PROTECTION OF INFORMATION: AN ESSENTIAL COMPONENT OF PHYSICAL PROTECTION OF NUCLEAR MATERIAL TRANSPORTATION

André Stasse
World Nuclear Transport Institute, Remo House, 310-312 Regent Street, London, W1B 3AX, United Kingdom

Matt Fox
World Nuclear Transport Institute, Remo House, 310-312 Regent Street, London, W1B 3AX, United Kingdom

PREAMBLE

We must be transparent in our core activity which is an industrial field directly linked to electricity production. This activity is strategic for all countries involved in nuclear electricity programs. Thus, the transportation of nuclear material from one country to the next is not only a typical element of the industry but a strategic element as well.

One of our main preoccupations in the transportation of nuclear material is to ensure the highest level of physical protection because nuclear material is, in one hand, firsly, a material which presents a risk of proliferation, and in the other hand this material is a dangerous good. To assure this protection, it is necessary to restrict information in order to reduce risks. In so doing, the industry is sometimes accused of being too opaque.

It is the same regulation to protect nuclear material into nuclear sites than during the transportation phase. Two types of regulations are applicable within the perimeter of nuclear sites - those being safety and physical protection. During the transportation phase, three types of regulations must be enforced: safety, physical protection and, in addition, international regulations for the transport of dangerous goods which mix safety and security requirements according to the vulnerability in public domain and gives international rules to apply. These rules include protection of the information in nuclear material transport organisation.

OBJECTIVES OF THE INFORMATION PROTECTION

1. Apply national and international regulations while adapting security to the context of different countries and to the situation.
2. Develop trust in the general public in our capacity to deal with potential incidents or accidents by proving that we are ready to manage emergencies. Affirm the positive image of nuclear activities by being professional.
3. Prevent all malevolent acts with consequences on public health by exerting an extremely high level of security.
4. Be ready to communicate on transport with necessary and sufficient information.
5. Prevent anti-nuclear non-governmental organisations (NGOs) from using rapidly rising nuclear electricity costs as a tool for propaganda by controlling the costs of nuclear material transport.

WHY PROTECT INFORMATION ABOUT NUCLEAR MATERIAL TRANSPORT

The level of security as well as the level of restricted information is proportional to the nature and quantity of nuclear material. Sometimes vulnerability of nuclear shipment could linked to the focus of medias and anti-nuclear campaigns. Information protection is thus an essential components of the physical protection of nuclear material transport. Why? Essentially

because States and Operators must prevent threats according to the well costs : paragraph 1 and 2. In support, to illustrate following two examples in paragraph 3 and 4. How ?

1. THREATS

1.1. Non Proliferation

The international standard for physical protection of nuclear material, INFCIRC 225 Rev. 4 strongly recommends the restriction of information when organising the transport of nuclear material which could be used as a proliferation target.

Obviously, the highest level of information protection must be organized to ensure the physical protection of transportation of nuclear material for highly enriched uranium, plutonium and MOX. Communication actions must be carefully prepared for these shipments. In most cases, a good practice consists of coordinating official positions of governments in order to avoid unauthorised disclosures.

Implementing intergovernmental agreements or memorandums of understanding is also a good practice to exchange, between operators, restricted, sensitive and classified information in the framework of an international shipment of nuclear material.

1.2 Possibility of attacks from terrorist movements for political purposes and from other malevolent organizations, for business profit and gains.

1.3 Individuals actions who might steal nuclear material for business or other motivations (resentment, revenge, ransom, etc.).

1.4 Irresponsibility of anti-nuclear NGOs who want to stop the nuclear industry by blocking transport providing creative scenarios to real malevolent or terrorist organisations. Furthermore, NGOs could be manipulated by real criminal organizations.

2. COSTS

Protection of information needs to be taken into account for the physical protection of shipments of nuclear material. Costs resulting from the mobilization of government forces against anti-nuclear NGOs and other threats are very expensive.

3. EUROFAB EXAMPLE

EUROFAB was a program in 2004 converting US military-grade plutonium (Pu) into MOX fuel in France.

During phase I of the transport (the arrival of the military plutonium), public communication led to the mobilization of many NGOs requiring the organization of a vast police and gendarmerie operation in France. While US Government disclosed information about transport through the web channel, it was difficult to protect the information and the NGOs benefited from television and radio coverage and several press conferences. A great number of French police forces were mobilized for the preparation and reception of the containers arriving from the USA! In Cherbourg alone, around 1,500 police and gendarmerie personnel were present to escort the cargo, protecting it from numerous NGOs.

The entire security operation was huge and seemed oversized.

