, and individuals' position in the university. Results from both studies were shared with the university administration to indicate in which groups and areas understanding of security was still lacking. The study highlighted the importance of achieving a broad security buy-in, the necessity to explain what it is being done and why, and the need to ensure safety and security focused personnel understand one another so they can effectively cooperate. In essence, the study revealed that it is essential to understand the key drivers and mechanisms that underpin security adoption within a specific organisation (in this case a university) and the importance of regular and transparent communication between all stakeholders. This helps guarantee that required changes and recommendations result in sustained actions. Follow-up surveys were also identified as an essential means of gauging whether awareness has evolved.

Challenges Encountered

As a public university, Purdue attaches great value to academic freedoms, transparency and collaborative work. With that said, Purdue also seeks to foster a 'questioning attitude', where individuals are encouraged to 'see something, say something' i.e., pay attention to what people are doing and report as needed to their supervisor or the export control office. In this context, the employment of a dedicated member of staff whose job it is to focus on information research assurance, and who can be approached to talk through issues, has proven to be useful.

Although there has reportedly been excellent leadership buy-in for security at Purdue, the development of security culture has also been a bottom-up movement. Since dedicated nuclear security culture training was introduced in 2018, students have arguably picked up on this faster than existing staff.[93]

For many, nuclear security and export controls are still relatively new concepts, and people have only recently begun to integrate this into their everyday behaviour and culture. Students and staff gradually become familiar with different security procedures and the synergy between safety and security culture through hands-on experience.

Despite the aforementioned initiatives, it has been nevertheless difficult to convince people at Purdue to prepare for the full range of potential threats the university faces. When prompted, staff and students confirmed that they believe a credible threat exists, but that they would not necessarily know how to prevent or respond to it.[94] To improve nuclear security awareness, both students and faculty members would benefit from an increased security-related training. With faculty members having an enormous influence on students, it would help for them to demonstrate their leadership on security culture with new and current students. This would create a stronger, more continuous, cycle of security awareness.[95] Systems and procedures should also be tested to detect vulnerabilities, rather than putting measures in place after an incident has taken place. To address this, a quarterly security culture and risk assessment would be constructive.

With regards to mental health, Purdue offers a multitude of services. However, this is not always clear to those who need to use them. Graduate students sometimes do not have the same level of access to mental health services as undergraduate students; nor do international students. Students tend to seek private help in the local community but many students cannot access those sources due to financial limitations. Here there is a concern in relation to the insider threat (i.e., an unhappy student or member of staff may potentially become a security risk). These challenges apply not only to Purdue, but to all universities and institutions of higher education.[96]

In terms of reporting requirements and confidentiality, these depend on the stakeholder.

93 Ibid. The surveys as well as in-person interviews with students and faculty indicated this. Students had a better answer on security questions than faculty. Specifically, the 'Nuclear Terrorism' component is thought to have been an effective tool for students to learn more about security culture.

94 Data from the radiological material user survey consisted of a written survey and follow-up in-person interviews.

95 Data from the nuclear security culture assessment.

96 The Chronicle of Higher Education and Council of Graduate Schools have published several articles related to the inadequacy of mental health services for graduate students. See: Colleen Flaherty, 'Mental Health Crisis for Grad Students', *Inside Higher Education*, 6 March 2018. https://www.insidehighered.com/news/2018/03/06/new-study-says-graduate-students-mental-health-crisis; Editorial, 'The mental health of PhD researchers demands urgent attention', *Nature*, vol. 575, 2019, pp. 257-258; Kathryn R. Wedemeyer-Strombel, 'Why We Need to Talk More About Mental Health in Graduate School,' *The Chronicle of Higher Education*, 27 August 2019. https://www.chronicle.com/article/why-we-need-to-talk-more-about-mental-health-in-graduate-school

For example, if a counsellor is worried about the behaviour of a graduate student (i.e., a 'student of concern' at immediate risk of harm), there is a mechanism they can pursue, through either the police, or the graduate school. In addition, there are different advisers and mediation specialists available within the college. The Dean of students may also become involved in matters relating to concerning behaviour or actions. There is not a central process however, suggesting a potential gap within the university's ability to respond.

Summary and Conclusions

Purdue has well-developed programmes to combat a wide range of security threats relating both to state and non-state actors. The university is now focusing on increasing not just the depth but also the breadth of security awareness amongst its staff and students. Here a particular initiative of note is their efforts to conduct a security culture assessment at Purdue, the results of which feed into new and revised security efforts.[97] During this process, they learned that even many of those who use radiological materials had a relatively limited understanding of security and security culture. Consequently, there remains more work to be done in this area, although the presence of robust existing processes and procedures for security-related awareness raising and training means that the university is in a strong position to enact these going forward.

97 Shraddha Rane, Jason T. Harris, Eric K. Foss and Courtney Sheffield, 'Nuclear and Radiological Source Security Culture Assessment of Radioactive Material Users at a University', *Health Physics*, vol. 115, no. 5, 2018, pp. 637-645.

Case Study 4 – Korea Institute of Nuclear Nonproliferation and Control: Encouraging Organisational Culture in Regulation

Organisation Overview

The Korea Institute of Nuclear Nonproliferation and Control (KINAC) was founded in 2006, bringing together and consolidating several functions previously distributed across South Korea's regulatory infrastructure.[98] Today, along with the Nuclear Safety and Security Commission (NSSC), KINAC plays a major role in demonstrating South Korea's commitment to nuclear security, and is responsible for a diverse range of activities in this area. The organisation manages South Korea's nuclear safeguards agreements, oversees nuclear material accountancy and control arrangements, enforces import and export controls on nuclear materials and relevant technologies, and conducts training and education programmes related to research and development on nuclear non-proliferation and nuclear security issues.[99]

KINAC also plays a leading role in strengthening security culture at South Korea's nuclear organisations. The country is a major user of nuclear technology and has a diverse and well-established nuclear technology sector.[100] Similar to other states, South Korea has traditionally paid greater attention to nuclear safety issues than nuclear security issues. National efforts to improve security culture across South Korea began in the 2000s.

However, after it became apparent that there was limited alignment between national standards of security culture in its nuclear industry and international guidance, South Korea initiated measures to improve nuclear security culture. At the 2010 Nuclear Security Summit in Washington DC, the country affirmed its commitment to 'work with industry to ensure the necessary priority of physical protection, material accountancy, and security culture.'[101] These words were translated into action through the formulation of a comprehensive national nuclear security culture framework and the introduction of a national implementation guide.

This case study aims to understand how KINAC and the NSSC have supported the development of nuclear security culture in South Korea, the challenges that they encountered, and how these were overcome.

National Nuclear Security Culture Implementation Guide

South Korea's primary document on nuclear security culture is the National Nuclear Security Culture Implementation Guide, which was developed by KINAC and the NSSC in 2013. This implementation guide is a key component of a national strategy formulated to raise awareness and improve understanding of nuclear security culture.[102]

98 'History', website of KINAC. https://www.kinac.re.kr/board?menuId=MENU00410&siteId=SITE00003

99 'Main Functions', website of KINAC. https://www.kinac.re.kr/board?menuId=MENU00411&siteId=SITE00003

100 The country is the sixth largest user of nuclear energy by generating capacity and has an active nuclear research sector. See: International Atomic Energy Agency, 'Operational & Long-Term Shutdown Reactors', IAEA PRIS. https://pris.iaea.org/PRIS/WorldStatistics/OperationalReactorsByCountry.aspx

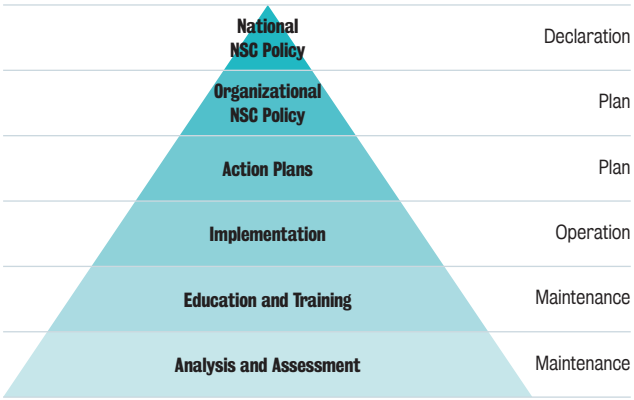
101 'Communiqué of the Washington Nuclear Security Summit', Archives of the White House – President Barack Obama, 13 April 2010. https://obamawhitehouse.archives.gov/the-press-office/communiqu-washington-nuclear-security-summit

102 Internal document of the Nuclear Safety and Security Commission (NSSC).

The implementation guide is directed at regulatory bodies, nuclear-related organisations, organisations charged with securing nuclear assets and the personnel of all these organisations – and it details the key expectations and requirements for these organisations. The development of the implementation guide was driven and consolidated by several important events. Most notably, the Nuclear Security Summit process resulted in nuclear security and nuclear security culture gaining political primacy in South Korea, with the 2012 Summit hosted in the country's capital Seoul. Building on this commitment, in 2014, South Korea hosted an International Physical Protection Advisory Service (IPPAS) mission of the International Atomic Energy Agency (IAEA), where an assessment of nuclear security culture was included as part of the national review process.

