ADVANCING GOOD PRACTICE: THE WORK OF THE WORLD NUCLEAR ASSOCIATION'S SECURITY WORKING GROUP

G.C. KASER
World Nuclear Association
London, United Kingdom
Email: greg.kaser@world-nuclear.org

R. HOWSLEY
World Institute for Nuclear Security
Vienna, Austria
Email: roger.howsley@wins.org

Abstract

The World Nuclear Association is an international trade body representing the global nuclear industry, including major reactor vendors, nuclear power plant operators, nuclear fuel suppliers and uranium miners, engineering, construction and waste management companies, along with professional service and transport providers. Its working group on fuel cycle security was reorganised in 2018 to better reflect member views and outputs from the Nuclear Industry Summit series held alongside the Nuclear Security Summits 2010–2016.

Whilst nuclear security is ultimately a state responsibility and an integral part of a state's national security, licensed nuclear operators are responsible for ensuring that their facilities and materials are protected physically and that their technology and data are secure in accordance with legal and regulatory requirements. The global nuclear industry is committed to effective security and to continual improvement through the exchange of best practice, personnel training and regular review of plans and measures. The World Nuclear Association's working group on security has adopted an agenda to examine a number of key areas: mitigating insider threats, cyber-security, the safety-security interface and culture, and to learning from other industries in order to establish good practice in corporate governance, communication with regulatory bodies and civil society, and gender diversity.

The paper reports on the progress made in these areas within the context of the changing security and market environment. It will offer suggestions on how the civil nuclear industry can work at the national and the international levels with governments, regulatory bodies and international organisations including the International Atomic Energy Agency to foster effective and efficient security within nuclear energy programs in established and embarking countries to engender a high level of stakeholder confidence.

1. INTRODUCTION

The World Nuclear Association is an international trade body representing the global nuclear industry, including major reactor vendors, nuclear power plant operators, nuclear fuel suppliers and uranium miners, engineering, construction and waste management companies, along with professional service and transport providers. The Association organizes a number of industry working groups to allow its members to share good practice, conduct analysis, and develop consolidated positions on economic, safety and environmental issues for members' business development.

The World Nuclear Association's working group on fuel cycle security was reorganised in 2018 to better reflect member views and the outputs from the Nuclear Industry Summit series held alongside the Nuclear Security Summits 2010–2016. Not all governments took part in the Nuclear Security Summits, which had been held at the initiative of the USA. Nor had the consultation process for drafting the joint declaration issued by the nuclear industry representatives been fully inclusive. Although the World Nuclear Association was consulted by the summit organizers it was clear that differing views existed within the global civil nuclear industry over its scope of responsibilities and in relation to the undertakings contained in the Joint Statement, indicating that further consideration needed to be given to the issues. The World Nuclear Association's security working group provided a forum through which companies from the nuclear industry could reflect on the results of the summit process.

New terms of reference for the working group were proposed in 2018 and agreed in 2019. These terms of reference stated:

> The Security Working Group is established to share expertise and good practice between World Nuclear Association members in the field of nuclear security and establish the view of the industry on nuclear security. The Working Group will not discuss or share classified materials or information.
>
> The Working Group supports the World Nuclear Association's mission to foster public confidence in the nuclear industry in the areas of security and the securing of materials under industry control.
>
> The Working Group acknowledges that nuclear security is an integral part of a State's national security. The responsibility for the national nuclear security regime within a State rests entirely with that State. Responsibility for the implementation of physical protection rests with the holders of the relevant licences or of other authorizing documents.

The Association's working group on security agreed an agenda and a two-year work program to examine a number of key areas: mitigating insider threats, cyber-security, the safety-security interface and culture, and to learning from other industries in order to establish good practice in corporate governance, communication with regulatory bodies and civil society, and gender diversity. The overall aim is to raise the profile of nuclear security among World Nuclear Association member organizations and the wider industry. These topics are discussed in the remainder of the paper.

2. MARKET AND POLICY CONTEXT

Nuclear energy is making a significant contribution to electricity generation and is poised to play a leading role in the transition to a clean energy system. However, some countries have decided not to invest in nuclear energy while others are closing their existing plants and phasing out the technology altogether [1]. Even where countries permit nuclear energy, mobilizing the necessary investment is hampered by uncertainty around cost recovery and policy continuity. Public concerns over the safety of nuclear power plants can drive ever more stringent regulation that renders continued operation or new construction unviable [2].

