Chapter 9

Building a Nuclear Security Regime: Questions to Be Asked

Régine Gaucher, Thomas Languin, and Erik Ducouso

Contents

9.1	Introduction	174
9.2	State Sovereignty and Responsibility	176
9.2.1	What Place for Nuclear Security Within the State's Global Security System?	176
9.3	The Threat: Threat Assessment and Design Basis Threat	178
9.3.1	Against What Do We Need to Protect Ourselves?	178
9.3.2	What Security Burden to Be Placed on the Operator? What Level of Threat to Be Taken Into Account for Nuclear Security Regulations?	178
9.3.3	How to Take Into Account the Threat From the Design Phase?	179
9.4	The International Framework	180
9.4.1	How Does Nuclear Security Fit in at the International Level?	180
9.4.2	How to Manage Interfaces?	182
9.4.3	How to Balance International and National Issues?	182
9.5	The Legislative and Regulatory Framework	184
9.5.1	How can Nuclear Security Best be Integrated into the Global National Framework?	185
9.5.2	How to Choose Between a Dedicated Administrative Regime and a Common One with Other Areas?	186
9.5.3	Prescriptive Approach or Performance-Based Approach? What Approach Should a State Prefer?	186
9.6	The Nuclear Security Authority	188
9.6.1	An Authority Dedicated to Nuclear Security?	188
9.6.2	How to Guarantee the Level of Requirement Applicable to this Authority?	189
9.6.3	How to Guarantee the Level of Competence of the Authority?	190
9.7	Operators' Responsibility	191
9.7.1	What Is the Place and Responsibility of the Operator in Nuclear Security?	191
9.7.2	Why an Operator's Responsibility?	193
9.7.3	What Are the Nuclear Security Obligations of the Operator?	193
9.7.4	What Cooperation with Other Government Departments?	194
9.8	Choice of Technological Options, Sites and Transport Routes	195
9.8.1	How Can Nuclear Security Be Integrated Into the Choice of Technology?	195
9.8.2	What Are the Transport Issues?	195

R. Gaucher (✉) · T. Languin · E. Ducouso
Department of Nuclear Security, Ministry for an Ecological Transition, French Nuclear Security
Authority, Paris, France
e-mail: Official.Mail@iaea.org

9.8.3	How Can Security Be Integrated with Respect to the Site Chosen and Its Environment?	196
9.9	Confidentiality, Transparency and Communication	197
9.9.1	What Are the Communication Challenges in the Face of Terrorism?	197
9.9.2	Why Protect the Information?	198
9.9.3	How to Balance the Protection of Information and the Principle of Transparency in the Nuclear Sector?	198
9.9.4	How to Protect Information During the Management of a Crisis?	199
9.10	Conclusion	200
9.11	To Go Further... ..	201
	References	202

Abstract This chapter outlines some of the key questions to be asked by a State when considering a nuclear programme and thus a nuclear security regime. In the context of globalization and the emergence of a world in which States are interdependent, it is recognized that the way one State carries out its mission to protect nuclear materials and nuclear activities concerns other States also. In response to this, and despite the reluctance of States to expose their sovereign security practices, an international framework, composed of legally binding or non-binding tools, has been built up with the idea of promoting greater consistency and thus providing guarantees to all States. It is also important, for this one State, to comprehend the national and international context beyond nuclear security within which it falls. This State has then to question itself, in the light of security issues and the fundamental principle of State sovereignty, on the essential concepts that are found in certain components of the nuclear field, such as the positioning of the competent authority, the protection of information, transparency or the place of the operator.

Keywords Nuclear security • Nuclear security regime • Threat assessment • Design basis threat (DBT) • International framework • Legislative and regulatory framework • State sovereignty and responsibility • Convention on the Physical Protection of Nuclear Material (CPPNM) • 2005 amendment to the CPPNM • Prescriptive approach • Performance-based approach • Transport • Confidentiality

9.1 Introduction

The field of nuclear energy, and more particularly that of civil nuclear energy, leads a State to take into account multiple components when it considers setting up nuclear facilities or activities for industrial (nuclear energy for instance), medical or research purposes. Preventing any risk of unacceptable consequences for the population and the environment is one of the fundamental elements that a State must take into consideration at all times during its nuclear programme. This fundamental element has three components: nuclear safety and radiation protection, the guarantee of the peaceful use of nuclear activities (safeguards), and nuclear security.

Nuclear security was historically developed in the context of the Cold War, when the predominant threat was the use of nuclear materials to make a nuclear weapon.

This context led to the establishment of an international framework dedicated to the fight against nuclear proliferation (notably with the signing of the Non-Proliferation Treaty, which entered into force in 1970).¹ This framework sets out the obligations that a State must implement to prove that its facilities and the nuclear activities it carries out are not misused and that nuclear materials are not diverted by this State from their peaceful uses. To complement this principle of safeguards, nuclear security was initially developed to prevent the risk of theft and misappropriation of nuclear materials used in nuclear activities by malicious persons. Afterwards, this concept has been extended to all malicious acts and terrorist actions that could lead to radiological consequences. This includes sabotage of nuclear materials and other radioactive substances, of their facilities and transportation, as well as the risk of theft or misappropriation for the manufacture of radiological dispersion devices. It is therefore commonly accepted that the term nuclear security covers the prevention, detection and response to any act of theft, sabotage, unauthorized access, illicit trafficking or any other form of malicious act involving nuclear materials, radioactive substances or nuclear facilities.

The last decades have marked the international stage by the universalization of the challenges and a world where States are more and more economically, politically and socially interdependent. Therefore, multilateralism is a necessary step to meet some of these challenges.

The nuclear field is particularly concerned by this statement because of its universalization and the risks to go beyond the strict framework of the borders of a State. Terrorism is a mode of action and sometimes an objective. No State can escape from it. Everyone must therefore be prepared for this highly evolving threat, which follows and takes advantage of the slightest technological developments. The nuclear industry can be a prime target for this type of action, not only because of the consequences but also because of its impact on the population. This is why nuclear terrorism can take various forms.

Because of the universalization of nuclear challenges, it is commonly accepted that the way one State carries out its mission to protect nuclear materials, radioactive substances or nuclear facilities concerns other States also. That is the reason why, over the last three decades, a number of international instruments (legally binding, such as the Convention on the Physical Protection of Nuclear Material (CPPNM) and its 2005 Amendment,² or non-binding, such as codes of conduct or the IAEA's series of recommendations on nuclear security) have been drawn up. This international framework aims at both helping the States to strengthen their nuclear security regime and providing guarantees to others. This requires particular attention to consistency in the provisions put in place for this area of high challenges.

¹Treaty on the Non-Proliferation of Nuclear Weapons, opened for signature 1 July 1968, entered into force 5 March 1970 (NPT).

²Convention on the Physical Protection of Nuclear Material, opened for signature 3 March 1980, entered into force 8 February 1987 (CPPNM). Amendment to the CPPNM, entered into force 8 May 2016 (A/CPPNM).

However, it is important to note that what falls within the scope of national security corresponds to the fundamental principle of a State's sovereignty. The nuclear security measures put in place by a State, although they also aim to meet international objectives, are initially part of a national approach to protect its populations and its environment, related to its local context. Thus, the fundamental concept of sovereignty, which responds to the principles of the Westphalian system at the origin of the current international system, remains an essential element in the development of the international framework and in the work carried out in the various multilateral forums.

The purpose of this chapter is to present the important steps that a State wishing to establish a nuclear programme must take into account to build a nuclear security regime that responds, on the one hand, to its national context and challenges, and on the other hand, to the recommendations and good practices set by the international framework.

9.2 State Sovereignty and Responsibility

9.2.1 *What Place for Nuclear Security Within the State's Global Security System?*

It is internationally recognized that responsibility for nuclear security rests entirely with a State, as specified by two principles of the 2005 Amendment to the CPPNM³:

FUNDAMENTAL PRINCIPLE A: Responsibility of the State

The responsibility for the establishment, implementation and maintenance of a physical protection regime within a State rests entirely with that State.