The guide draws on key international treaties and guidance, the most notable influences being the Amendment to the Convention on the Physical Protection of Nuclear Material (CPPNM/A) and the IAEA's Nuclear Security Series.[103] The key principles in these documents were adapted to suit the country's national nuclear security environment in terms of both regulation and operations. The guide also places emphasis on the importance of leadership in developing a robust security culture and the interaction between safety and security culture.[104] A six-step framework was developed to systematically foster a nuclear security culture through the development of individual action plans, where organisations are encouraged to formulate their internal principles and statements to reflect the guide's core elements. Sustainability is promoted through continuous education and training, with organisations encouraged to assess and analyse their nuclear security culture as it develops.

Figure 1: Structure of the National Nuclear Security Culture Implementation Guide. Source: Nuclear Safety and Security Commission, 'National Nuclear Security Culture Implementation Guide', Seoul, 2013.



Organisations are expected to prepare their own security policy statement, establish appropriate management structures, ensure resources for security and conduct self-assessments. This practice can vary depending on the nature of each organisation, but the core elements recommended by the guide should be incorporated into the organisations' principles. Recognising the important role of managers in promoting nuclear security culture through their influence on employee attitudes, the guide stipulates their role in detail – covering key responsibilities, practice management, qualification and training, motivation, and performance enhancement. Staff members are expected to recognise their current security environment and understand the potential consequences of their behaviour in the context of credible threats to nuclear security, while also being conscious of how their roles and actions shape and impact nuclear security culture.

However, it should be noted that the principles enunciated in the guide are only recommendations, and currently, organisations are not legally obliged to foster an effective nuclear security culture within South Korea. Without the power to compel organisations, the South Korean state thus focuses on encouraging all stakeholders to comply with best practice guidelines and on providing education and training programmes. Indeed, although the use of the national implementation guide is voluntary, the guide nonetheless serves as a useful focal point of standards and normative expectations.

103 International Atomic Energy Agency, 'Nuclear Security Culture', IAEA Nuclear Security Series, No. 7, Vienna, 2008.
104 Nuclear Safety and Security Commission, 'National Nuclear Security Culture Implementation Guide', Seoul, 2013.

Notably, major South Korean organisations such as Korea Nuclear Fuels (KNF), Korea Hydro and Nuclear Power (KNHP) – both subsidiaries of the Korea Electric Power Corporation (KEPCO) – and the Korea Electrotechnology Research Institute (KERI) have issued policy statements and action plans on the basis of the national implementation guide.[105] In particular, KINAC and the NSSC regularly conduct nuclear security culture-related surveys on workplace attitudes. If the results indicate a need for improvements, further investigations are conducted and additional training is organised to improve standards.

International Nuclear Nonproliferation and Security Academy

To meet its 2010 Nuclear Security Summit commitments, in 2014, KINAC founded the International Nuclear Nonproliferation and Security Academy (INSA) as a Centre of Excellence to provide practical education and training programmes related to nuclear security. Since its establishment, INSA has sought to enhance both domestic and international nuclear security culture. It has a dedicated teaching staff as well as the ability to draw upon a vast network of academic and research institutions. This has enabled the academy to develop its own education and training materials such as textbooks, online e-learning contents, training aids and security laboratories.

As the official education and training centre for nuclear security, INSA conducts various activities in this area. Within South Korea, INSA runs compulsory training programmes for domestic nuclear power plant operators, a certificate course for nuclear inspectors, and various public awareness programmes. For international audiences, INSA jointly conducts education courses with the IAEA and special education sessions for nuclear newcomer countries. In 2017, INSA became the first organisation in the field of nuclear security education globally to obtain International Organization for Standardization (ISO) certificates. These included Quality Management System (ISO 9001) and Learning Services in Non-Formal Education and Training (ISO 2990) certificates.

Article 106 of the country's Nuclear Safety Act mandates that all business operators and research institutions related to nuclear energy should provide 'Nuclear Control Education' for their employees. This pertains to safeguards and export control issues in the context of nuclear non-proliferation. Training is conducted by INSA, whose education and training objectives include helping organisations understand the international regime on nuclear control, meet their nuclear non-proliferation obligations, and prevent, detect and respond to potential threats faced by their facilities. In addition to 'Nuclear Control Education', a course on 'Physical Protection Education' is compulsory for operators. INSA holds lectures at its centre in Daejeon or at other facilities located nationwide for the convenience of trainees. Over 2,000 people per year complete the aforementioned courses.

International Education for Nuclear Newcomer Countries

In addition to training domestic staff, South Korea trains international audiences in a range of nuclear security activities, and this includes introducing nuclear newcomers to the importance of security culture. In this context, INSA has worked closely with its partners such as the IAEA, as well as governments and institutions from the US, China and Japan, to develop education and training curricula. These have been used to train government officers, regulators, researchers and technicians from countries with nascent nuclear power programmes. INSA's 'International Training Course' (ITC) comprises lectures, group exercises, learning sessions and technical visits to nuclear facilities.

Since 2014, over 1,000 international trainees have participated in INSA's ITCs, which are delivered in English. Initially, INSA alternated introductory and intermediate courses annually, but since 2017 it has conducted both levels every year. The duration of the courses is five days, and course themes include 'Nuclear Security Infrastructure Development', 'Physical Protection System Elements', 'Security Contingency Plan' and 'Fundamentals of Cybersecurity at Nuclear Facilities'. INSA's ITC was developed to differentiate from existing courses delivered by education institutions in other countries and other international organisations.

105 Hosik Yoo, 'Nuclear Security Culture: In Case of ROK', Korea Institute of Nuclear Nonproliferation and Control, 20 March 2014. https://ec.europa.eu/assets/jrc/events/20140320-nuclear-security/20140320-nuclear-security-yoo.pdf

In addition to providing education and training programmes, KINAC and the NSSC have hosted annual meetings in partnership with the Federal Authority for Nuclear Regulation (FANR) of the United Arab Emirates (UAE) since 2011. This cooperative initiative was originally designed to resolve technical or policy issues regarding the export of South Korean nuclear power plants to the UAE. Initially, issues related to export controls were mainly discussed, since the primary concern was transferring nuclear items and related technologies to the UAE. However, the scope of the meeting agenda was expanded in 2013, after which other issues such as safeguards and physical protection were also discussed. Over the course of nine annual meetings, various topics related to nuclear security have been addressed, including physical protection of power plants, security of nuclear fuel in transport and cyber security. This has been supplemented by additional technical meetings in order to deal with practical issues.

Protecting Sensitive Information

In 2011, South Korea established the 'Act on Prevention of Divulgence and Protection of Industrial Technology' (PITA)[106] to protect sensitive information and other information. This act outlines the concept of 'National Core Technology', which is defined across 12 categories and encompasses 71 specific technologies. PITA is overseen by the Minister of Knowledge Economy, who may 'require the submission of data necessary to formulate comprehensive plans from the heads of relevant central governmental administrative agencies and the heads of enterprises, research institutes, specialized institutions, universities, etc. which possess industrial technology.'[107] Nuclear energy is one of the defined categories and includes five specific technologies.