The same issues arise in relation to security. Although security concerns have not been as prominent as safety risks in public opinion, if a nuclear facility is not secure then it poses a safety risk. The initial rise in the level of concern over nuclear security appeared in the context of confrontational protest actions by environmental and peace activists. The possibility that nuclear materials in transit could be stolen, or that a shipment could be diverted, threatened security goals. Later the threat of terrorism in other sectors became more prominent. In many cases it led to prescriptive regulatory oversight being exercised over civil nuclear activities despite the lack of incidents specific to the sector. These issues are addressed more fully in the next section but they provide the backdrop to the way regulatory factors have weighed upon enterprises operating nuclear facilities.

The function of an enterprise in a market economy is to satisfy consumer demand. In the case of a nuclear power plant this is to sell electricity. Most markets are sufficiently 'imperfect', in the sense of economic theory, to permit enterprises some latitude in adopting marketing techniques that respond to different customer segments or profiles, and thus to avoid competing purely on price. They also allow enterprises room for manoeuvre in balancing short-term targets with longer-term objectives, and between rewarding employees and investors today and making investments in the business for tomorrow. Enterprise leaders can choose strategies which take account of the enterprise's various stakeholder interests.

In the case of a power plant its product is electricity and this does not lend itself easily to product differentiation (although the debate over climate change has altered this to some degree, as consumers demand carbon-free energy). Furthermore, a vertically integrated energy utility has more of a chance to tailor its suit of products to consumer preferences but market liberalization policies have pushed utilities to restructure and separate their generation activities from electricity sales and related services.

Additionally, while many countries have deregulated their energy markets to encourage greater competition, nuclear energy remains subject to considerable regulation, aimed at assuring safety and security. Typically, therefore, a nuclear power plant operates in a closely regulated environment while seeking to sell a homogeneous product on pricing considerations alone. Little or no value accrues to nuclear generation's around-

the-clock reliability and small environmental footprint in deregulated energy markets. Thus the 'playing field' on which nuclear power competes with other generating sources is often not a truly level one.

In these circumstances, a nuclear generator must make best use of a nuclear power plant's critical advantage: its technology. The nuclear fission process releases such a vast quantity of energy that a reactor can operate with a high level of efficiency. Operational performance improved steeply from the 1970s to stay at over 80 percent capacity from the mid-1990s onwards. In 2017, the global average capacity factor was 81.1 percent, up from 80.5 percent in 2016. Increased load-following by nuclear power plants will mean that the average capacity factor will fall in the future but this level of performance remains outstanding in comparison to other generating technologies [3].

The nuclear industry also has an excellent track record in technological innovation. Advanced 'Generation III' reactors are designs with higher availability and longer operating life (for example, 60 years or more), greater fuel efficiency, and have reduced possibility of core melt accidents. Several such designs entered service recently and are operating well. 'Generation II' reactors, which form the bulk of the world's fleet, have been upgraded to operate with higher levels of safety and performance. New accident-tolerant fuels are being developed for the market, again enhancing the overall safety of nuclear power plants.

These two aspects of operation – safety and efficiency – are linked because enhancing safety has a cost and this can sometimes only be absorbed if the nuclear power plant can reduce other operating costs through efficiency improvements given its need to sell electricity at the market price. In regions where electricity prices have fallen as a result of cheap gas or because renewable energy sources are selling power for almost nothing, helped by subsidies, some nuclear power plant operators have chosen to halt operation altogether rather than invest in the safety upgrades demanded by regulators.

The same is true of security enhancements. Additional expenditure on security can only be achieved if the plant's operating performance is improved or if economies can be realized in the security function or in other budgets. These constraints on the enterprise are not always given the attention they deserve by the national authorities and enterprise leaders can face difficult choices.

3. NUCLEAR SECURITY UNDER SCRUTINY

The importance of security in nuclear facilities has gained increasing prominence over recent decades. There has been a shift of attention from ensuring that nuclear materials are not diverted from peaceful uses towards protecting plants from sabotage, armed assault and cyber-attacks.