FUNDAMENTAL PRINCIPLE B: Responsibilities During International Transport

The responsibility of a State for ensuring that nuclear material is adequately protected extends to the international transport thereof, until that responsibility is properly transferred to another State, as appropriate.

Nuclear security is an important component of national security and as such, it is fundamentally the role of a State. Since at least the 19th century, States have increasingly understood defence and security in a global way, war and economy being intrinsically linked.

Similarly, it is no longer possible to dissociate internal and external security. Recent events only confirm that external actions have a strong influence on internal security and vice versa. For example, the rise of the terrorist threat in France in recent years is inextricably linked to the international context and in particular to the actions of Al Qaeda and the self-proclaimed Islamic State, as well as to French policy against these organizations.

³A/CPPNM, above n. 1, Article 2a, para 3.

Thus, there is a continuum between crime, terrorism and State threats, and these different components of threats may have strong links.

In this context, nuclear materials, facilities and transportation, as well as the development of a nuclear programme, can represent important targets. To illustrate this, we can consider the computer attack carried out with the Stuxnet worm in 2010 on a uranium enrichment facility in the Islamic Republic of Iran, or the reading of Anders Breivik's manifesto,⁴ which calls for "using European nuclear power plants as a weapon of mass destruction".

Thus, a State that wishes to develop a nuclear programme will have to consider very early on the impacts of this programme on its defence and national security.

The first question to ask is the risk acceptance associated with nuclear power. The establishment of a nuclear security regime will therefore be an essential part to manage threats and risk. It should be borne in mind that the lower the risk that a State is prepared to accept, the higher the level of protection will be and therefore the more expensive it will be. Moreover, this level of acceptable risk, an eminently political choice, must be periodically confronted with changes in threats. Thus, in France, over the last few years, the combined effect of a greater demand for risk control by the population and a high level of threat has led to a very significant increase in the level of security required, and consequently in the human and financial efforts, both for the State and for nuclear operators. This aspect should not be underestimated because the cost of security can be significant and must therefore be taken into account in the economics of a project.

The State already has laws, regulations and institutions in place to deal with national security. It will therefore have to determine how to integrate nuclear security into this context (see Sect. 9.5.3) to establish its regime. For example, in France, nuclear security is regulated by the Code of Defence,⁵ which includes aspects related to the physical protection of nuclear materials, their installations and their transport (Article 1333) and aspects related to the protection of vital installations (Article 1332), dedicated to economic defence. Nuclear security is consequently dealt separately from nuclear safety, which is covered by the environmental code considering the prevention of pollution and environmental risks.

The fact that nuclear security is primarily a matter for States is significant, because it imposes particular constraints that are less common for nuclear safety. Indeed, if the responsibility for the implementation of safety can be entirely given to the operators, this is not the case for security, which always requires State resources. The choices made by the States will have a strong influence on the way to develop international cooperation (see Sect. 9.4), the legislative and regulatory framework (see Sects. 9.5.3 and 9.6) and communication (see Sect. 9.9).

⁴Breivik 2011.

⁵Code de la Défense 2021, pp. 236–252. <https://codes.droit.org/PDF/Code%20de%20la%20d%C3%A9fense.pdf>. Accessed 30 August 2021.

9.3 The Threat: Threat Assessment and Design Basis Threat

9.3.1 Against What Do We Need to Protect Ourselves?

One of the main markers of a State's sovereignty in the field of nuclear security is its design basis threat (DBT). This is generally national and confidential security information, which is protected accordingly.

Regardless of the fact that a protection system for nuclear activities must meet obligations of means (prescriptive approach) or objectives of results (performance-based approach), the purpose is always the same: to protect against an identified and characterized threat.

Among the many responsibilities of a State, a primary question will be to identify the threats that its country faces and therefore that could affect its activities. This analysis requires the involvement of government services and agencies in charge of national security (e.g. police, intelligence, cybersecurity). It must be based on known events in the country but must also include what is happening abroad.

9.3.2 What Security Burden to Be Placed on the Operator? What Level of Threat to Be Taken Into Account for Nuclear Security Regulations?

When it comes to protecting specific activities, such as those related to the nuclear sector, which are particularly relevant to the terrorist threat, the State faces a political choice. It is difficult to imagine, considering the exhaustiveness of the threats identified, that a State would decide to place the protection of nuclear activities exclusively on its operators. The State can therefore decide either to carry sole responsibility or to adopt a complementary approach between the public authorities and the operators. The use of the first solution by a State would lead to a complete disengagement of the operators, which would not make sense.

Effective security cannot exist without the benefit of the knowledge and experience of the operators, especially when dealing with facilities as technically and organizationally complex as those that we find in the nuclear sector (e.g. interfaces between security and other risks inherent to the facility). The insider threat is a relevant example that highlights the major role of operators both to prevent the emergence of such a threat within their own organization, but also to protect themselves as effectively as possible from it (anticipatory measures). It is true that the State plays an essential role, particularly in the context of a trustworthiness programme, but alone it would not be effective.

Thus, it is commonly accepted by the international community that a complementary approach is preferable to ensure the protection of a nuclear activity. This is

particularly expressed in security plans aimed at defining the strategies adopted to detect, slow down, stop the progression and neutralize the threat. In this situation, the State must decide which of the previously identified threats the operator must be able to respond to with its own resources. This is generally referred to as the design basis threat, or DBT, used for the design and evaluation of protection systems in the IAEA recommendations.

9.3.3 How to Take Into Account the Threat From the Design Phase?

To be effective, nuclear security must be considered as early as possible in the design of a project (whether it is a new activity or a modification of an existing activity).

This implies that States must begin by defining a DBT when they wish to embark on a nuclear programme. The applicable national legislative and regulatory provisions must be added to this DBT. This set of elements is essential for any State wishing to promote a ‘security by design’ approach. This approach is achieved by combining an inherently secure design with inherent features of the facility that will help reduce the number of targets, allow better mitigation of the potential consequences of the remaining vulnerabilities, and thus facilitate proactive physical protection to address the facility’s vulnerabilities. Such a ‘security by design’ approach is qualified as an ‘integrated approach’ since it includes safety aspects and maintenance in addition to nuclear security.

Threat modes of action and means evolve over time. The concept of ‘security by design’ makes it easier to take into account both current threats and to anticipate their evolution during the lifetime of a facility. For example, space can be designed for additional physical protection systems. In the continuity of the constant evolution of the threat, it is relevant for a State to periodically foresee a re-examination of its DBT and of the obligations of the legislative and regulatory framework that result from it.

As mentioned above, this DBT applies to the operator, but it is also an essential element for the State internal security forces concerned. As part of a complementary approach, the State internal security forces can intervene on the facility to provide assistance to the operator’s forces to secure the area, or to stop the security crisis.

Some threats, such as cyberattacks or even overflights of drones, are means available to malicious persons to make more difficult or even prevent the intervention of State internal security forces. It will then be relevant to identify appropriate interdisciplinary practices to enable an effective response in all circumstances and to define coordinated strategies for managing potential malicious acts.

9.4 The International Framework

9.4.1 *How Does Nuclear Security Fit in at the International Level?*

The objective of nuclear law, as presented in the literature,⁶ is to provide a legal framework to conduct activities, which involve nuclear energy and ionizing radiation in a manner that adequately protects individuals, property and the environment. As mentioned above, the universalization of civil nuclear issues has led to the development of a number of international instruments, both to help strengthen physical protection and to promote greater coherence in the provisions of the nuclear field. However, nuclear security, like the other components of the nuclear field, brings together several tools (legally binding or not), both at the international and national levels (see Sect. 9.5.3). At the international level, each of these different components responds to specific logics and aims to achieve broader objectives related to security, or even to other areas closely linked to nuclear security, without this being its main concern. It is therefore necessary for a State to be able to know and understand these important interfaces in order to adopt a policy that meets both national needs and expectations, while responding to the various international concerns.