In the nuclear field, the approach is supported by security vetting, which prospective staff should undergo before being hired. This applies to both industrial organisations and research and academic institutes with nuclear assets.

Since its introduction, PITA has undergone several revisions, including one for awarding harsher punishments for technology leaks.[108] For example, an amendment to PITA was passed in August 2019 which came into force on 21 February 2020. In cases of technology leaks, the amendment imposes 'a mandatory sentence of a minimum of 3 years imprisonment and a fine of up to KRW 1.5 billion [~US$ 1.3 million] on offenders.'[109] In effect, the amendment seeks to impose stringent limits on the transfer of intellectual property, specifying that 'if national core technology is brought into a company by an employee who formerly worked at another company who owns the national core technology, it is likely that the company with the leaked technology will be subject to penalty in Korea.'[110]

Furthermore, the Enforcement Regulation of the Act on Physical Protection and Radiological Emergency (APPRE) requires the management of information related to physical protection systems at nuclear facilities in South Korea. Each nuclear operator should establish and maintain appropriate information security systems, which must be certified by the Nuclear Safety and Security Commission. Violations of APPRE can attract severe sanctions, and this enforcement regulation is intended to deter actions that might circumvent information security controls.

Protection of intellectual property and sensitive information also extends to research and development work. Here, all new nuclear fuel cycle-related activities must undergo a government pre-screening process before any work is commissioned. If pre-screening indicates that a project involves sensitive information, the South Korean government may order the implementation of additional security measures. In such a case, in addition to any specific measures that apply to the project, project managers should also complete 'Nuclear Control Education' at INSA.

106 Korea Law Translation Center, 'Act on Prevention of Divulgence and Protection of Industrial Technology', Korea Legislation Research Institute, 25 July 2011. https://elaw.klri.re.kr/eng_service/lawView.do?hseq=24351&lang=ENG#:~:text=The%20purpose%20of%20this%20Act,development%20of%20the%20national%20economy

107 Ibid.

108 Lee & Ko, 'Korea Strengthens Protection of National Core Technology and Industrial Technology (Amendment of the Prevention of Divulgence and Protection of Industrial Technology Act)', The Legal 500, 2 October 2019. https://www.legal500.com/developments/thought-leadership/korea-strengthens-protection-of-national-core-technology-and-industrial-technology-amendment-of-the-prevention-of-divulgence-and-protection-of-industrial-technology-act

109 Ibid.

110 Ibid.

Both tangible and intangible transfers of nuclear technology are also regulated by the 'Foreign Trade Act'. For instance, if a foreign national is to be recruited for a research project related to the nuclear fuel cycle or if a research paper is to be presented at an international conference, the specific contents should be approved by the government through a review process. In instances where such projects are deemed to contain strategic information, an export licence is required.

Nuclear Security Culture Self-Assessment

Since compliance with various regulations often comes down to the behaviour of individuals, KINAC and the NSSC have developed a comprehensive methodology for evaluating nuclear security culture. The methodology has been widely disseminated to nuclear-related organisations for practical use. This Nuclear Security Culture Assessment Programme is based on a self-diagnostic survey (which has been conducted since 2010) and an objective assessment by KINAC and the NSSC.[111] It contributes to analysing the strengths and weakness of an organisation so that an optimal security arrangement can be devised and reflected in its security policies.

As part of this programme, KINAC and the NSSC carry out annual surveys on nuclear security awareness of employees at the country's nuclear power plants. After collecting data from questionnaire returns, interviews are conducted to support the interpretation of the survey results and to develop appropriate action items to strengthen nuclear security culture policy. After reviewing the survey results, if KINAC or the NSSC believe that an organisation's nuclear security culture is weak and requires improvement, the issues are addressed through additional consultations, which might include workshops aimed at raising nuclear operators' awareness of nuclear security. Often consultative meetings specifically target an organisation's leadership, given their importance in supporting developing a robust nuclear security culture.

Challenges Encountered

A robust nuclear security culture does not develop overnight and needs to be continually promoted. Sustaining operator attention in this area is arguably the biggest challenge faced in South Korea. To overcome this challenge, KINAC and the NSSC have applied both short- and medium-term strategies, focusing on immediate changes that organisations can make to strengthen nuclear security and longer-term capacity building. This is done cooperatively with nuclear organisations, given that nuclear security culture considerations remain a recommendation rather than a legal or regulatory requirement and hence cannot be implemented under compulsion. In addition to more structural challenges, national training efforts have been disrupted by the global pandemic. In 2020, most of the onsite courses and in-house lectures were cancelled due to Covid-19 restrictions. To ensure continuity of training, INSA swiftly adjusted the plan to conduct more online lectures and develop e-learning materials to cover all compulsory education and training demands.

Summary and Conclusions

KINAC and the NSSC have adopted a multi-pronged approach to strengthen nuclear security in the South Korean nuclear industry and abroad. Capitalising on the political momentum imparted by the Nuclear Security Summit process, they have developed and promoted a range of guidance, services, education and training programmes. In particular, emphasis has been placed on translating this high-level support to the organisational level so it can effectively shape security practice in different working environments. Although nuclear security culture is not covered by current nuclear regulations, this largely informal approach is deemed to have been successful as evidenced by the increasingly active engagement by operators in nuclear education, training and self-assessment activities.

111 Hosik Yoo, 'Nuclear Security Culture: In Case of ROK', Korea Institute of Nuclear Nonproliferation and Control, 20 March 2014. https://ec.europa.eu/assets/jrc/events/20140320-nuclear-security/20140320-nuclear-security-yoo.pdf

Case Study 5 – King's College London: Balancing Academic Freedom with Security

Organisation Overview

King's College London (King's) is a public research university located in central London, United Kingdom (UK). Established by a Royal Charter from King George IV in 1829, King's is a founding college and member institution of the federal University of London. From its inception King's had a medicine department and, over the years, accumulated additional institutions and campuses, including the United Medical and Dental Schools of Guy's and St Thomas' Hospitals.[112] King's has an particularly diverse community, with around 150 different countries represented among its student and staff body; in fact, 'internationalisation' is a key strand of King's 'Strategic Vision' for the next decade, referring to institutional efforts to build strategic networks of academic collaboration around the world.[113]

Today, the university community consists of more than 30,000 students, supported by over 9,000 academic and support staff.[114] King's is the largest educational centre in Europe for doctors, dentists and other healthcare professionals. It is also renowned internationally for teaching and research in other disciplines, especially the natural sciences, social sciences and law. As a large teaching and research university with specialisms in the natural sciences and medicine, King's has a number of hazardous materials onsite, including radiological sources. Several of these are category one high-activity sealed sources (HASS) which have the potential, if not properly controlled, to cause significant harm to humans.[115]

The Evolving Security Context

The case study of King's serves as a compelling example of the challenges involved in the protection of nuclear materials and sensitive information, where academic freedom and access to information need to be balanced against the realities of security risks in a metropolitan area.

From a nuclear security[116] perspective, King's faces several diffuse threats by virtue of its location as London's most centrally located university – occupying four riverside campuses in the heart of the city (with a further campus to the south). Not only is central London densely populated, but it is also a major international capital and one of the world's largest financial centres. All the university's four riverside campuses are located either near London's financial centre, near the UK's government at the Houses of Parliament, or near key tourist attractions such as the South Bank area.

King's affords high priority to the protection of all its hazardous materials and there are dedicated security staff based across the estate buildings. The implementation of nuclear security is aligned with the International Atomic Energy Agency (IAEA) categorisation of the radioactive materials kept onsite, but the university is also cognisant of the particular nature of its city centre location and bustling campuses, which adds another layer of complexity to security arrangements. Reflecting the specialised nature of working with hazardous materials and machinery, undergraduate and taught master's students do not have access to radioactive materials at King's.