During phase II (the return of MOX fuel to the USA), the gendarmerie located in the *South East* plants engaged as decoys in discussions with NGOs, waiting for the transport. AREVA was able to discretely organize the return shipment using, instead, direction to La Hague. Police and gendarmerie forces could then be better used in their usual security function.
The phase II costs of the security operation were adapted and proportionate to the threats. This example demonstrates the necessity to protect information in order to reduce the threat.

4. EXAMPLE OF IRRESPONSIBILITY OF ANTI-NUCLEAR NGOs

During the investigation following his attacks in Morocco at Casablanca, in 2003, a French terrorist revealed that his subsequent objective was to attack vehicles which transport plutonium in France.

Only a few moments after the events in Casablanca, an NGO published on the website "STOP PLUTONIUM" a map, with the installations, itineraries and transportation schedules (i.e. confidential information) linked to plutonium and MOX shipments.

The French Authorities tried reason with this NGO, but too much information had already been disclosed which could be used by criminal organizations.

5. DEFENSIVE DEFENCE APPROACH

Different defence approaches can be adopted, either in depth or gradually, including information protection measures which are, indeed, essential. One aspect of defensive positioning consists of restricting information to a need-to know basis.

The context according to the country is totally different. For example, in Germany, it is necessary to provide a high level of security to protect shipments of nuclear material against the numerous anti-nuclear movements. In this case it is very difficult to protect information.

We have noticed that when a nuclear material shipment is communicated by the Authorities or by other nuclear operators, the level of mobilization by anti-nuclear opposition groups is stronger. Well balance communication is not easy but essential.

Gradual physical protection measures must be implemented to ensure the security of nuclear material shipments. They may depend on the transport mode (rail, air, sea and/or road) and must be designed around realistic scenarios with objectives to detect and delay aggressors and to raise the alarm. This could differ from one State to another one. The physical protection measures must be combined with active and multiple combinations of escort provisions. The details of these measures need to be protected as sensitive or classified information.

CONCLUSION

Communication concerning the transport of nuclear material must be coordinated between Competent Authorities and operators and must be adapted to the context (potential public events) and to the operational logistics plans. As a result, the use of the governmental security forces which protect shipments of nuclear material will be optimized. All protective measures

must be adapted according to the recommendations of the International Atomic Energy Agency (IAEA). Then, the protection of information is really an added value to the physical protection of nuclear material transportation.

Transparency is a necessity, but protection of information to ensure the security of transportation is also essential. The challenge is to deal with the two imperatives by getting the right balance.

REFERENCES

1. **INFCIRC 225 The physical protection of nuclear material and nuclear facilities**

> **4.3 CONFIDENTIALITY**
>
> "The State should take steps to ensure appropriate protection of specific or detailed information the unauthorized disclosure of which could compromise the physical protection of nuclear materials and nuclear facilities. It should define requirements for the confidentiality of physical protection systems and associated documentation."
>
> 4.3.2 "Management of physical protection systems should limit access to sensitive information to those who need to know for the performance of their duties. Information addressing possible vulnerabilities in physical protection systems should be highly protected as it could indicate means of successfully removing nuclear material or of carrying out sabotage."
>
> 4.3.3 "Sanctions against persons violating confidentiality should be part of the State's legislative or regulatory system."

2. **IAEA Nuclear Security Series N°9 (NSS9), Implementing Guide for Security in the Transport of Radioactive Material**

> **4.2 Basic Security level**
> ***Exchange of security related information***
> "Operators should cooperate with each other and with the appropriate authorities to exchange information on applying security measures and responding to security incidents where the exchange of information does not conflict with requirements for security in respect of sensitive information."
>
> **4.3 "Enhanced Security Level**
> **The security plan should include …** Measures to ensure that the distribution of sensitive transport information is limited, to maintain security of the information."
>
> **4.4 "Additional Security Measures**
> **Additional measures** consistent with national requirements may be taken to protect the confidentiality of information relating to transport operations including detailed information on schedules and routes."

3. **Security of dangerous goods international guide (Chapter 1.10 of ADR and RID)**

Establishment of a security plan including restricted information relating to movements of dangerous goods and limiting this information to the directly concerned staff.
The totality of measures of the security plan constitutes a single and stand-alone document which could be entitled “SECURITY PLAN” or “SECURITY HANDBOOK.”

This document is CONFIDENTIAL for the COMPANY and should be known only by a limited number of people. In addition, if the plan is stored in the IT system, it needs particular and adapted security measures.

The SECURITY PLAN must not be disclosed to third parties except other operators or Authorities for verifying contract and legal requirements.