During the 1970s, the peace movement began to campaign against nuclear power by linking it to the production of plutonium, and thus, tendentiously, to the possession of nuclear weapons, and to a wider critique of so-called technocracy.[1] Site occupations halted construction of a reactor at Wyhl, on the River Rhine, and a waste repository at Gorleben, both in Germany, and a reactor being built at Plogoff in France in the years 1975-79 [7] [8] [9]. On the other side of the world, unfounded rumours that nuclear waste would be dumped in the oceans spurred the formation of the Nuclear Free Pacific Movement in 1975. Protests against civil nuclear shipping took place in parallel with attempts to stop nuclear weapons testing from 1971 onwards by Greenpeace and Peace Squadron vessels [10]. In addition to direct action at sea, activist groups attempted to block the arrival of used nuclear fuel for reprocessing at La Hague, France, in 1979. Such attempts to interfere with shipments resulted in growing government concerns over the possible sabotage or theft of materials in transit and spurred the adoption of the Convention for the Physical Protection of Nuclear Material in 1979 [11]. The CPPNM, which entered into force in 1987, was the first international treaty to deal with nuclear security.

The threat from terrorism over the last two decades has caused governments and civil society to accord ever greater attention to nuclear security. In actuality the nuclear industry has been largely free from violent assault, with the only cases having taken place in the 1970s and early 1980s, when the anti-nuclear protests already referred to were at their height. These incidents were directed at nuclear plants that were under construction as a way of demonstrating common cause with the wider peaceful anti-nuclear movement. Leftist guerrillas briefly occupied the Atucha construction site in Argentina in 1973. The Basque separatist group ETA set off bombs and fired shots at the Lemóniz nuclear power plant in Spain while it was under construction on three occasions between 1977 and 1979, killing three workers, and also assassinated the project's chief engineer

[1] See for example, Jungk, [4]; Lovins, [5]; and Harvey, [6].

and his replacement in 1981 and 1982 respectively. Four small bombs planted by an anti-apartheid sympathiser working at the Koeberg nuclear power plant in South Africa during its construction were detonated in 1982, without causing loss of life or injury. Rocket-propelled grenades were fired at the Creys-Malville fast reactor while it was under construction in France by associates of the Red Army Faction in 1982, causing minor damage [12] [13] [14].

Chemicals have been used in terrorist attacks around the world but so far there has never been a case where radiological materials have been employed (despite some apparent plans to do so by jihadi fighters). To date, no operating civil nuclear facility has been attacked by an armed group.

The opening up of cyberspace has additional created security challenges. Former Director-General of the International Atomic Energy Agency (IAEA), Yukiya Amano, stated:

> "Digital systems promise higher reliability, more functionality, better plant performance, additional diagnostic capabilities and many other advantages. But, of course, new digital systems also bring new challenges, including those related to nuclear safety and security." [15]

Concerns that plant personnel could be subverted by extremist ideas and provide insider support to non-state armed groups have grown, alongside the possible role of insiders in facilitating cyber-attacks. These concerns have probably arisen as a result of cases where confidential information has been stolen by hackers and whistle blowers, which demonstrated the vulnerability of computer systems to unauthorized intrusion. Attacks have occurred at nuclear power plants, the most recent example being that in India at the Kudankulam plant, although in all cases the reactors' control and protection/safety systems were unaffected [16]. However, cyber-attacks have recently succeeded in compromising the safety systems in the petro-chemical sector and threat trends in the industrial control systems/safety systems domain continues to increase hence the threat to nuclear installations cannot be excluded.

Addressing the interrelated challenges has been the underlying theme of the discussions at the World Nuclear Association's security working group. As part of the Nuclear Industry Summit Statement of March 2016 the industry pledged to "further enhance nuclear security" to, *inter alia*, secure all nuclear and radiological materials in industrial facilities and applications; minimize stocks of nuclear and radiological materials requiring special precautions where technically and economically feasible; promote a culture of safety and security among management and personnel; improve cyber-security; and provide appropriate information, where permitted, to the public and stakeholders on the effectiveness of security in the civil nuclear industry [17]. However, each of these aspects involves some degree of shared responsibility between the state and commercial enterprise. Getting the balance right is critical.