Over the past two decades, security has been increasingly prioritised within King's in response to a growth of international jihadist networks and a spate of terrorist attacks targeting London in the post-9/11 era. Such increased securitisation was in line with other European and US cities although the focus on site security at King's arguably reached a later 'peak' with the 2012 London Olympics.[117] Notably, this was when individual London landmarks were identified as potential targets by the security services. During this period, Counter Terrorism Security Advisers (CTSAs) from the Metropolitan Police provided direct guidance to King's to identify and assess sites that might be vulnerable to terrorist attacks.[118]

112 King's College London, 'About us: History', website of King's College London. https://www.kcl.ac.uk/about/history

113 King's College London, 'Internationalisation 2029 – King's Strategic Vision 2029', August 2020. https://www.kcl.ac.uk/internationalisation/assets/internationalisation-2029-strategy.pdf

114 King's College London, 'Update on Cases', website of King's College London, 24 January 2022. https://www.kcl.ac.uk/coronavirus/campus/updates

115 These sources are category one on the matrix arrangement used by the IAEA. See: International Atomic Energy Agency, 'Categorization of Radiation Sources – Corrected Version', Vienna, March 2001. https://www-pub.iaea.org/MTCD/Publications/PDF/te_1191_prn.pdf

116 Note that in the United Kingdom 'nuclear' tends to refer to nuclear materials only. In the context of this case study, 'nuclear security' encompasses the broader IAEA definition to refer to the security of radioactive materials.

117 King's staff member in discussion with the author, July 2020.

118 Government of the United Kingdom, 'Guidance: Working with counter terrorism security advisers', National Counter Terrorism Security Office, 30 July 2020. https://www.gov.uk/government/publications/counter-terrorism-support-for-businesses-and-communities/working-with-counter-terrorism-security-advisers

Following these concerted efforts and additional resources leading up to the 2012 Olympics, the emphasis on security at King's appeared to have reached a 'critical mass'.[119] However, the rise and subsequent fall of Islamic State in Syria and Iraq triggered a wave of terrorist attacks in central London during 2017.[120] As a result of this new threat landscape, additional security measures were implemented at King's – most notably the installation of security barriers and the compulsory wearing of name badges. While Covid-19-related protocols have further altered the delivery of many services at King's, onsite security across all the estate is currently at an all-time peak.[121]

Regulation and Governance of Nuclear Security

In England (as distinct from the UK), the enforcing authority for radioactive materials is the Environment Agency (though the principal regulatory body for nuclear materials – the Office for Nuclear Regulation – assumes regulatory control when such materials are in transit). Following the UK's departure from the European Union in January 2019, the legislation governing radioactive sources across the country is the 'Environmental Permitting (England and Wales) Regulations 2016'.[122] Other legislation that has relevance to radioactive sources at King's is the 'High-activity Radioactive Orphan Sources Regulations 2005'.[123]

Notwithstanding this oversight structure, it is the responsibility of the licensee – i.e. King's – to ensure that the security of radioactive materials is established and maintained. The Environmental Agency in its regulation of radioactive materials takes a relatively prescriptive approach and directs the licensee. The Environmental Agency also consults with CTSAs (see above) within the country's police forces regarding onsite arrangements.[124]

Furthermore, the UK's Health and Safety Executive (HSE) is responsible for assisting with certain matters relevant to the protection of hazardous materials at King's. Owing to HSE's sometimes onerous requirements, King's tends to plan carefully ahead of any changes to HSE provisions to ensure that health and safety resources are available and sufficient. This places the burden on the protection team keeping abreast of the relevant legislation and directives, including on nuclear security.

King's also consults regularly with the London Fire Brigade. The arrangement for a major emergency is governed by the London Emergency Services Liaison Panel (LESLP), which comprises all the emergency responder agencies and is chaired by the Metropolitan Police. In the event of an incident, the London Fire Brigade takes the lead over other responders and would be aware of the type and location of radioactive materials contained within the King's estate. The protection team also liaises with radiation protection societies, including the Association of University Radiation Protection Officers (AURPO).[125] Run by volunteers, AURPO's membership mainly consists or radiation protection and safety officers working in education, research and teaching establishments. AURPO's principal aim is "to increase knowledge and understanding of radiation protection through the protection and interchange of information and best practice."[126] It consults with officials working in government and regulation and also publishes its own guidance documents.

In addition, King's has links with the Society for Radiation Protection (SRP), which works to "promote the science and art of radiation protection and allied fields for the public benefit."[127]

119 For example, evidence of how austerity affected police resources during this period is available in the Institute for Government's 'Performance Tracker 2019' for 'Police', Institute for Government, 2019. https://www.instituteforgovernment.org.uk/publication/performance-tracker-2019/police

120 David Anderson, 'Attacks in London and Manchester – March-June 2017 – Independent Assessment of MI5 and Policy Internal Reviews', December 2017. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/664682/Attacks_in_London_and_Manchester_Open_Report.pdf

121 King's staff member in discussion with the author, July 2020.

122 Statutory Instruments, 'The Environmental Permitting (England and Wales) Regulations 2016', United Kingdom Statutory Instruments, 11 December 2016. https://www.legislation.gov.uk/uksi/2016/1154/introduction/made

123 Ibid.

124 Government of the United Kingdom, 'Guidance – Secure hazardous materials to help prevent terrorism', National Counter Terrorism Security Office, 24 November 2014. https://www.gov.uk/guidance/secure-hazardous-materials-to-help-prevent-terrorism

125 More information can be found on the website of the Association of University Radiation Protection Officers (AURPO): https://aurpo.org.uk

126 Website of the Association of University Radiation Protection Officers (AURPO): https://aurpo.org.uk

127 More information can be found on the website of the Society for Radiological Protection (SRP): https://srp-uk.org

These associations are deemed to be valuable for sharing best practice and disseminating information that is directly relevant to the implementation of nuclear security at King's, with their specific expertise of an academic setting. Establishing informal links with other protection officers around the UK and abroad is an important way that King's has benefitted from 'lessons learnt' at other comparable institutions.[128]

Nuclear Security Management and External Engagement

In parallel to the threat landscape evolving, the implementation of nuclear security at King's has changed over the years. There are two separate streams for managing nuclear security at the university: first, under onsite security; and second, under radiation protection. Until 2011 onsite security was an area directly managed by King's staff, later it was implemented by external contractors, and more recently it was brought back inhouse. Meanwhile, radiation protection was initially handled by the relevant NHS Foundation Trusts but today it is managed fully onsite, with regular input from the Environment Agency and CTSAs over specific issues including any remedial work. CTSAs also provide an annual security audit of King's, and occasionally the security team meets with the Metropolitan Police's Counter Terrorism Command unit. This interaction with external agencies is designed to ensure that King's is well-prepared for an armed response by the authorities to any potential future security incident on its estate.

All those working with radioactive sources at King's are required to complete a dedicated safety training programme. This includes both the users (mainly academic staff and PhD students) and those staff involved in the maintenance of the materials. The programme, which is implemented and assessed by King's protection staff, also contains a (limited) focus on nuclear security. Meanwhile, all those working with HASS materials additionally receive specific security training.

The security training is designed to be comprehensive and introduces fundamental concepts of nuclear security, such as defining the threat and building awareness that the 'threat is real' (aligned to the Nuclear Security Series published by the IAEA).[129] The training also makes good use of case studies, enabling participants to engage with the nuances and complexities of a real-life situation, while comparing the implications of different courses of action.[130]

In the past, terrorist attacks have occurred in close proximity to King's, thus the potential for a security incident at the university is not just a theoretical concept. Security personnel regularly monitor the risks and are highly aware that King's is exposed to specific vulnerabilities by virtue of its central location, perception as a high-value target, and diverse student and staff body.[131] This suggests that the security culture is robust, and staff are not simply complying with the relevant nuclear security guidelines as a 'box ticking exercise'. [For more on security culture, see below.] Equally, risk assessments of hazardous materials at King's are very specific to each campus layout and geographical location in London. This means that any potential future terrorist attack in central London would not necessarily be considered to pose a direct threat to all hazardous materials at King's.