To understand the international framework for nuclear security, it is necessary to begin with the United Nations (UN), whose history is linked to that of nuclear power. The very first resolution adopted by the UN General Assembly on 24 January 1946,⁷ was to establish a committee to deal with the problems raised by the discovery of atomic energy and other related issues. The normative role of the UN to fight against terrorism has led them to take a large number of decisions, often in the form of resolutions. Among these various resolutions, some relate to nuclear security. For example, UN Security Council Resolution 1540 (2004),⁸ although primarily concerned with preventing the proliferation of nuclear weapons, refers to measures “required by the Convention on the Physical Protection of Nuclear Materials and those recommended by the IAEA Code of Conduct on the Safety and Security of Radioactive Sources”. It calls on States to “develop and maintain appropriate effective physical protection measures”. With its resolution 51/210 of December 1996,⁹ the United Nations initiated three international treaties that are relevant to the international framework for nuclear security: the International Convention for the Suppression of Terrorist Bombings, the International Convention for the Suppression of the Financing of Terrorism and the International Convention for the Suppression of Acts of Nuclear Terrorism.¹⁰

⁶Stoiber et al. 2003.

⁷UNGA 1946.

⁸UNSC 2004, pp. 2–3.

⁹UNGA 1997.

¹⁰International Convention for the Suppression of Terrorist Bombings, opened for signature 12 January 1998, entered into force 23 May 2001. International Convention for the Suppression of the

The main objective of the International Atomic Energy Agency (IAEA) is to promote, together with its Member States, the safe, secure and peaceful use of nuclear technologies and applications. To this end, it encourages Member States to ratify the conventions and codes of conduct of which it is the depository. It also conducts a wide ranging assessment of nuclear security, needs, priorities and threats, particularly those related to terrorism. The IAEA thus supports the establishment of international partnerships and networks. It also develops non-legally binding instruments, consisting of recommendations, guides and technical or operational procedures that form the Nuclear Security Series of publications. The IAEA also offers services to States, such as the International Nuclear Security Advisory Service (INSServ). This service is designed to assist States in establishing and maintaining effective nuclear security regimes. There is also the International Physical Protection Advisory Service (IPPAS) programme, which is a fundamental element of the IAEA's nuclear security strategy. It proposes assistance to Member States, upon request, in evaluating their physical protection regimes. This evaluation includes a review, at the national level, of the legal and regulatory framework, as well as the measures and procedures implemented in facilities and during transport to meet regulatory requirements. The assessment is based on the requirements defined in international instruments, as well as in IAEA recommendations and guidance. These include the main texts listed here, together with all other relevant IAEA documents, including the Nuclear Security Series of publications or other guidance/recommendations: the CPPNM and its 2005 Amendment, the Fundamental Principles and Objectives of Physical Protection (IAEA GOV/2001/41),¹¹ the IAEA's Code of Conduct on the Safety and Security of Radioactive Sources,¹² as well as IAEA Nuclear Security Series publications No. 20, No. 13 and No. 14.¹³

The CPPNM is an international treaty adopted on 26 October 1979. It came into force on 8 February 1987.¹⁴ It is one of many international tools against terrorism and remains the only legally binding instrument dedicated to the physical protection of nuclear materials. It is a convention whose technical provisions deal with the protection of nuclear materials during international transport, while its penal provisions, and those relating to judicial cooperation, are also applicable to nuclear materials in use, storage or transport on national territory. In 2005, an amendment to the CPPNM was adopted. It aims, in particular, to extend the scope of application of the CPPNM to nuclear materials in use, storage and transport on national territory. It also introduces the twelve fundamental principles of the physical protection (responsibility of the State, responsibilities during international transport, legislative and regulatory framework, competent authority, responsibility of the licence holders, security

Financing of Terrorism, opened for signature 10 January 2002, entered into force 10 April 2002. International Convention for the Suppression of Acts of Nuclear Terrorism, opened for signature 14 September 2005, entered into force 7 July 2007.

¹¹Fundamental Principles and Objectives of Physical Protection (IAEA GOV/2001/41).

¹²IAEA 2004.

¹³IAEA 2011a, b, 2013.

¹⁴CPPNM, above n. 1.

culture, threat, graded approach, defence in depth, quality assurance, contingency plans, and confidentiality). Therefore, when a State considers embarking on a civil nuclear programme, it is strongly recommended that it becomes Party to these two international instruments: the CPPNM and its Amendment.

9.4.2 How to Manage Interfaces?

This brief introduction, which defines the main tools that constitute the international framework for nuclear security, illustrates that nuclear security is intrinsically linked to a much larger set of international laws that address specific concerns and that may sometimes go beyond the nuclear sector.

Nuclear security is only one part of the nuclear issues. An identical situation exists for nuclear safety and radiation protection, as well as for safeguards. These different components, although responding to a common objective of protecting the population and the environment from the risks represented by nuclear energy, have their own goals and therefore have their own logic. It is therefore important to identify and evaluate the necessary interfaces so that each of the components can achieve its fundamental objective without compromising the global finality. The current international organization consists in allowing the development of an international framework specific to each component of the nuclear sector under the supervision of a single organization, the IAEA. The IAEA has put in place an organization that allows experts from the different Member States to efficiently build and develop the international framework related to their field of specialization. This allows them to take into account the considerations of other related fields outside the nuclear sector, while providing the necessary bridges to identify and deal efficiently with the interfaces with the other components of the nuclear field. This approach avoids the situation where all nuclear issues are brought together under a single international framework. Although this approach could be understood from the point of view of interface management, it may have disadvantages that should not be overlooked.

One of the main risks would be to fall into a restrictive nuclear approach, with the effect of distancing experts from a particular field in favour of generalist profiles. Such a situation would not allow the necessary relationships with other related components. In the long term, this could lead to isolating the nuclear sector from the broader context in which it is embedded and with which interfaces are indispensable.

9.4.3 How to Balance International and National Issues?

As mentioned before, nuclear security is a component, sometimes a very important one, of a State's national security. The current context is marked by the universalization of issues and a world where States are increasingly interdependent. This does not mean that certain major principles that have governed international relations for

many decades have disappeared, such as the sovereignty of States, the self-interest of States (the COVID-19 health crisis is a concrete and recent example), or the tensions between States that evolve over time. In this context, nuclear security must be approached in an international context with great caution. The fundamental principle of confidentiality, introduced by the 2005 Amendment to the CPPNM, has a very particular relevance in the framework of multilateral relations set up in order to face the challenges of the global threat of the nuclear sector, even if its scope is primarily national. To guarantee the confidentiality of sensitive information of the physical protection system, for example, is an essential element.

In other nuclear fields (such as nuclear safety or radiation protection), transparency associated with a convergence of practices representing the state of the art makes sense. The risk to which the measures in these fields must respond are climatic hazards, material failures or the result of human actions without malicious intent. It is certainly evolving, but it does not adapt to the situation it faces. This standardized approach therefore makes it possible to respond efficiently to the objective of a high level of protection shared by all and to the need for confidence in their implementation requested by the various States and by the civil society. The consequences of a nuclear accident will necessarily have a transboundary, radiological, economic or social effect.

In the area of nuclear security, and security in general, the threat faced by States has this capacity to adapt itself, since by definition it is a malicious human action. Thus, contrary to the objectives in areas that allow transparency, it is appropriate to think that any attempt to move towards more transparency and convergence on common practices in nuclear security may be suspected of false naivety from some States, or even of manipulation, in order to obtain information. In this context, the fundamental principle of confidentiality is of particular importance for States, and refers to the importance, in the field of security, of finding the right balance between what can be shared and what must remain known only to those who need to know.

The emergence of international treaties in recent decades is explained by a growing adhesion to various elements of the international society. Common interests of States, which face problems that they cannot solve alone, drive the need to address issues in a multilateral framework. As highlighted earlier in this chapter, today's nuclear security challenges are global. There is therefore a strong need for States to engage the international community in addressing these issues. Conventions, such as the CPPNM and its Amendment, are the most appropriate instruments. Encouraging States to ratify these instruments and to participate in review conferences is the first, and certainly the most important, step to ensure a global strengthening of nuclear security. However, there are different degrees of application of these tools. On the one hand, there is a political aspect, where the objective is to ensure that the States Parties share a common appreciation of the challenges and of the efforts that need to be made to address them. On the other hand, there is a technical aspect, the aim of which is to ensure that international instruments can have a concrete effect on the physical protection measures taken by the States Parties.