4. SECURITY AS PART OF RISK MANAGEMENT

Responsibility for the implementation of measures to protect nuclear facilities and nuclear material, including material during transport, and the confidentiality of information relating to physical protection and to maintaining a security culture within the organization rests with the holders of the relevant licenses or of other authorizing documents, that is, usually, the facility's operator. Senior management is expected to ensure that appropriate and effective physical protection and other nuclear security arrangements and training are applied at nuclear facilities and in their operations and during transport. In a competitive market environment, company boards need to be looking for all opportunities for efficient and effective operation. It is essential that company boards ensure that there are effective governance and oversight arrangements in place to make sure that the security function is structured and resourced appropriately with meaningful assurance mechanisms based on evidence and leading performance metrics.

According to the World Institute for Nuclear Security (WINS), the costs of security at nuclear installations has risen in many countries since the 9/11 attacks. Much of the increase can be attributed to the cost of enhanced guarding arrangements, a higher ratio of armed guards being deployed at nuclear facilities, and greater attention being given to cyber-security measures.

Nuclear facilities are usually required to pay for a guard force to protect their operations, including shipments of radioactive materials during transport. In many countries, the guard force is part of the police service or gendarmerie, but in some states it is employed either directly by the operator or contracted to a

specialist security company. The security function at the nuclear facility then becomes effectively an out-sourced arm of the national security set-up, and at best its accountability to the enterprise is blurred. Furthermore, from the enterprise leadership's point of view, security becomes seen as simply an activity that must be undertaken to comply with regulatory requirements, and, therefore, there is no point spending management effort in thinking about how to do it. Such an attitude, rooted in long-standing practices at governmental and enterprise levels, is out of step with good risk management in business, which takes into account the full spectrum of risk and assigns clear responsibility for addressing these.

Risk management lies at the heart of business strategy. Enterprises (as well as non-commercial organizations) draw up risk registers as part of a formal process to identify, analyse and evaluate the risks to its business and to put in place measures to address the risks, appropriate to their severity. The scope and scale of any facility's security function should be planned to be sufficient to address the risks it faces.

For the most part, the risks identified by an enterprise will involve a mix of external market factors and internal organizational and technical factors. The impact will be measured in terms of production down-time, revenue losses or additional costs incurred. Tolerable risks will include the normal commercial risks from undertaking business, for without accepting some level of commercial risk, the enterprise will not likely gain any reward. On the other hand, an intolerable risk could involve an event that puts the enterprise out of business or infringes regulations or the law. Any potential event that causes harm to the enterprise's workforce, its neighbours or customers should always fall into a 'reduce risk' or 'intolerable risk' category depending upon the severity of the consequences.

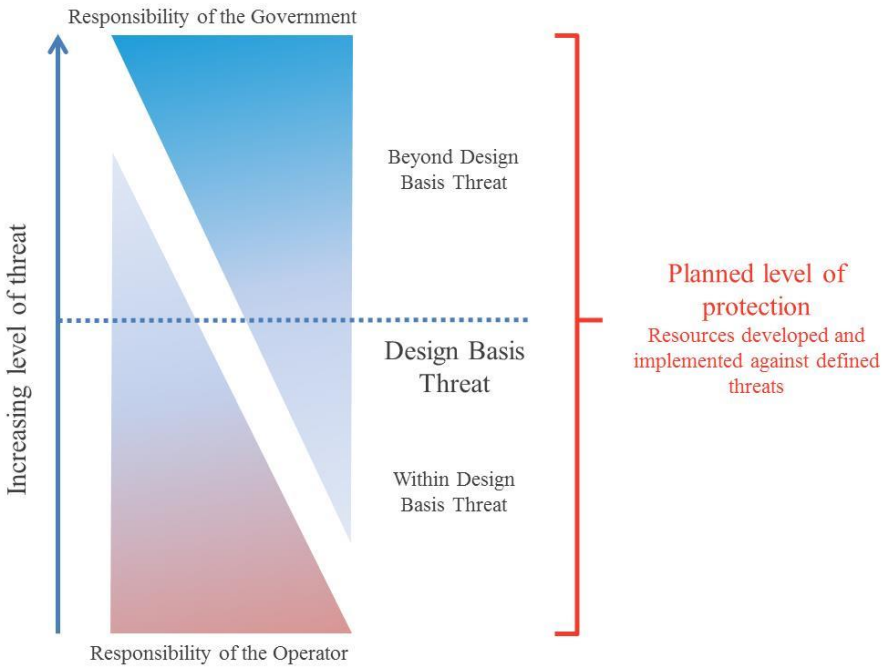
Some measures will involve putting in place contingency plans, taking out insurance, and controlling the factors that give rise to the risk, such as ensuring that personnel are properly trained to handle hazardous equipment or materials, and so on. Under the International Atomic Energy Agency's framework, operators of nuclear facilities are entirely liable for ensuring nuclear safety, whereas physical protection measures, which are the responsibility of the operator, form part of the overall national nuclear security regime established and maintained at governmental level. The operator of a nuclear facility is obliged to consider a set of threat scenarios defined by the government, known as the Design Basis Threat (DBT).