Nuclear Security Implementation

The protection of hazardous materials at King's originated in concerns about safety but now extends to security too. Nuclear security at King's encompasses vulnerability assessment, physical protection, security culture, insider threats, personnel vetting, information security, emergency procedures and contingency planning, the latter of which comprises response plans. The implementation of nuclear security at King's is based on international best practice guidance, most evidently in its alignment to the IAEA Nuclear Security Series.

128 King's staff member in discussion with the author, July 2020.

129 'Nuclear Security Series', website of the International Atomic Energy Agency. https://www.iaea.org/resources/nuclear-security-series

130 Thomas N. Gilmore and Ellen Schall, 'Staying alive to learning: Integrating enactments with case teaching to develop leaders', *Journal of Policy Analysis and Management*, vol. 15, no. 3, 1996, pp. 444-456.

131 King's staff member in discussion with the author, July 2020.

Despite the distinctive features of the university – with its central London location, high footfall and diverse student and staff population – there is no significant variance in the types of nuclear security measures applied to comparable inventories of nuclear and radiological materials in other parts of the world. This underlines the universality in nuclear security guidance and its common implementation, including in academic settings.

The measures in place at King's that have visible plans and procedures for nuclear security can be broadly divided into the following categories:

- Physical security onsite:
  - Site Security Plan
  - Floor plans
  - Physical Security Rated barriers
  - Intruder Detection systems
  - CCTV Monitoring
  - Authorised Access Control Systems and related procedures
- Information security
- Personnel:
  - Vetting procedures
  - Approval, authorisation and access procedures
  - Usage authorisation procedures
- Emergency and contingency planning:
  - Identification of hazards
  - Temporary weakness scenarios
  - Reporting procedures
  - Emergency procedures
  - Security system testing
  - Reporting procedures

The small size of the group of individuals at King's working on protection helps ensure that procedures are well-integrated.

Aiding this approach, protection personnel work on broad areas across the university, including:

- Campus security
- First responders
- HSE/EA/CTSA inspectors (on production of valid identity cards)
- Campus Operations
- Campus Operations Manager
- Health and Safety Services
- Radiation Protection

As discussed, the implementation of nuclear security at King's has evolved significantly in the past few decades – and most of this change has aligned the university's security provision with guidance contained in the IAEA's Nuclear Security Series. In the past, the approach for mitigating security risks was primarily focused on 'delay'; now this has been extended to emphasise an integrated approach across 'deter', 'detect', 'delay' and 'respond'.[132] The other significant way in which nuclear security has been strengthened at King's is the re-appraising the level of protection required for the individual components of its inventory of hazardous materials and radiological sources. Following a broad analysis and audit of this inventory, it was determined that the level of protection required for some materials (such as high-activity sealed sources; HASS) was akin to critical national infrastructure. While King's would not be formally considered as part of the UK's critical national infrastructure, it was deemed appropriate for the university to protect its materials to a similar level, and advice is sought on a regular basis from the UK's Centre for the Protection of National Infrastructure (CPNI).

Insider Threats and Human Reliability Programmes

As an academic institution with a diverse student and staff body from across the world, King's arguably faces a heightened risk from 'insiders' – referring to a security risk that originates from people within an organisation. The insider threat can be harder to spot within an academic environment owing to the general transiency of the population and the deep-seated principle of academic freedom.

132 Ibid.

At King's, there is a variety of avenues for reporting in place, including for students and staff to discuss concerns with line managers and the security team. King's has also implemented a confidential 'whistle blowing' reporting service, enabling staff and students to report any concerns, including those relating to security.

At entry to the university, the Human Resources department conducts verification checks on all staff and students, with additional vetting for individuals in sensitive roles such as those with access to highly hazardous materials. A staff assessment committee – which includes both security staff and Human Resources officers – assists with the vetting process. King's also continually monitors all users working with hazardous materials and controlled information, and periodically carries out full vetting of these individuals. Staff and students are encouraged to feed into this process, in order to provide full visibility for those involved. While much of the verification process is largely generic – and shares similarities with other similar educational institutions – King's has sought to go further than others by independently confirming all the information declared by individuals.

In the past, the vetting process at King's focused on a simple Enhanced Disclosure and Barring Service (DBS) check but in recent years this has evolved to a broader personnel security risk assessment, based on guidance provided by CPNI. Indeed, through the university's regular contact with CPNI, one of the areas identified as an area of potential improvement was enhancing the vetting process. A significant change implemented in 2014 was the monitoring of social media, which is now largely handled by a third-party on behalf of King's under appropriate data protection controls. Certain content shared by the individual at entry while being vetted, or by immediate contacts under the principle of 'first degree of separation', might be flagged for further investigation or result in the individual not passing the vetting checks.

Organisational and Security Culture

The IAEA's guidance on security culture, derived from Edgar Schein's work on organisational security,[133] applies equally to educational institutions as nuclear plants. In an academic environment where footfall can be high and the population transitory, highly visible security procedures are critical, as are clearly defined routes for reporting security concerns. One of the greatest challenges in ensuring a strong security culture within an academic environment, however, is when such efforts overlap with other initiatives. In a large institutional setting such as King's, there is potential for decisions being taken to achieve broader objectives such as promoting the university's global research agenda or improving broader organisational culture, but which may inadvertently stymy security efforts. As an example, the protection team encountered a practical challenge when the university at one time promoted 'being kind' on campus; this had the unintended consequence of encouraging people to open doors for one another, presenting a security challenge through facilitating 'tailgating' into secure areas of the estate. It is therefore essential that the fundamental belief in the importance of security (i.e., 'a credible threat exists')[134] co-exists readily alongside other guiding principles of the university.

At King's, there is no dedicated security culture topic within the nuclear security training provided to students and staff. Nonetheless, the university's protection team recognises the critical importance of fostering a good security culture, noting that awareness of this concept and mechanisms for strengthening it could be further improved. The focus is currently more on the conventional aspects of protection, as outlined in the university's visible system of procedures and systems (see above). The protection team at King's has become involved with external security culture-related engagement activities delivered by academics and researchers within the Department of War Studies.[135] This collaboration between 'users' and 'educationalists' has helped to strengthen the university's internal training on nuclear security and underlines how security culture might be developed through both formal and informal mechanisms.

133 Edgar Schein, *Organisational Culture and Leadership 4th ed*., San Francisco, CA: Jossey-Bass, 2010, p. 18.

134 International Atomic Energy Agency, 'Self-assessment of Nuclear Security Culture in Facilities and Activities – IAEA Nuclear Security Series: Technical Guidance', IAEA Nuclear Security Series, no. 28-T, Vienna, 2017. https://www.iaea.org/publications/10983/self-assessment-of-nuclear-security-culture-in-facilities-and-activities

135 Centre for Science & Security Studies, 'Training', website of the Department of War Studies, King's College London. https://www.kcl.ac.uk/csss/training

Balancing Security with Academic Freedom

As discussed in the introduction to this handbook, there have been past cases where actors with malign intent have applied to academic organisations in order to gain access to controlled technology and materials. In addition to the catastrophic security and safety implications of enabling a malicious actor to obtain nuclear or radiological materials, there are serious impacts for a university from reputational damage and/or criminal penalties. In the UK, penalties include a fine of up to £20,000, imprisonment or both.[136] Reputational damage could make it harder in the future for the university to attract high-quality students and staff, as well as lucrative research grants.

King's faces the perennial tension between, on the one hand, implementing nuclear security to protect the wider community and, on the other, ensuring academic freedoms through facilitating independent and original research. For King's, this balancing act is all the more acute because a potential radiological incident would contaminate not only the university campus but a densely populated metropolitan city and a global financial hub. King's is renowned as a 'research university', which denotes the institution is committed to producing original and innovative research. The university's protection team focuses on being flexible and facilitating research while using risk assessment to mitigate potential security risks.[137] In some cases this requires varying regulatory permits or applying additional security protocols (as well as for health and safety). As such, the remit of security officers working in an academic and research environment is arguably more demanding and complex than other organisations holding equivalent radioactive materials, such as hospitals where there tends to be more routine and consistent use of these.