These two aspects highlight the basic principle of the enforcement of any international treaty, which is based on the good faith of States Parties and its inherent unverifiability. This reflects the need for trust (to be understood in the sense of reliance on one's word) among the parties, which is the essential for good faith concept. This is particularly relevant when tools such as the CPPNM and its Amendment are considered from a technical perspective. Verifying, in a concrete and qualitative way, that the measures taken by States allow them to achieve a sufficient level of security with respect to the threat they face, is difficult to achieve in the framework of a multilateral forum. The principles of confidentiality and sovereignty of States in the security area will constrain the exchanges, referring to the need for trust between States. Potentially, certain barriers could be removed in more limited exchanges, such as at regional or even bilateral levels, when common interests are found and when a relationship of trust can be established. These constraints are duly taken into account for IAEA peer review missions (IPPAS), where the host country can choose, among a pool of international experts from several countries, experts from countries with an appropriate relationship.

After many years of development under the leadership of the IAEA, the international nuclear security framework has reached such a level of maturity that it is difficult to identify any short term needs for structural development. This observation is in accordance with the fact that relations are to be further developed at the regional and even bilateral levels. Nevertheless, it is necessary for the IAEA to maintain a central role to coordinate international cooperation. This means, in particular, assistance to States such as the organization of training and peer review missions (IPPAS) or the provision of services such as INSServ.

The IAEA must continue to facilitate international cooperation to enable States to maintain an adequate level of nuclear security in the long term. Furthermore, workshops, conferences and other events allow the establishment or maintenance of an international network of specialists, where each State can find good level partners when it wishes to share and obtain a reference information on an identified subject. The IAEA's role is also essential to enable the establishment of the bridges that are crucial to the identification and an appropriate management of the interfaces between the three components of the nuclear sector, while guaranteeing the respect of their singularity for the proper integration of considerations from their related environments going beyond the concerns of the nuclear sector.

9.5 The Legislative and Regulatory Framework

Another important responsibility of the State is to establish the legislative and regulatory framework, as reiterated by Fundamental Principle C of the CPPNM¹⁵:

FUNDAMENTAL PRINCIPLE C: Legislative and Regulatory Framework

¹⁵ A/CPPNM, above n. 1, Article 2a, para 3.

The State is responsible for establishing and maintaining a legislative and regulatory framework to govern physical protection. This framework should provide for the establishment of applicable physical protection requirements and include a system of evaluation and licensing or other procedures to grant authorization. This framework should include a system of inspection of nuclear facilities and transport to verify compliance with applicable requirements and conditions of the license or other authorizing document, and to establish a means to enforce applicable requirements and conditions, including effective sanctions.

9.5.1 How can Nuclear Security Best be Integrated into the Global National Framework?

The regulation on nuclear security is part of a rich legislative and regulatory framework already in place. As the IAEA Handbook on Nuclear Law reminds us,¹⁶ it is important to note that there is no single definitive model for nuclear regulation. This is particularly true for nuclear security, considering its many regulatory interfaces with other regulations:

- Protection of information;
- Protection of vital infrastructures;
- Protection of information systems;
- Regulated professions, linked to national security, for which administrative inquiries or vetting may be required;
- Regime for the possession and use of weapons;
- Regulation and limitation of land, air and sea space;
- Crisis management.

In view of the above-mentioned interfaces and as indicated in Sect. 9.2, nuclear security is a component of national security. As such, it will be part of the public debate on security and its balancing with public liberties.

For example, a trustworthiness inquiry is required to identify situations where people may present vulnerabilities, which do not allow them to access nuclear sites or to perform sensitive functions in the nuclear field. In France, the operator requests such an inquiry by the competent administrative authority. They may seem intrusive and contrary to freedoms. However, it is essential to note that the rules that are imposed are public and known to all and offer possibilities of appeal for people who feel they have been unfairly excluded from sensitive positions for which they have applied. The freedoms are not absolute but are exercised within the legislative and regulatory framework that governs them. The administrative authority gives the operator an opinion on the vulnerability that the person may represent. The decision to give access is then up to the operator.

It is therefore essential to define, with the utmost rigour, the notion of a ‘sensitive position or sensitive information’ in order to ensure a good balance that meets the security challenges. For example, many people may be involved in the preparation

¹⁶Stoiber et al. 2003.

of a transport of nuclear material, which requires complex logistics. This could lead to the organization of controls on a large number of people. The question of the feasibility and proportionality of the measures in relation to the impact on public liberties must be taken into account.

The security challenges are so important that the legislator has decided to make access to installations or information subject either to a trustworthiness inquiry procedure or to a national defence clearance procedure, which is based on a strengthened trustworthiness inquiry. This is the case for the nuclear industry. The clearance procedure must be applied to jobs listed in a catalogue established by the competent ministry. The absence of a clearance procedure is cause for dismissal.

In response to threats, the question of an armed response inevitably arises. The possession and use of weapons is cultural and therefore varies greatly among countries. In France, it is highly regulated and is only possible outside the State forces in very specific cases governed by the code of internal security. In the nuclear sector, operators may have an internal armed service or, more recently, may call on an armed service from an external source.¹⁷ This answers the need for a first response to the threat, which requires a rapid kinetic.

9.5.2 How to Choose Between a Dedicated Administrative Regime and a Common One with Other Areas?

What place should nuclear security have in the regulatory framework of a State? It is undoubtedly possible to integrate nuclear security into existing processes for safety, the environment protection, critical installations, defence, national security, radiation protection, etc. However, there is a risk that the specificities of nuclear security will not be properly addressed, that certain conflicts of objectives or means will not be identified, and that choosing between options will not be possible. This is why France has chosen a regime specific to nuclear security and decided to assign its responsibility to a State authority.

9.5.3 Prescriptive Approach or Performance-Based Approach? What Approach Should a State Prefer?

A prescriptive approach consists in setting out very precisely the obligations of an operator, and in particular the means to be used. This approach has the advantage of being more comprehensive and easier to implement by the operator and by the competent authority to control.

¹⁷Decree No. 2017-1844 of 29 December 2017, and Ministerial Order of 15 November 2019, issued to implement Article 35 of the Decree.

This approach is well adapted to setting a minimum level of requirements even in a context where operators are not familiar with security culture. This approach is used in France for the security of radioactive sources and in the case of nuclear materials for transport and installations with the lowest risk (categories III and below). However, it has limits because the requirements may become obsolete in the short to medium term with changes in technology and in terms of the threat. Particular care must also be taken to avoid any conflict with the requirements of other fields such as nuclear safety and radiation protection. For example, in the case of radioactive sources, information concerning the location of their detention was initially considered as sensitive, and therefore should have been restricted. However, from the point of view of radiation protection, which requires the reporting of any potential danger linked to a source, this information must be communicated widely.

A performance-based approach consists of setting results-based objectives for the operator and leaving it up to the operator to determine the means to achieve them. This approach makes it possible to achieve higher levels of protection but requires a very high level of expertise on the part of the operators and the people in charge of control.

This approach has the advantage of being able to adapt more easily to the different installations encountered, to operating regimes, to the location, etc., but also to technological developments and to changes in the threat. It also allows the development of original solutions, specific to each operator and therefore less known. Finally, it does not need to be revised frequently in order to keep up with current events. In France, this approach prevails for high risk nuclear facilities. The requirements set in 2009 have remained valid despite changes, feedback and lessons learned from computer threats, drones attacks, etc.

The performance-based approach also makes it possible to achieve very high levels of security, because it forces the operator to design a nuclear security system that is very effective and very well adapted to the object to be protected. In particular, assessing the performance reached allows to identify residual vulnerabilities and to plan the necessary reinforcements. Typically, in France, this approach has led to substantial progress. Security resources that seemed very strong at first turned out to be insufficient: a very important lesson was to show that it is not enough to put together a huge set of resources to be effective. This has led several operators to change their security strategy and to design different and often more important means in order to reach the required performance.

Such an approach requires a very high level of expertise, both from the operators and from the authorities. This has required an increase in skills and staff within the authority. In fact, the assessment of performance achievement is evaluated during the examination of applications for authorization, both at the time of the initial application and at the time of periodic re-evaluations or when changes are made to the infrastructure or operating procedures.