The DBT is used for development, establishment and sustaining of the appropriate measures for physical protection by the operators. It is the responsibility of the enterprise not only to ensure that its internal capability is sufficiently robust to deal with plausible events, but also that it can obtain additional assistance for any security risks that it is unable manage on its own, in compliance with existing national laws and regulations. In the event of an armed attack, for example, a nuclear plant should expect to receive rapid assistance from the police, gendarmerie or military. Procedures must be in place to enable the operator to draw upon such external assistance if and when required.

The state and the operator therefore share the responsibility for effective physical protection: the operator has the primary responsibility for mitigating the threats included in the DBT, and the state has the primary responsibility for threats exceeding the DBT limited by the maximum threat capabilities against which protection will be reasonably ensured [18]. The roles and responsibilities are illustrated in the following figure (Fig.1).

Senior management will want to see a business case for making the necessary investment or associated on-going running costs along the lines of a cost-benefit analysis. Such an evaluation is undertaken in order to ensure that the physical protection measures proposed are appropriate to meet the threats effectively; the need for risk reduction is not the issue and some form of preventive and protective measures must be undertaken regardless.

FIG.1: Responsibilities for protecting against threats



5. THINKING POSITIVELY ABOUT SECURITY

Concerns over terrorism have skewed the discussion within governments and civil society over nuclear security into trying to make nuclear facilities impregnable against unlikely threats just in case they were to occur. It can pull the security effort away from threats that are more likely to arise towards those that are less plausible but appear to be graver in their impacts. For example, a nuclear facility may well find itself under almost continual cyber-attack from a range of threat actors, including anti-nuclear hacktivists, fraudsters and other criminals and possibly even adversarial governments. The enterprise is probably in the best position to guard its computer networks from unauthorized intrusion, with the government providing advice on techniques to manage threats from its own cyber-security teams. The enterprise is less capable of withstanding a military-style assault without making considerable additional investment in its guard force, however.

The scope for a group of attackers, or hackers, to engineer some sort of radiological event at a nuclear facility that would result in a hazard to the site workforce or the public is limited. Nevertheless, the anxiety generated could be far higher than the true impact on health and the environment. The consequence of a security breach is therefore analogous to any other serious safety event, which carries a mix of objective hazards and psychologically traumatic impacts alongside reputational damage. Therefore, the operator of a nuclear facility should be expected to protect its assets from misuse and to protect people and the environment from the radiological consequences of malicious acts involving nuclear material under its control, and to be ready to communicate effectively in an emergency with the authorities and society. For its part, the operator should be afforded appropriate protection by the state from threats that are beyond the operator's capacity to manage.

The enterprise should also be permitted a degree of discretion over the form physical protection measures should take alongside its actions to ensure information confidentiality, human reliability and trustworthiness, and to engender a security culture. In this case, a balanced regulatory approach comprising of prescriptive and performance-based requirements could be the optimal solution. However, a mixed approach is suitable only when the operator possesses sufficient knowledge, skills and experience. It also depends on maintaining good communication between the operator and the police and security services, for example, in selecting routings for the transport of nuclear materials, which should allow for variation but also relies on local knowledge of the route that the operator may not be aware of.