In parallel to the physical risks of radiological materials going out of regulatory control, King's is obliged to protect controlled information related to radiological materials. This area presents a particular challenge as it goes to the heart of the tension between nuclear security and academic freedom. As an example, the university's protection team might need to verify what information in lab reports or academic articles enters the public domain, for instance in a journal publication. In certain cases, some information or data might be redacted if it compromises the locations of radiological sources or types of devices. Nevertheless, the overriding emphasis at King's is on retaining as much research value as possible in the spirit of the open culture present at the university. One of the challenges, though, is in ensuring that all users are accurately able to distinguish controlled information from non-controlled information. Achieving this distinction ensures resources for security can be allocated according to need, as in the case of controlled information, while enabling the relevant aspects of non-controlled information to enter the public domain and strengthen the university's research outputs.

Resilience and Business Continuity

In the Covid-19 era, a key issue to have emerged is the capacity of organisations holding nuclear and radiological materials to cope with extra demands associated with the pandemic. In the case of King's, these new challenges include absenteeism due to illness and self-isolation, travel restrictions, furloughing of staff, and extra operating costs (such as for personal protective equipment, body temperature screening and additional cleaning). King's has faced particular difficulties in implementing the multi-person rule, where two or more people are required to be present where a sensitive action is being performed to ensure compliance and security. The requirement of social distancing has served to erode that action. Furthermore, the pandemic has complicated the availability of certain radioisotopes due to the disruption to international trade and transport, with additional disruption related to the UK's departure from the European Union.[138]

The issue of staff capacity is particularly acute for educational institutions holding radiological materials owing to the specialised skillset required by their security teams.

136 United Kingdom, 'Radioactive Substances Act 1993', chapter 12, The Stationery Office of the United Kingdom, 1993 and 1999. https://www.legislation.gov.uk/ukpga/1993/12/pdfs/ukpga_19930012_en.pdf

137 King's staff member in discussion with the author, July 2020.

138 Christopher Hobbs, Nickolas Roth and Daniel Salisbury, 'Security Under Strain? Protecting Nuclear Materials During the Coronavirus Pandemic', *The RUSI Journal*, 12 January 2021, pp.40-50.

Indeed, the smaller the protection team or the more specialised the job requirements are, there is a real risk of a 'single point failure' if any single staff member were to leave office without an immediate well-trained replacement. This is an issue for universities and academic institutions across the world, although it arguably affects the lesser-funded institutions more. At King's, the issues are mitigated by regularly assessing resilience and redundancy in the security and safety procedures.

Summary and Conclusions

The implementation of nuclear security in an academic environment shares many similarities with other settings where radioactive materials are present. Above all, if organisations are abiding by best practice approaches – embodied by the IAEA's nuclear security guidance – there is a consistency in approach and culture, and in many cases these organisations share the same regulator, which oversees this consistent implementation. In England for example, the Environment Agency is the enforcing agency for all non-nuclear sites holding radioactive materials and this includes universities, hospitals and industry.[139] Yet, while recognising the similarities, this case study has shown that academic institutions are often very distinctive settings for radioactive materials. They often face more significant challenges in the implementation of nuclear security while having fewer resources at their disposal.

Above all, educational institutions where research is a primary focus, as in the case of King's, must allow for original and innovative research and this inevitably can create challenges when security precautions appear to be in tension with the fundamental principle of academic freedom. Although the institution will need to ensure that the cumulative security of its radioactive materials is not compromised, this necessitates the protection team devising a more flexible security arrangement and mitigating risks by scaling up other security measures. Challenges can often occur when users are working with controlled information relating to radioactive materials, since data is sometimes perceived (erroneously) as a lesser security risk as compared to the physical risks of radioactive materials going out of regulatory control.

This issue is likely to become all the more salient in the future as the domain of cyber security takes off as a new threat vector. Considering all the specific challenges in implementing nuclear security, it is particularly important that academic institutions establish formal and informal networks in which these issues can be deliberated.

139 United Kingdom Government, 'Radioactive substances regulation (RSR) for non-nuclear sites: Environmental permitting of radioactive material and radioactive waste at non-nuclear sites in England', website of the United Kingdom Government, 13 August 2019. https://www.gov.uk/government/collections/radioactive-substances-regulation-for-non-nuclear-sites

Case Study 6 – Institute of Nuclear Research, Ukraine National Academy of Sciences: Applying Export Controls Best Practice in Research Settings*

REGIONAL CENTRE: CRIMEAN DONETSK KYIV NORTHEAST PRYDNIPROVSKY SOUTHERN WESTERN

Figure 2 – Map of Ukraine showing locations of NAS research institutes. Note that institutes in the Crimean region have not been operated by the NAS since 2014. The colour indicates to which regional research centre the institution belongs.

**Note that this case study was completed in January 2022*

Organisation Overview

The National Academy of Sciences of Ukraine (NAS) is the largest self-governing scientific research organisation in Ukraine.[140] Founded in 1918, the NAS is state-funded through the National Council of Ukraine for the Development of Science and Technology,[141] and is divided into three sections managing 14 departments between them. From its headquarters in the capital Kyiv, the NAS manages the overall research programmes of five regional research centres (based in Pokrovsk, Lviv, Odessa, Kharkiv and Dnipro) and approximately 180 research institutes, centres, and other research facilities across Ukraine,[142] some of which were originally established by the Ministry of Defence of the former Soviet Union.

NAS institutes cooperate and collaborate with academic institutions, government agencies, other research organisations and the private sector both within Ukraine and internationally, with 138 research agreements in place with organisations in more than 50 countries, plus 240 further agreements with academic institutions. Research topics range from mathematics, engineering and the natural sciences to the social sciences and humanities. At the time of writing, the NAS employed 28,500 staff, of which slightly over 50% were researchers. The NAS is governed by the General Meeting of its members, who are scientists elected as members of the organisation on the basis of outstanding contributions to their field. At the time of writing, there were over 600 members. NAS activities encompass both fundamental scientific research and applied research on a wide variety of topics, including some involving dual-use goods, materials and technology. Consequently, efforts have been made within the organisation to apply export controls measures to prevent these from being improperly transferred.[143]

Export Control Implementation in Ukraine

Like many countries, Ukraine operates list-based export control laws, where the legislation includes lists of goods, materials and associated technology and software which are subject to controls and cannot be exported without a licence granted by the State Service of Export Control of Ukraine (DSECU).[144] These lists include goods and materials which have applications in conventional arms and weapons of mass destruction (WMD) and their delivery systems. Ukraine's lists are taken from lists prepared by the four multilateral export control regimes (MECRs), which are the Nuclear Suppliers Group (NSG),[145] the Missile Technology Control Regime (MTCR),[146] the Australia Group,[147] which controls chemical and biological weapons-relevant goods and technology, and the Wassenaar Arrangement,[148] which controls conventional weapons and other military-relevant goods and technology.

Under Ukrainian law, organisations seeking to import or export goods or technology of military relevance, or those seeking to acquire a general or open export licence for ongoing trade (as opposed to a one-off licence for a single international trade), are further legally required to have a detailed internal compliance programme (ICP). This ICP must be approved by the DSECU, and the operation of ICPs of this type requires specialised and dedicated personnel and funding. However, ICPs are still considered to be best practice, and so organisations may choose to implement ICP elements in order to better fulfil their export control duties.[149]

140 National Academy of Sciences of Ukraine, 'Information About the National Academy of Sciences of Ukraine', website of the NAS, 2017 [translated]. https://www.nas.gov.ua/UA/About/Pages/default.aspx

141 Website of Government of Ukraine. https://www.kmu.gov.ua/diyalnist/nacionalna-rada-ukrayini-z-pitan-rozvitku-nauki-i-tehnologij

142 National Academy of Sciences of Ukraine, 'Structure of the National Academy of Sciences of Ukraine', website of the NAS, 2017. https://www.nas.gov.ua/UA/Structure/Pages/default.aspx

143 In the preparation of this case study, researchers from King's College London interviewed two senior experts from the Export Control Group (ECG) at the Institute of Nuclear Research (INR). The interview was conducted on 26 August 2020 with the Head and Deputy Head of the ECG, who are also senior researchers with the INR. Further information was provided by the interviewees by email on 18 March 2021.