Over the past five years, the French authority has therefore set up a special authorization process called 'in-depth technical examination'. This process consists, first, in identifying the most important technical questions in an operator's security demonstration and, second, for the authority to refer the matter to its technical support (in

France, the IRSN),¹⁸ which will discuss the issues raised with the operator and provide the authority with argued recommendations. Depending on the nature of the requests for expertise and the complexity of the subjects, this analysis may take several months, even years. This process will include meetings during which the authority will decide on potential differences of opinion between the operator and the IRSN.

Of course, this file examination is only one part of the evaluation. The authority also carries out a number of on-site inspections to test the operator's strategy. These checks can lead to questioning solutions that seemed solid on paper. Tests, including destructive ones, may also be requested to support the operator's demonstration, for example to test the resistance of barriers to crossing or destruction by explosives. Finally, exercises to assess overall security are also implemented and are used to identify any weakness in the operator's security demonstration.

This approach is the one that allows the best response to fit with changes. This is a challenge when you consider that nuclear facilities have a lifetime of several decades. It is therefore necessary to have a vision that goes beyond present conditions. A forward looking vision that considers possible evolution is important.

9.6 The Nuclear Security Authority

Nuclear security, to be effective, must be controlled by an authority as provided for in Principle D of the CPPNM¹⁹:

FUNDAMENTAL PRINCIPLE D: Competent Authority

The State should establish or designate a competent authority which is responsible for the implementation of the legislative and regulatory framework, and is provided with adequate authority, competence and financial and human resources to fulfil its assigned responsibilities. The State should take steps to ensure an effective independence between the functions of the State's competent authority and those of any other body in charge of the promotion or utilization of nuclear energy.

9.6.1 *An Authority Dedicated to Nuclear Security?*

The question may then arise of setting up an authority separate from that in charge of nuclear safety, for example.

The principle adopted in France is that of a single authority in charge of regulating nuclear safety and nuclear security, the minister in charge of energy, who has two different departments: one in charge of safety, the General Directorate for Risk Prevention (DGPR), and one in charge of security, the Department of the High Official for Defense and Security/Department of Nuclear Security (SHFDS/DSN). The

¹⁸IRSN: Institut de Radioprotection et de Sûreté Nucléaire.

¹⁹A/CPPNM, above n. 1, Article 2a, para 3.

law has also designated an authority independent from the government,²⁰ the Autorité de Sûreté Nucléaire (ASN) to control the implementation of safety regulations by operators.

The choice of an authority independent from the government cannot be made for security, since the control concerns not only the operators but also the government services that contribute to nuclear security as explained above. The advantage of this system is that it ensures a global vision and a high degree of coherence between the actors, whether they are State authorities or private authorities.

Many countries, especially when they start drawing up the development of a nuclear security regime, will be interested in the creation of an authority that will be in charge of all the aspects of nuclear energy. This of course often makes a lot of sense, especially from a practical point of view. However, we must not forget all the issues mentioned above.

The nuclear security authority will necessarily need to have strong links with ministries and other agencies. In this respect, there should be no misunderstanding about the independent nature of the authority. In matters of nuclear security, this independence could only be relative. It is difficult to see how an authority independent from the government could evaluate the response provided by the ministries involved in national security. However, as was indicated earlier, nuclear security should not be reduced to the premises of the operators alone. Nevertheless, it is important that the choice of a State authority is not contradictory to Fundamental Principle D: independence is required with respect to the organizations responsible for the promotion and use of nuclear energy.

9.6.2 How to Guarantee the Level of Requirement Applicable to this Authority?

The main reason for requiring independence regarding the promotion of nuclear activities is to ensure that the authority cannot be influenced in its decision process by political or economic issues.

One option is to limit the role of the competent authority strictly to that of control and to have a regulatory body that must also meet the objective of independence. Under these conditions, the authority in charge of control does not set the rules itself. It ensures only that the legislative and regulatory framework is implemented. If the framework provides that any failure to comply with the rules must be acted upon by the competent authority, this authority will not be in a position to modify the rules in order to take a decision in favour of the operator. It will therefore have to act appropriately in accordance with the national legislative and regulatory framework.

²⁰Independent administrative authority: a State entity, with no legal duty but with its own power, in charge of one of the following missions: to ensure the protection of citizens' rights and freedoms, to ensure the proper functioning of the Administration in its relations with its citizens or to participate in the regulation of certain sectors of activity.

However, such an organization is not sufficient. A national regulation, whose objectives are not in line with the minimum requirements set by the international framework (the CPPNM, its Amendment and application guides), will be considered adequate by the national authority without guaranteeing a sufficient level of security.

Compliance with the international framework is therefore a very important protection. To this end, a process to promote universalization of the CPPNM and its 2005 Amendment is needed. It includes inviting all States to demonstrate compliance with the international framework through the information required under Article 14.1 of the CPPNM, encouraging them to use IPPAS missions to ensure that their regime complies with the CPPNM and to demonstrate to the rest of the international community their commitment.

While the requirements of the CPPNM should be seen as the minimum level required, they are not necessarily sufficient for a State, which must therefore compare this level with the threats it has assessed. For States with high risk nuclear facilities, this review again argues for the implementation of a performance-based approach (see Sect. 9.5.3).

The ability of a State to have a high level of security will depend on the capacity of its services to evaluate in a simple and sincere way the efficiency of the system it has set up. This requires courage, when the expectations are more often to reassure politicians and the population than to raise awareness of the challenges, to demonstrate efficiency and competence rather than to point out the limitations and the need for progress. An efficient evaluation requires full-scale exercises or simulations, which combine the response provided by the operator's and the State's resources, and which are based on scenarios consistent with the relevant threat level. We need of course scenarios, which are unexpected. Nothing is worse than a long-prepared exercise, where everyone expects what is going to happen and has been able to plan how to react, only to have the 'scenario' played out. Additional evaluation methods exist via simulations (reduced scale or numerical tools) but also via experience feedback.

9.6.3 How to Guarantee the Level of Competence of the Authority?

At the technical level, nuclear security requires a wide range of skills that are not necessarily all gathered within the nuclear security authority. For example, in the field of drones or computer security, the nuclear security authority must often rely on the expertise developed by other State services. If the specificities of the nuclear industry can be reduced to identifying the targets to be protected, the evaluation of the offensive capacities of the threat and the means to face them are common to all domains (banking domain, penitentiary domain, etc.). Specialists can be found in other authorities involved in national security. In France, for example, we can mention the National Agency for Security of Information Systems (ANSSI).²¹

²¹This agency depends on the Prime Minister.

The essential cooperation as indicated above leads to the need of, in matters of nuclear security, an authority placed at a good hierarchical level in a government to be able to set a relevant legislative and regulatory framework.

The various competencies will thus be coordinated, under the leadership of the nuclear security authority. The various actors will be able to participate in the implementation of the control. This will be the case, for example, for the police or the army to control the armed response measures of the operators, or for cybersecurity agencies to control the protection of information systems, etc.

In France, it has been decided that no additional requirements should be introduced for nuclear security to those that already exist in the general regulatory framework for information system security. Therefore, work is being carried out in cooperation with the ANSSI to specify how to apply this general framework to the specific subject of nuclear security and to take advantage of synergies and complementarities of approaches, particularly in the context of the control of operators (inspections and exercises).

9.7 Operators' Responsibility

Another fundamental principle established by the CPPNM is the responsibility of operators²²:

FUNDAMENTAL PRINCIPLE E: Responsibility of the License Holders

The responsibilities for implementing the various elements of physical protection within a State should be clearly identified. The State should ensure that the prime responsibility for the implementation of physical protection of nuclear material or of nuclear facilities rests with the holders of the relevant licenses or of other authorizing documents (e.g., operators or shippers).

However, in some regulatory models such as the French one, the place of the operator in nuclear security is not as obvious as it may seem.

9.7.1 *What Is the Place and Responsibility of the Operator in Nuclear Security?*

The State must consider the place and responsibility of the operator in relation to that of the State. At first glance, in a model such as the one in France, it does not seem obvious that nuclear security should be given to an operator. Indeed, the Civil Code,²³ one of the fundamental texts of French law, virtually unchanged since Napoleon I, sets out the principles of liability:

²²A/CPPNM, above n. 1, Article 2a, para 3.