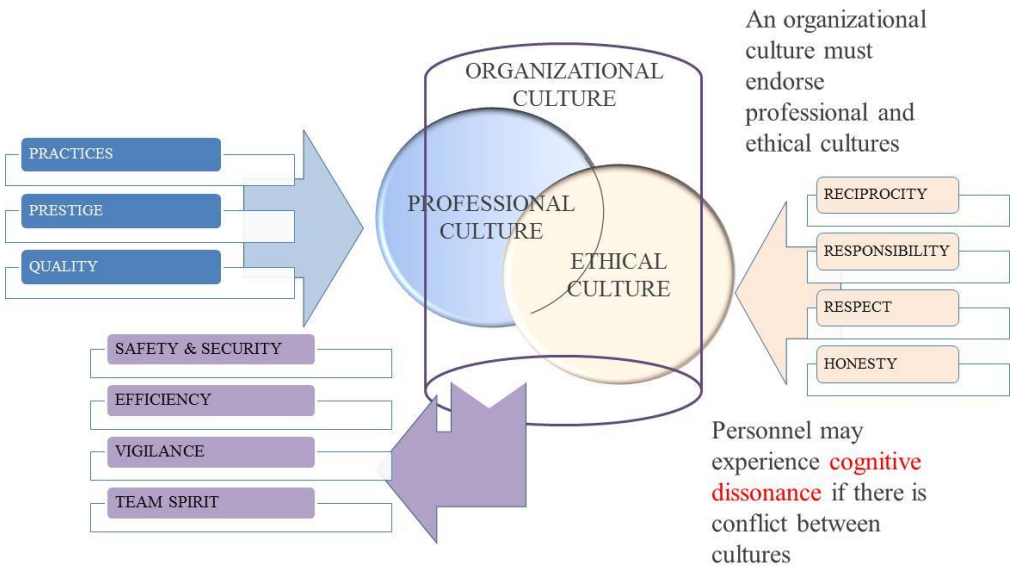
On the other hand, making sure that no-fly zones are respected by aircraft (of all sizes) would be normally a matter for the state. A guard force with capability to shoot down a manned or unmanned aircraft would need to be licensed to do so. In many countries only the state has the legitimate authority to use this level of potentially lethal force. Even where private guard forces are licensed to employ force, there are practical constraints as a result of the potential for civil litigation. People's civil and human rights must be respected and there is a danger that private security forces may not be regarded as legitimate guardians by local communities living around the facility, especially if guards undertake patrols beyond the site boundary.

Thus, from the point of view of an enterprise, physical protection of a facility or of materials during transportation aims at preventing any harm to people and the environment during an incident and the use of force should be limited to that necessary for self-defence. The objective is to prevent, detect and respond to an assault. This may be achieved through unobtrusive security at the perimeter of a site, where ditches and embankments are used to deter unauthorized entry. A determined intruder would then have to be prevented from proceeding further by rings of high fences until he or she is intercepted by the guards. Such a philosophy can be seen, for example, at new airport complexes.

Another important part of security at nuclear facilities is a security-conscious and conscientious workforce and an engaged and supportive community as its neighbour. Management at the facility has the responsibility for implementation measures for both nuclear safety and nuclear security. The management should also serve as an example of safe and secure behaviour. Nuclear safety and security must be coordinated from the very start and a culture for nuclear safety and security should be developed, established and fostered in the organization. It is important to instruct and train new employees; simultaneously, it is vital to constantly organize seminars, training and workshops in order to highlight the importance of safety and security culture.

Moreover the organization's corporate culture should endorse the ethical and professional cultures of its staff so as to reinforce the commitments to responsible behaviours and adherence to good practices. If there is a clash of cultures within the organization, staff could experience what psychologists call cognitive dissonance: Discomfort or psychological stress experienced when holding two contradictory beliefs or values or between a belief or perception and an action. Internal psychological conflict could be a trigger for some personnel to become insider threats. Theft of nuclear materials and information are crimes that are most easily perpetrated by insiders. Acts of sabotage committed by insiders have occurred in fuel cycle facilities and nuclear power plants, albeit without leading to serious consequences, such as a radiological incident.