144 Government of Ukraine, 'State Export Control Service of Ukraine', 2020. https://www.dsecu.gov.ua/

145 Nuclear Suppliers Group, 'About the NSG', website of the NSG, 2021. https://www.nuclearsuppliersgroup.org/

146 Missile Technology Control Regime, 'MTCR Brochure – Who We Are and What We Do', website of the MTCR, 2020. https://mtcr.info/mtcr-brochure-who-we-are-and-what-we-do/

147 The Australia Group, 'The Australia Group', website of the Australian Department of Foreign Affairs and Trade, 2007. https://www.dfat.gov.au/publications/minisite/theaustraliagroupnet/site/en/index.html

148 The Wassenaar Arrangement, 'Introduction', website of the Wassenaar Arrangement, 2020. https://www.wassenaar.org

149 Deputy head of the ECG in discussion with the authors, 26 August 2020.

Export Control Programme at the NAS

Much of the institutional expertise on export controls within the NAS exists within the organisation's Export Controls Group (ECG), a small group of individuals based at the Kyiv-based Institute for Nuclear Research (INR),[150] within the Department of Nuclear Physics and Power Engineering. Since the 1960s, the INR has operated a 10-megawatt 'VVR-M' research reactor and conducted various nuclear science and engineering research, which necessitates the occasional international transfer of nuclear goods, materials and services. First established by a NAS directorial decree in the late-1990s, the ECG provides guidance and technical expertise on export controls issues both within the INR and NAS more broadly. Initially created to work on international export controls projects, such as the delivery of seminars, creation of handbooks, technical reviews of licences and so on, the ECG has since developed to support internal export control-related activities, such as applying for export licences and goods identification. NAS administration staff direct all export control queries to ECG members.[151]

As an example of a case where the ECG were able to prevent a potentially sensitive technology transfer, the ECG identified the planned hiring of two postdoctoral researchers from Iran to conduct nuclear-relevant research at the INR, during a time when Iran was under international sanctions for the suspected military dimension of its nuclear programme. If this exchange had occurred, it would have been in violation of export controls and could have facilitated the transfer of sensitive information, goods and technology.[152] Today, the ECG consists of four subject matter experts, one of whom specialises in international affairs, plus an administrator who handles export licence applications and related matters. The ECG handles all matters related to export controls compliance, including preparation of paperwork and licence applications, commodity identification, advising other researchers, communicating with technology producers and suppliers, and conducting education and awareness raising activities.[153]

The nature of research at the INR does not require a fully and formally certified ICP. However, the INR does voluntarily implement elements of internal compliance programmes in order to strengthen its own compliance practices. However, some elements of full-scope ICPs are not implemented. For example, the NAS does not perform detailed due diligence checks on foreign partner organisations or provide training for all its research staff on the importance of not sharing controlled technology when travelling internationally. Here, individual researchers have the option to engage with ICP programme elements on a voluntary basis.[154]

A particular element of note from broader ICP best practice which is implemented at the NAS is senior management buy-in. The Director of the NAS is well-informed about export controls legislation and ICP implementation. Whilst he has not signed a formal declaration committing the NAS to export control compliance, as would be required for a full ICP checked and certified by the DSECU, the interviewed experts stated that it is implicit in various documents from the NAS that the organisation will not support the proliferation of WMD. The ECG also works closely with a NAS deputy director, helping ensure that key issues are communicated to the NAS leadership.[155]

Awareness Raising and Training

Staff at the NAS are not currently provided with formal training in export controls. Export control issues are sometimes covered during NAS 'scientific council' meetings, which are open to all staff, although these mainly focus on research topics. Rather than blanket training for all staff, export control support is instead focused on those scientists across the institution working on topics of dual-use concern. One of the interviewees explained that in his experience, export controls issues are best solved in person, and that his "door is always open" to any head of department or individual scientist, who can come and seek his advice.[156]

150 Institute for Nuclear Research, 'Institute for Nuclear Research', website of the National Academy of Sciences of Ukraine, 2020. http://www.kinr.kiev.ua/index_en.html
151 Deputy head of the ECG in discussion with the authors, 26 August 2020.
152 Ibid.
153 Ibid.
154 Ibid.
155 Ibid.
156 Deputy head of the ECG, email message to the authors, 18 March 2021.

For these individuals, members of the ECG hold seminars on export controls in an effort to familiarise them with key issues and raise awareness of compliance requirements. These training efforts are judged to be largely effective, with relevant researchers proactively engaging with the ECG to seek the latest information and advice.[157] However, the interviewees stated that they considered this approach insufficient, and for that reason they were seeking to implement a full ICP across the whole of the NAS.[158] There are projects currently underway to expand the provision of export controls training across the NAS (to be discussed later).

Vetting, Screening and Human Reliability

There are processes in place at the NAS for the screening of individuals seeking employment, as well as for visiting staff who will be staying with the organisation for an extended period. For visiting staff, the ECG prepares a detailed dossier on the individual, including information on the justification for their visit, whom it will work with, locations it will attend at the NAS and so on. This might also include information regarding their past employment, such as whether the individual has previously worked at a defence-related research organisation in a country of concern. The resulting dossier is passed to the Ukrainian national security services, which will make the decision as to whether the individual may attend the NAS. Work is planned to further expand and deepen screening procedures as part of the ICP development project.

The ECG does not currently carry out a formal export control or non-proliferation assessment of other institutions with whom it intends to engage in collaboration. However, the ECG does carry out some due diligence, in order to decide how much screening will be necessary for individuals from institutions with whom it intends to partner.

Protecting the Transfer of Sensitive Information

The NAS does not have a general policy aimed at controlling the exchange of scientific and technological information both amongst its own researchers and with external organisations, preferring instead to encourage open communications. Visiting scientists at the NAS are subject to various restrictions on accessing facilities and so on, but personal contact between researchers is not restricted. Whilst there are general measures in Ukraine to protect against the theft of sensitive information by cyber means, these do not prevent scientists from sharing export-controlled information with one another. NAS staff are generally warned against the dissemination of classified information, but not all export controls-relevant information is classified, and thus such information sharing is not yet covered within NAS policies, a limitation recognised by interviewees who stated the need to develop appropriate training and instructions on this topic.[159]

Institutes within the NAS that manufacture goods for export generally have good awareness of what is required of them in terms of export controls compliance. However, the interviewees reported a lower than ideal level of understanding across the rest of the NAS regarding which technologies are subject to export controls. Sensitive technology is protected, but this is driven by a desire to prevent the loss of intellectual property rather than by export control considerations.[160] The lack of a systematic approach to the management of technology transfer risk means that intangible technology transfer is more likely to occur, and export control processes will be required to ensure that proliferation-relevant information is not spread through collaborative research activities.

157 Deputy head of the ECG in discussion with the authors, 26 August 2020.
158 Deputy head of the ECG, email message to the authors, 18 March 2021.
159 Ibid.
160 Ibid.

Physical Measures, Information Security and Security Culture

Whilst export controls compliance measures at the NAS are partially implemented and developing, the organisation has given great attention to physical security for a long time, and security was described by the interviewees as being very strict. The site is managed by national guardsmen, who protect the NAS with some specific areas of particular focus, such as the research reactor installation. The NAS also seeks advice and guidance from the George Kuzmycz Training Center for Physical Protection, Control and Accounting of Nuclear Material. This centre is the official training provider for all nuclear security officers in Ukraine, physical security of nuclear installations and related matters.[161]

In terms of security culture, it was noted that while this concept is not formally promoted or assessed, a security culture exists at the NAS which is still shaped to an extent, particularly amongst older staff members, by the approach taken during Soviet times, when security including the protection of sensitive information was apparently extremely strict. Nevertheless, younger staff are more open to the idea of sharing ideas with other researchers, including internationally. Overall though, the security culture at the NAS was deemed by the interviewed experts to be important in acting to prevent the sharing of sensitive information, helping to reduce the risk of illicit technology transfer and negating the lack of formal ICP procedures.[162]

Support to National Government and Customs

Beyond its role within the NAS, the ECG is sometimes approached by the Ukrainian government for technical advice on export controls issues. This includes support in commodity identification and licencing risk assessment. For such requests, the ECG will gather the necessary information, conduct research, and provide its advice to the government. The ECG might also work with frontline staff of Ukraine's customs authorities.