²³Translations taken from Cartwright et al. 2016.

Article 1241

Everyone is liable for harm which he has caused not only by his action, but also by his failure to act or his lack of care.

Article 1242

One is liable not only for the harm which one causes by one's own action, but also for that which is caused by the action of persons for whom one is responsible, or of things which one has in one's keeping.

The responsibility of an operator in matters of nuclear safety can be interpreted as the application of these above-mentioned principles to the particular case of nuclear field: the operator has a nuclear installation under his responsibility. The operator is in charge of operating a nuclear installation that presents risks likely to cause very significant damage, and it is the operator's responsibility to apply measures proportionate to these risks.

However, what about nuclear security? These above-mentioned principles imply that one is not responsible for damage caused by the act of others. This is illustrated by the Franck decision of 2 December 1941,²⁴ famous for having set an important case law. In this case, Dr. Franck had lent his car to his son. The car was stolen and the thief, whose identity remained unknown, struck and fatally injured a postal worker. The court then ruled that Dr. Franck was not liable for the damage caused to the postal worker.

Thus, if we come back to the nuclear field, is the operator considered responsible if a malicious person intentionally attacks an operator to cause damage to its facilities?

If we return to the international framework, and to the conditions of nuclear liability, we see that these above-mentioned principles, provided in particular by the Paris Convention,²⁵ are adapted to cases of accidents due to a nuclear safety problem. However, its application in the case of malicious acts, in particular terrorist acts, seems less obvious.

Thus, in France, nuclear security is based on conditions that must be met by operators in order to carry out their nuclear activities. Their responsibility in this area is not engaged automatically. It is strictly limited to the application of the provisions required by the regulations. This is a fundamental difference from nuclear safety, where the operator's responsibility is engaged systematically and where it is up to the operator to determine the means to ensure nuclear safety.

²⁴Cour de cassation - Chambre réunies, *Connot v Franck*, 2 December 1941, No. N, Bull. civ., N. 292 p. 523. <https://www.doctrine.fr/d/CASS/1941/JURITEXT000006953144>.

²⁵Convention on Third Party Liability in the Field of Nuclear Energy of 29 July 1960, as amended by the Additional Protocol of 28 January 1964 and by the Protocol of 16 November 1982. https://www.oecd-neo.org/jcms/pl_31788/paris-convention-full-text. Accessed 30 August 2021.

9.7.2 Why an Operator's Responsibility?

Thus, the State must first ask itself what is the responsibility of the operator in the field of nuclear security. Why should nuclear security be the responsibility of the operator rather than of the State? Several reasons can be given.

Logic dictates that nuclear security measures are most effective when they are located as close as possible to the materials and facilities to be protected. Thus, they must be taken into the operator's organization and be coordinated with other requirements, in particular those of nuclear safety. Only the operator can ensure this appropriate integration. This is particularly true in the case of security crisis management, where it may be necessary to deal with malicious actors and at the same time with the consequences of their actions for nuclear safety. The involvement of the operator is therefore essential.

In addition, nuclear security must be everyone's business. At the operator, each employee must understand the importance of nuclear security measures and participate in their implementation. This ensures that a malicious act or attempted of malicious act can be detected as soon as possible. This is the meaning of the Fundamental Principle F²⁶:

FUNDAMENTAL PRINCIPLE F: Security Culture

All organizations involved in implementing physical protection should give due priority to the security culture, to its development and maintenance necessary to ensure its effective implementation in the entire organization.

Insider threat constitutes an important vulnerability for nuclear security. Because of the proximity and hierarchical links with personnel, who could potentially be responsible for malicious acts or facilitate them, the operator has an essential role. The operator must be organized to prevent this threat as well as to detect it and to confront it.

Thus, even in a country such as France, where it has long been considered that security is the prerogative of the State, it is not possible to implement a good level of nuclear security without the involvement and a very strong contribution of the operators. However, the role of the State will always remain important and decisive.

9.7.3 What Are the Nuclear Security Obligations of the Operator?

In practice, nuclear security is therefore a matter of complementary responsibilities between the State and the operator. The national regulations must therefore specify what the responsibility of the operator is.

If the State chooses a performance-based approach, the operator sets up its protection system on the DBTs. If the State considers that operators must be able to deal,

²⁶A/CPPNM, above n. 1, Article 2a, para 3.

on their own, with all of the identified threats that the country has to face, the DBTs should include all of these threats. However, a State may consider it inappropriate to require operators to deal with all threats alone. In France, it is considered that the operator's armed forces cannot manage the crisis alone. They will give the State forces time to intervene. It is a configuration of a complementarity and coordinated response. In this case, the DBTs will be able to take up only part of the threats identified by the State. For example, in the French case, the national security directive for the civil nuclear sub-sector, in which the DBTs specific to the nuclear sector are described, clearly specifies which missions are under the responsibility of operators and which are under the responsibility of the State.

9.7.4 What Cooperation with Other Government Departments?

The role of the operator is limited by the prerogatives and means that can be given to a private person, for example:

- The possibility to collect information and to gather intelligence;
- The possibility to use weapons, in particular weapons of war;
- The possibility to intervene with weapons in public space or only on private property;
- The use of cameras, detectors, etc. outside private property (beyond the perimeter of the premises, sea and air, approaches to private property, etc.);
- The possibility to control people, to stop them, etc.;
- The possibility to regulate objects to be introduced onto private property and to search a person or a vehicle, etc.

All these issues are often already regulated in a country and will strongly influence the way roles in nuclear security can be shared between the State and the operator.

Because these means are highly regulated and controlled in countries committed to individual liberties, the State keeps a preponderant role in nuclear security, for example in terms of intelligence, counter terrorism (interruption of malicious acts before they are perpetrated), air and maritime security, armed response in the event of a terrorist attack, judicial investigations and criminal sanctions, etc.

9.8 Choice of Technological Options, Sites and Transport Routes

9.8.1 How Can Nuclear Security Be Integrated Into the Choice of Technology?

When a State considers implementing a nuclear programme, nuclear security must be one of its first concerns, in the same way that other issues such as nuclear safety are to be taken into consideration. The concept of ‘security by design’ mentioned earlier focuses on taking into account the DBT to better define the protection measures for the installation that need to be adapted to its operation.

This approach may lead to the choice of one technology over another, particularly after having evaluated the various existing technological choices regarding the national framework and the applicable DBT.

The difficulty that a State may have to face with concerns the sharing of sensitive information from the point of view of national defence (DBT) with a foreign entity. It is always good to remember Alexandre Dumas’s citation: “Today’s friends are tomorrow’s enemies” and vice versa.

It is therefore normal for a State to question what it is willing to share with a foreign entity, even though the decision to choose this technology may be the result of a relationship of trust with the manufacturer, or even with the State from which the manufacturer originates.

As mentioned above, the DBT is the result of a State’s decision to require that an operator is able to protect their facility from some of the threats that the State itself has to face.

In assessing a foreign technology, the State may choose to define a standard with an appropriate level of information that can be shared without compromising the integrity of its national security while ensuring its complementary responsibility in the protection of the facility.

9.8.2 What Are the Transport Issues?

‘Security by design’ can also be extended to the whole chain necessary for the operation of the nuclear activity and its security. Generally, a nuclear activity can hardly exist by itself. It depends on other related activities linked to its life cycle, such as the supply of fuel or materials required for its operation, the reprocessing of spent fuel, storage of the materials, etc.

These various activities may be carried out close to or far from each other (in particular to respond to land planning challenges, which are often of political concern, but which have non-negligible impacts in terms of security). This raises the issue of the transport of nuclear materials and other radioactive substances, which includes

inherent risks. Of course, this implies the need for special provisions for the physical protection of these transports, both at the national and international level when the State has to import or export such products.