FIG.2: Relationship between cultures in an organization



It is the responsibility of the organization's leadership and management to resolve any apparent or real conflict between the organization's values and objectives and the wider professional and ethical norms in society (see Fig. 2). Establishing a corporate culture where safety and security are priorities will encourage all

staff to be vigilant and conscientious. It will engender an *esprit de corps* (team spirit) that emphasizes that every member of the organization, including contractor personnel, is valued and contributes to the company's mission.

The World Nuclear Association's security working group prepared briefings to raise awareness of nuclear security issues which its member organizations are free to use in their personnel induction training and professional development.

6. COMMUNICATION WITH REGULATORY BODIES AND CIVIL SOCIETY

There is an increasing expectation that nuclear organisations (including both operators and regulators) should publish assurance reports for their stakeholders. An effective assurance regime recognises that assurance flows upwards from the operator where nuclear security is managed and implemented in accordance with the national and international regimes. The visible commitment of senior management to an effective assurance regime for security forms a key element to the further enhancement of nuclear security. The World Nuclear Association is encouraging its member organizations to report on security performance by raising awareness of the importance of nuclear security to corporate standing.

Many organisations publish annual reports on their corporate governance and commitment to social responsibility and environmental sustainability to provide such assurances, increase recognition and credibility with stakeholders, and to improve the board of directors' engagement with all aspects of operation. It is well recognised that a positive reputation for corporate responsibility is key to long-term business success. A well-governed company "always has a sustainable long-term plan in its sights", according to research undertaken for the World Economic Forum [19].

> "Leaders, at both the management and board levels, must become better storytellers about the company and its direction and must do a better job at making a case for a company's strategy and the level and duration of financial returns it will produce. By framing [its reporting] as a step in that longer-term story, stakeholders can not only foresee the expected destination, but also contextualize deviations from the expected path. … To improve the quality of engagement, it is important that consistent metrics be developed to measure the success of long-term strategies. These should cover performance beyond a purely financial story, extending to matters such as the strength of purpose and values, the effectiveness of the corporate governance framework, the loyalty and quality of the workforce and its morale and performance, the capacity for innovation, the sustainability of the supply chain and so on." [20]

Reporting on security to shareholders and other stakeholders with due consideration for the sensitivity of security-related information and legal requirements should add rather than detract from the company's public image and its engagement with its shareholders and other stakeholders. Too often, the prevailing attitude is that one should not talk about security because it might reveal too much to the industry's critics or to an adversary. The reassurance that a facility is protected through an appropriate physical protection system should be seen as a positive, although it should also be unobtrusive whenever possible to allay concerns that nuclear energy is itself threatening.

An enterprise must be sufficiently mature if it is to manage these different objectives: for operational safety and security; for business success; for employee morale; for social development and environmental sustainability; and for customer satisfaction. Integrating the security function into the enterprise's management system, including its approach to risk management, strengthens the facility's security and makes vigilance and preparedness part of its normal day-to-day activity. It establishes a line of accountability to senior management and the company's board. Regular reporting on security issues and performance, with due regard for the avoidance of disclosing sensitive information or infringing privacy and commercial confidentiality, can help improve public confidence and understanding.

The state has an important role as well, since, as already pointed out, if a nuclear facility is not secure then it poses a safety risk and the government will be ultimately held accountable by the public if anything goes wrong. It is the state's obligation to prevent nuclear facilities and radioactive materials from being misappropriated for terrorism and to define the competencies of the regulatory bodies assigned to supervise the nuclear industry. Striking the right balance is not easy so there has to be good communication between the

operator, regulatory bodies and security services but from the government side there must also be understanding of the commercial situation that the enterprise is working within.

The World Nuclear Association also seeks to contribute to maintaining an effective global framework for nuclear security through its representation as an observer at the IAEA's Nuclear Security Guidance Committee.

The theme of ICONS 2020 is "Sustaining and Strengthening Nuclear Security" at national and international levels. Fostering effective and efficient security regime in both established and embarking countries is vital to preserve a high level of stakeholder confidence in nuclear energy programs. It is also a prerequisite for the economic vitality of the sector. Assembling an enabling policy framework rests upon maintaining good communication between the nuclear industry, government and regulators, and other key stakeholders, so that all parties understand the constraints and choices involved.