When faced with shipments it cannot identify or on which it requires technical input, customs officers will often seek advice from the NAS ECG as to whether the goods are controlled and what should be done.[163]

Beyond the NAS, the ECG is involved in a long, ongoing project to develop the skills and capabilities of Ukraine's customs services. This programme has previously been supported by a project funded by the US Department of Energy (DoE), which requested the input of the ECG as subject matter experts at events it funded within Ukraine. The use of ECG members as experts was deemed to be highly beneficial in the US-funded project, as this allowed real knowledge of the local situation to be included in the training, which had previously been limited due to the use of only US-origin trainers. Members of the ECG have also been involved in higher education teaching in Kyiv, delivering lectures to Master-level students on economics degrees on the topic of non-proliferation and related international issues.[164]

Challenges Encountered

In discussing the challenges faced in applying export controls at the NAS and across the research sector more broadly, one major issue identified was that researchers would often insist that their research was fundamental in nature, rather than applied, which would make it exempt from most export controls licencing.[165] However, research can cross the border into the realm of applied research, even to the point of being dual-use relevant, without staff realising it. Here it was noted that this is a particular issue for universities, where academics are not full-time researchers. Rather, they found that academics' primary focus was on education, with research activities being only one of a range of demands on their time. As a result, it was particularly hard to communicate to academics that their work is of proliferation relevance and to motivate them to take action.[166]

161 Deputy head of the ECG in discussion with the authors, 26 August 2020.

162 Ibid.

163 Ibid.

164 Ibid.

165 Export control regimes often differentiate between fundamental or basic research, which studies underlying phenomena and scientific facts, and applied research, which considers the application of scientific knowledge towards particular purposes. Fuller definitions of fundamental and applied research are provided in Organisation for Economic Co-operation and Development. 2015. *Frascati manual 2015: Guidelines for Collecting and Reporting Data on Research and Experimental Development*. OECD Publishing, Paris. www.conicyt.cl/wp-content/uploads/2014/07/Manual-Frascati-2015.pdf

166 Deputy Head of the ECG in discussion with the authors, 26 August 2020.

The Russian annexation of Crimea has led to Ukraine imposing sanctions on Russia, and this has significantly altered the way that the NAS must operate. Historically, Russia and Ukraine have been very close, and many years of working together have had to be unwound. For instance, NAS researchers used to collaborate closely with Russian scientists, but such collaboration has not been able to continue. All dual-use and military-relevant exports to Russia are now subject to export licencing. The interviewees reported that many of the researchers were still unaware of the impact of these sanctions, and that a range of new procedures have had to be introduced over the previous five to six years in order to prevent researchers from engaging in what are now illegal practices. Not all research staff have fully accepted these new procedures, and some have pushed back in an effort to continue work with Russian colleagues.[167]

The interviewed ECG members further said that the expertise required for their export controls role is very different than the expertise required to be a scientific researcher, and spoke about the difficulties in finding suitably qualified and interested personnel to work on export controls compliance.[168] Due to restrictions on how research funding is used, their work on export controls cannot be their main role and must only be carried out alongside their primary research activities.

Beyond a core group of scientists working on dual-use issues, it was noted that it would be very challenging to set up and manage a system to familiarise all NAS scientists with export control issues.[169] This was particularly given the extensive control lists of sensitive goods and technologies, as well as potential emerging technologies which do not yet feature on such lists. Furthermore, when asked about training programmes and processes for the wider organisation, the interviewed experts expressed their belief that a reliance on formal processes and best practice in export control compliance would not be a suitable approach for the NAS, stating such a system would be viewed research scientists as overly prescriptive, strict or controlling.

Instead, they believed that the only way to address the challenge is to provide researchers with information about export control issues, risks, malign actors, and so on, and then give them responsibility for ensuring their own compliance. They hope that current projects to roll our ICP measures, coupled with ongoing support from international partners will help to raise the profile of export controls compliance within the NAS.[170]

This bottom-up approach to compliance was viewed as most suitable as the interviewees said that scientists are not responsive to measures that restrict their ability to share information. They said that the "scientists believe that their ideas, theories, calculations… – everything which lives in their heads – is their private business,"[171] and that work would be required to clarify where the boundaries of confidential and export-controlled information lie, and convince researchers to abide by the associated controls. The interviewees said that researchers are generally passionate about their work and wish to share it with others through publications, international conferences, and so on. Furthermore, researchers are always conscious of the limited longevity and precarious nature of their funding, and will resist attempts to reduce their possible range of funding sources.

Summary and Conclusions

The NAS is a large organisation whose research includes a broad range of topics, some of which are of dual-use relevance and subject to export controls. Within the NAS, the ECG) operates from the INR to provide export controls advice and support to staff across the wider organisation. Researchers can approach the ECG with any questions and concerns, and the ECG provides support with the implementation of some elements of internal compliance programmes to manage the risks of export-enabled proliferation.[172] According to interviewees, the NAS is committed to the principles of non-proliferation and to being a reliable strategic and research partner.

167 Ibid.
168 Ibid.
169 Ibid.
170 Ibid.
171 Deputy Head of the ECG, email message to the authors, 18 March 2021.
172 Deputy head of the ECG in discussion with the authors, 26 August 2020.

The organisation is perceived to have a strong security culture and strict security processes, thanks in large part to Ukraine's history as a part of the USSR. However, the younger generation of researchers are increasingly distant from the organisation's Soviet past, and as time goes by the organisational culture may be changing towards an increased willingness to share and collaborate. Whilst there are measures in place regarding the vetting of research collaborators, these need to be communicated clearly to all staff in the organisation to ensure that the changing culture does not undermine security.[173]

The ECG carries out its export control role alongside its primary research activities. Whilst there is support from the senior management of the NAS, many researchers on the ground are either unaware of the potential export control risks of their research, or find the need to comply with export controls to be a burden, and seek to present their research as fundamental or otherwise low risk in order to avoid the need to seek export licences or engage with due diligence activities. The ECG combats this by engaging with key leading researchers in areas of particular concern, and is working towards the provision of training across the organisation to increase the awareness of export control compliance requirements.[174]

The ECG is also seeking funding and carrying out projects to bring training and tools to the full range of researchers across the NAS. For example, when the interview was conducted, the ECG was hoping to acquire funding to further develop their ICP frameworks for the NAS from the Science and Technology Centre of Ukraine, an EU-funded organisation, and the project resulting from this funding, 'Development of the ICP for National Academy of Sciences',[175] is now about to begin. The funding would enable a large project to fully develop and roll out a full range of procedures needed to enable export controls compliance across the wide portfolio of research activities undertaken at the NAS.

A preliminary project to explore how this could be done was already underway, supported by internally provided funding. This project, known as NEXUS (Non-proliferation and Export control for Ukrainian Science), aims to develop an online system to communicate, consult and inform researchers about export controls issues and procedures. A component of this is the development of an online training programme for NAS staff in export controls and non-proliferation, which would include elements of assessment. The ECG hopes to share results of their ICP development work with academic and other research organisations in Ukraine, which were seen by the interviewees as vulnerable to infiltration by individuals who might seek to acquire sensitive technology.[176]

Overall, the ECG within the NAS has the potential to be a key hub of information, and has already been highly effective both within and beyond the NAS. Whilst there are some areas of export control and sanctions compliance which have yet to be fully addressed, the ECG recognises this and is taking steps to address them. Additional funding and support for the ECG will enable it to further embed compliance best practice into organisational culture and procedures, both within the NAS and beyond.

173 Ibid.

174 Deputy Head of the ECG, email message to the authors, 18 March 2021.

175 Ibid.

176 Ibid.

Disclaimer

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

kcl.ac.uk/csss
@KCL_CSSS