As far as nuclear materials are concerned, the CPPNM, before being extended by its amendment to nuclear facilities, already set out obligations on transport. The implementation of these international requirements is specified by recommendations recognized by the international community, without legally binding value, contained in INFCIRC/225/Rev.5.²⁷ The purpose of these transports is to bring nuclear materials or other radioactive substances to the facility. Consequently, it is also important, from the design phase of a nuclear facility, to take into account this transport component (arrival/departure) and find the most suitable way to secure it.

9.8.3 How Can Security Be Integrated with Respect to the Site Chosen and Its Environment?

Land planning challenges have been indicated above and echo the important principle of ‘security by design’: the choice of the location of the facility at which the nuclear activity will be operated. This choice may often respond to interests other than those related to security: political, economic, social (particularly in terms of the acceptability of the project by the local populations), operational constraints, etc.

However, security shall not be neglected in the choices made. In the field of security, there is no single solution (a standardized security solution) that can be adapted without taking into account the local context. Protection strategies must be different in order to be best adapted to the facility and in particular to its environment. Operational modes and tactics of the adversary will depend on the location of the facility. This requires an appropriate protection system for the facility as well as from the State response, which need to be dimensioned accordingly.

Let us illustrate this with an example from outside the nuclear sector. It shows that these concepts are not so new. The example of the Palais Garnier (one of the two opera houses in Paris) is a concrete example that illustrates these two components of the ‘security by design’ principle. On 14 January 1858, Napoleon III was the victim of a bomb attack in front of the opera house which was located at that time on rue Le Peletier. After this attack, he decided to build a new opera house, more prestigious but also better secured. It is one of the most famous monuments of Paris we have today, the Palais Garnier. Security was therefore one of the major concerns to the building. Feedback from the attack led to the idea of a short, fast and secure route between the emperor’s place of residence and this new opera house. The result was the creation of the Avenue de l’Opéra, which was large enough and connected the two places in a straight line to make it very difficult to plan an attack during the journey.

²⁷IAEA 2011a.

This perfectly echoes the need to have an integrated assessment of the industrial context around the nuclear facility and the need for transport to be considered at the very beginning, from the phase of reflection on the location of the activity. Another interesting element of the original design of the Palais Garnier is the ‘Emperor’s Rotunda’. This construction offers secure access reserved for the emperor, since it provides effective protection against any remote attack.

This highlights the importance of this transitional phase, which can sometimes present significant vulnerabilities if not anticipated, when a transport of nuclear materials or radioactive substances arrives at the facility.

9.9 Confidentiality, Transparency and Communication

Confidentiality is one of the twelve fundamental principles of nuclear security included in the 2005 Amendment²⁸:

FUNDAMENTAL PRINCIPLE L: Confidentiality

The State should establish requirements for protecting the confidentiality of information, the unauthorized disclosure of which could compromise the physical protection of nuclear material and nuclear facilities.

Therefore, States apply, as referred to several times in this chapter, this principle both at the national and international levels, particularly in the development and drafting of international instruments. It also interacts with other elements specific to the nuclear sector, such as the principle of transparency, or of the management of a radiological crisis and the associated communication needed.

9.9.1 *What Are the Communication Challenges in the Face of Terrorism?*

In the field of security, the threat is generally characterized by a motivation (an ideology, a personal cause, etc.), a capability (accessible material and human resources, knowledge of the relevant field, etc.), and a target, which is attractive to the adversary. This last aspect covers the symbolic dimension that the target represents. At present, the main threat against which States are protecting themselves is terrorism. Without wishing to give a universal definition to this concept that is difficult to characterize, it is interesting to quote Raymond Aron who defines terrorism in the following way: “A violent action is called terrorist when its psychological effects are out of proportion with its purely physical results.”²⁹ Another way of characterizing terrorism, which reflects the symbolism that a potential target may have, is the

²⁸ A/CPPNM, above n. 1, Article 2a, para 3.

²⁹ Aron 1962, p. 276.

following proverb: “It is better to kill one and be seen by a thousand than to kill a thousand and be seen by one.” When one thinks of a nuclear activity, especially in certain highly nuclearized countries, the symbolic aspect is obvious. Thus, in the event of a terrorist act, the issue of communication and acceptance of nuclear energy will necessarily be essential, and each State must be well prepared.

9.9.2 Why Protect the Information?

More pragmatically, the attractiveness of a target is characterized by the fact that it can be reached with the means available to the adversary. Among the various measures that can be taken to make a target more difficult to reach is the principle of deterrence. There are several ways to achieve this objective: to provide for sanctions in the national legislative framework, to bring to light the high security of the facility (e.g. imposing barriers, numerous cameras), to set up random patrols of guards and of intervention forces inside and outside the restricted zone of a nuclear facility, etc. However, deterrence does not require total transparency, which would obviously make it easier for an adversary to plan a malicious act. It is therefore necessary to evaluate carefully the information that is essential to protect.

9.9.3 How to Balance the Protection of Information and the Principle of Transparency in the Nuclear Sector?

In the nuclear sector, transparency is often set up as a fundamental value. In France, the main law in the nuclear field is called the law on transparency and security in the nuclear field.³⁰ It defines transparency as “all the measures taken to guarantee the public’s right to access a reliable information on nuclear security”. This principle therefore interacts with the confidentiality objectives relating to nuclear security mentioned above. It is necessary to find the right balance between what can be communicated and what must remain known only to those who need to know. This highlights the importance of the interfaces between nuclear safety and nuclear security when it comes to communication, especially from a technical perspective. For example, when a significant safety or radiation protection event occurs in France, there is an associated communication. This communication is graded according to the importance of the event and its scope. The communication may consequently remain local or be national or even international. In order to respect the objectives of the law indicated above, technical details of the origin and consequences of the event may be included in the communications. The information can potentially create

³⁰In this law, nuclear security includes nuclear safety, radiation protection, and prevention against malicious acts as well as civil security actions in case of accident.

vulnerabilities for the facility concerned, and can be misused by certain persons. The High Committee for Transparency and Information on Nuclear Security (HCTISN) is, in France, a body in charge of public information and the organization of consultations and debates on the risks associated with nuclear activities. Numerous debates within this institution have led to guidance to better define the information that needs to be protected for the purpose of nuclear security.

9.9.4 How to Protect Information During the Management of a Crisis?

Transparency provisions also apply when managing a security crisis. Communication must be balanced, knowing that there will be media pressure to cover the event and give information to the public.

In the case where the origin of the crisis is security, certain communications or behaviours can interfere with the proper conduct of the actions of State security forces. France was affected by major attacks in 2015. Some media behaviours may have disturbed security operations during the crisis. The information mission of the media may have led them to communicate information that was used by the terrorists. For example, one of the terrorists regularly used a computer to watch different news channels to be informed of the external situation (in particular, the organization of the State security forces present on site). Again, in this context, we highlight the importance of managing the interfaces with all the actors, considering the differences in their objectives.

In France, any major crisis is managed at the national level within a single framework, regardless of its origin: nuclear (technological, natural, malicious, etc.), terrorist or of any other nature. A single authority manages it. A nuclear crisis with a malicious origin will be managed primarily by the authorities that usually deal with counterterrorism (services of the Prime Minister and the Ministry of the Interior). The authorities in charge of nuclear safety and nuclear security³¹ will provide advice and situation updates in their field of competence, but will not have any decisional role. It should be noted that the decision making authorities are generally not directly involved in the work carried out by the IAEA. The interface is therefore ensured at the national level by the experts of the nuclear security authority on the matters related to their field of competence. These experts will preferably use their international communication channels developed in accordance with their needs and objectives. This underlines the importance of the IAEA's role in coordinating the development of tools that meet the specific challenges of the nuclear sector.

³¹In France, the security authority is in charge of the regulations and of the control of their implementation. It is therefore the privileged interlocutor in multilateral bodies such as the IAEA.

9.10 Conclusion

The purpose of this chapter is not to outline in a few pages the entire process required to create a nuclear security regime, but rather to provide an overview of some of the major questions that a State must consider when planning to engage a nuclear programme and consequently to develop a nuclear security regime.