ACKNOWLEDGEMENTS

The authors thank the members of the World Nuclear Association Security Working Group who contributed to the drafting of the paper, notably Taisiya Afanasyeva, Phil Litherland, Robert Rodger, and Laurence Williams.

REFERENCES

[1] IEA, Nuclear Power in a Clean Energy System, International Energy Agency, Paris (2019), pp. 3 and 17.

[2] IEA, Nuclear Power in a Clean Energy System, International Energy Agency, Paris (2019), p. 48.

[3] WORLD NUCLEAR ASSOCIATION, World Nuclear Performance Report, World Nuclear Association, London (2018), p. 12.

[4] JUNGK, R., Der Atom-Staat: Vom Fortschritt in die Unmenschlichkeit (The Nuclear State: From progress to de-humanization), Kindler Verlag, Munich (1977).

[5] LOVINS, A.B., Soft Energy Paths: Towards a durable peace, Harper & Row, New York (1979).

[6] HARVEY K., Anti-Nuclear Coalitions: Pacifism, radical action, and a rising atomic threat, Chapter 1 in HARVEY K., American Anti-Nuclear Activism, 1975-1990: The Challenge of Peace, Palgrave Studies in the History of Social Movements, Palgrave Macmillan, London (2014) pp. 12–41.

[7] LIBERATORE, A., The Management of Uncertainty: Learning from Chernobyl, Routledge, Abingdon (2013) p. 128.

[8] BLOWERS, A., The Legacy of Nuclear Power, Earthscan Routledge, Abingdon (2017) pp. 148 and 188.

[9] AUGUSTINE, D.L., Taking on Technocracy: Nuclear power in Germany, 1945 to the Present, Berghahn, New York (2018) p. 3.

[10] WITTNER, L.S., Nuclear Disarmament Activism in Asia and the Pacific, 1971-1996, The Asia-Pacific Journal, **7** 25-5 (2009).

[11] ANTHONY I., Reducing security risks by controlling possession and use of civil materials, in SIPRI Yearbook 2007, Stockholm International Peace Research Institute and Oxford University Press, Oxford (2007) p. 448.

[12] BOHIGAS X., Nuclear terrorism at a glance, Centre Delàs d'Estudis per la Pau, 13 February 2014 at <http://www.centredelas.org/en/armament/1311-una-ojeada-al-terrorismo-nuclear-2>.

[13] STAFF REPORTER, How we blew up Koeberg (… and escaped on a bicycle), Mail & Guardian (Johannesburg), 15 December 1995 at <https://mg.co.za/article/1995-12-15-how-we-blew-up-koeberg-and-escaped-on-a-bicycle>.

[14] NDOYE, G.W., Retour sur Malville: Chaïm Nissim á coeur overt (Return to Malville: Chaïm Nissim opens up), Continent Premier (Geneva), 4 July 2007, at <http://www.continentpremier.com/?article=1277&magazine=38>.

[15] AMANO, Y., IAEA Director-General's Statement, INDEX Conference on Nuclear Digital Experience, Paris, France, 26 June 2018 at <https://www.iaea.org/newscenter/statements/director-generals-statement-at-index-conference-on nuclear-digital-experience>.

[16] REPORTER, World Nuclear News, Kudankulam cyberattack no threat to plant operations, minister confirms, 22 November 2019 at <https://www.world-nuclear-news.org/Articles/Minister-confirms-details-of-Kudankulam-cyberattac>

[17] NUCLEAR INDUSTRY, Nuclear Industry Summit 2016 Joint Statement of 30 March 2016; at <http://nis2016.org>.

[18] IAEA, Development, Use and Maintenance of the Design Basis Threat, Nuclear Security Series No. 10, International Atomic Energy Agency, Vienna (2009) p. 6.

[19] WORLD ECONOMIC FORUM, The Modern Dilemma: Balancing Short- and Long-term Business Pressures, World Economic Forum, Geneva (2019) p. 10.

[20] WORLD ECONOMIC FORUM, The Modern Dilemma: Balancing Short- and Long-term Business Pressures, World Economic Forum, Geneva (2019) p. 8.