It is essential for the State to understand that nuclear security is part of a context of intense national cooperation, especially in areas where there are strong interfaces, such as intelligence, screening, cooperation with State security forces, and computer security. It is therefore crucial to set up a national governance. The competent authority for nuclear security, whose position is adapted to the national security environment, should participate, as necessary, in this coordination in order to contribute to the coherence of the national and international framework for nuclear security. This authority is also in interaction with the other components of the nuclear sector and with civil society. As a rule, transparency is a fundamental value that conflicts with the need for confidentiality or protection of information. In order to avoid possible isolation of the competent authority from all its partners, it is necessary to find the best balance between protection and sharing.

The threat that an operator faces is another particularity of nuclear security, since the malicious act is a human act able to adapt, whereas the operator must take into account natural or unintentional aggressions in the field of risk prevention. In the design and authorization processes, it is essential for the operator and the competent authority to conduct their analysis from the point of view of the malicious person. This paradigm change is not intuitive, as the logic in the risk evaluation is usually done from the point of view of the 'defender'. Some measures promoted to secure a nuclear activity are initially designed to ensure nuclear safety functions. It is therefore essential to ensure that these measures are effective and robust against one or more individuals with malicious intent. This also allows us to identify certain operational modes or malicious scenarios that are difficult to predict otherwise.

It is always useful to remember that, despite the sovereign responsibility of States, nuclear security is part of global security issues. Terrorist threats are often international and require effective international cooperation to combat them. The consequences of malicious acts on nuclear activities are such that each State is concerned about the way other States approach nuclear security issues.

Nuclear security, as a field related to national security, has very specific aspects, particularly in terms of sovereignty and protection of information, which make it different from other components of the nuclear sector. It is linked to a larger set of international law that responds to specific concerns, through its own logic and objectives. This situation also exists for nuclear safety and safeguards. An overly nuclear approach could have the effect of distancing thematic experts in favour of cross-cutting profiles; this would not ensure coherence with related environments beyond the concerns of the nuclear sector, for example security in the broad sense at both the national and international levels. Using this logic, the IAEA plays an

essential coordinating role to enable the establishment of the bridges that are indispensable for the identification and relevant treatment of the interfaces between the three components of the nuclear sector, while guaranteeing the maintenance of their singularity for the proper integration of the considerations mentioned above.

International cooperation is essential for sharing good practices among nuclear security specialists and for establishing recommendations that are recognized by the international community.

In this respect, the IAEA occupies a central place, whether through its Nuclear Security Series, the numerous training courses, workshops and conferences it organizes, or the various services it offers to States.

However, one shall bear in mind that in many areas it may also be appropriate to use regional or bilateral relationships. As an example, there is an association of nuclear security authorities of several European countries called the European Nuclear Security Regulators Association (ENSRA). It offers the opportunity to discuss specific issues and exchange information more freely than in the more open framework of the IAEA. In addition, States usually establish bilateral cooperation agreements with other States, which contain confidentiality rules.

9.11 To Go Further...

Although the CPPNM can be seen primarily as a political instrument (the States Parties say that they respect the obligations of the Convention without detailing the modalities of their implementation), this does not mean that the States Parties will not act in good faith in implementing their commitments. Some States Parties take a different view and consider that the objective of the Convention is to ensure, in a very concrete way, that other States provide effective protection of their facilities and provide guarantees to them. It could be expected from these States that a verification mechanism be established. However, this vision runs up against the above-mentioned principles.

The possibility for States Parties to convene a conference under Article 16 of the CPPNM and its Amendment is a method of assessment that is again based on the principle of good faith. It is generally accepted that States must rely on the accuracy and completeness of the information provided by each party for this type of exercise. Civil nuclear energy is a sensitive subject at both the national and international levels, since civil society has a real concern as regards this technology. This raises the following question: to what extent is a State ready to share on the international scene, in a very transparent manner, any weaknesses in its facilities or organization? Even if this information is not accessible to the public, keeping a good reputation is an important consideration for States.

Because of these constraints, it seems difficult that the conference is the most appropriate tool to guarantee to all States, in a concrete and valuable way, the respect of the obligations of the Convention from a technical point of view.

As mentioned above, the IAEA has an IPPAS programme to evaluate a State's physical protection regime based on the obligations of the CPPNM, its 2005 Amendment and INFCIRC/225/Rev.5. This assessment includes a detailed examination, at the national level, of the legal and regulatory framework, as well as the measures and procedures implemented by the State in accordance with the provisions of the international framework. This programme, proposed by the IAEA, offers a secure peer review framework, perfectly adapted to nuclear security. It allows the country concerned to receive a detailed report, following a detailed analysis by a team of recognized international experts. Although the most sensitive information cannot be shared with the experts, this tool is well adapted to the objective of guarantee that some States Parties may wish to assign to the Convention. It is therefore appropriate to encourage all States Parties to host an initial IPPAS mission and to plan to request further periodic missions.

References

- Aron R (1962) *Paix et guerre entre les nations*. Calmann-Lévy, Paris
- Breivik A (2011) 2083—A European Declaration of Independence. <https://info.publicintelligence.net/AndersBehringBreivikManifesto.pdf>. Accessed 20 August 2021
- Cartwright J, Fauvarque-Cosson B, Whittaker S (2016) The Law of Contract, The General Regime of Obligations, and Proof of Obligations. The New Provisions of the Code Civil Created by Ordonnance n° 2016-131 of 10 February 2016 Translated into English. http://www.textes.justice.gouv.fr/art_pix/THE-LAW-OF-CONTRACT-2-5-16.pdf, <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000032004939/>. Accessed 20 August 2021
- Code de la Défense (2021) <https://www.legifrance.gouv.fr/codes/id/LEGITEXT000006071307/>. Accessed 20 August 2021
- International Atomic Energy Agency (IAEA) (2004) Code of Conduct on the Safety and Security of Radioactive Sources, IAEA/CODEOC/200. IAEA, Vienna
- International Atomic Energy Agency (IAEA) (2011a) Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5), IAEA Nuclear Security Series No. 13. IAEA, Vienna
- International Atomic Energy Agency (IAEA) (2011b) Nuclear Security Recommendations on Radioactive Material and Associated Facilities, IAEA Nuclear Security Series No. 14. IAEA, Vienna
- International Atomic Energy Agency (IAEA) (2013) Objective and Essential Elements of a State's Nuclear Security Regime: Nuclear Security Fundamentals, IAEA Nuclear Security Series No. 20. IAEA, Vienna
- Stoiber C, Baer A, Pelzer N, Tonhauser W (2003) *Handbook on Nuclear Law*. IAEA, Vienna
- United Nations General Assembly (UNGA) (1946) Establishment of a Commission to Deal with the Problems Raised by the Discovery of Atomic Energy, Resolution 1(I). [https://undocs.org/en/A/RES/1\(I\)](https://undocs.org/en/A/RES/1(I)). Accessed 20 August 2021
- United Nations General Assembly (UNGA) (1997) Resolution 51/210, A/RES/51/210. <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N97/761/65/PDF/N9776165.pdf>. Accessed 20 August 2021
- United Nations Security Council (UNSC) (2004) Resolution 1540, S/RES/1540. [https://www.un.org/ga/search/view_doc.asp?symbol=S/RES/1540%20\(2004\)](https://www.un.org/ga/search/view_doc.asp?symbol=S/RES/1540%20(2004)). Accessed 20 August 2021

The opinions expressed in this publication are those of the authors/editors and do not necessarily reflect the views of the IAEA: International Atomic Energy Agency, its Board of Directors, or the countries they represent.

Open Access This book is licensed under the terms of the Creative Commons Attribution 3.0 IGO license (<http://creativecommons.org/licenses/by/3.0/igo/>), which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the IAEA: International Atomic Energy Agency, provide a link to the Creative Commons license and indicate if changes were made.

Any dispute related to the use of the works of the IAEA: International Atomic Energy Agency that cannot be settled amicably shall be submitted to arbitration pursuant to the UNCITRAL rules. The use of the IAEA: International Atomic Energy Agency's name for any purpose other than for attribution, and the use of the IAEA: International Atomic Energy Agency's logo, shall be subject to a separate written license agreement between the IAEA: International Atomic Energy Agency and the user and is not authorized as part of this CC-IGO license. Note that the link provided above includes additional terms and conditions of the license.

The images or other third party material in this book are included in the book's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the book's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.