This item is the archived peer-reviewed author-version of:

The security of transport of radioactive and nuclear material in Belgium

Reference:
Goetstouwers Maarten, Sauer Tom.- The security of transport of radioactive and nuclear material in Belgium
Full text (Publisher's DOI): https://doi.org/10.1080/13669877.2021.1905692
To cite this reference: https://hdl.handle.net/10067/177700151162165141
The Security of Transport of Radioactive and Nuclear Material in Belgium

Maarten Goetstouwers, MSc, BSc & Prof. Dr. Tom Sauer
University of Antwerp

Abstract

This article describes and assesses the security of transport of radioactive and nuclear material in Belgium that has been boosted after the terrorist attacks in Brussels in 2016. The article looks at the different possibilities of terrorist attacks on transports of radioactive and nuclear material and the possible consequences: theft of radioactive material for use in a radioactive exposure device, a radioactive dispersal device, or an improvised nuclear weapon; or a conventional attack on a transport, releasing radiation into the environment. The focus on insider threat is a step forward, but it may not divert attention from regularly updating security measures against outsider threat. Some recommendations are provided to ensure continuous improvement in the transport of radioactive and nuclear material.

Maarten Goetstouwers, Master of Science in International Relations and Diplomacy, is a researcher associated with the University of Antwerp

Prof. Dr. Tom Sauer is Associate Professor International Relations at University of Antwerp and specializes in International Security and Non-Proliferation.

1 Introduction

Terrorists have (tried to) use(d) chemical, biological, and radioactive and nuclear (CBRN) weapons. In 2017, two brothers were arrested in Sydney for plotting to release a lethal poison gas in an airplane (Mitchell, 2019). The 1995 Tokyo Metro attack is seen as the onset of catastrophic terrorism. The high number of casualties, injuries, and the use of sarin gas are the main difference with 'conventional' terrorist actions (Nacos, 2016). An ISIS-fighter admitted to have used chemical weapons near Raqqa (Ali, 2019). The threat of CBRN terrorism will probably continue to rise (U.S. Department of State, 2018; Carpintero-Santamaria, 2018).

This article focuses on the risks associated to transports of radioactive and nuclear material in Belgium. We distinguish two types of terrorist attacks on transports: (1) a conventional attack or (2) theft. The first would spread radioactive or nuclear material over a wide area, contaminating it. Depending on the substance, on the physical and chemical forms, on the activity and quantity, the consequences could range from limited to catastrophic. The second, stolen substances, can be used (1) to receive funding through smuggling and sale (FANC, 2018c); (2) as a resource for a radiological exposure device (RED); (3) as a resource for a radiological dispersal device (RDD), or dirty bomb; or (4) as a resource for an improvised nuclear device (IND) (Sauer & Volders, 2016). This paper focuses on the threat and possible consequences of a conventional attack or theft of radioactive or nuclear substances during transport.

This article sets out to analyze the terrorist threat against transports of radioactive material in Belgium. It will assess the current security situation, analyze the terrorist threat, and try to develop recommendations to protect against future threat.
2 SECURITY OF TRANSPORTS OF RADIOACTIVE AND NUCLEAR MATERIAL

First, we describe the main transport movements in Belgium and how they are organized. Then, we discuss current security measures.

2.1 TRANSPORTS OF RADIOACTIVE AND NUCLEAR MATERIAL IN BELGIUM

Most transports are by road, while long distance transports of short-living radiopharmaceutical materials are transported by air. Other packages can be transported by road, water or air depending on the whereabouts of the facilities, but for large, heavy fissile packages, railroad transportation is mostly used (FANC, 2017c).

Nuclear fuel rods are used in Belgium as fuel for nuclear power plants and as material for the production of medical radioisotopes. About 60 percent of all transports of nuclear materials in Belgium are transits from one border to another. They do not have their origin...
and destination in Belgium. Radioactive materials are used in research centers, industrial, agricultural, medical and home applications, e.g. smoke detectors (americium-241)\(^1\) (FANC, 2017b, 2017c). Some transports are conducted by rail (Decelle, 2018; FANC, 2018c; Greenpeace, 2018). For security, the transportation of packages containing radioactive or nuclear material is considered as ‘one of the higher risk activities in the lifetime of these materials’ by the International Atomic Energy Agency (IAEA, 2018, July 9\(^{th}\) §1).

In Belgium, there are an estimated 35,000-40,000 transports per year of radioactive material for medical and scientific purposes, and 3,000 carry radioactive material for industrial applications, agriculture and research. The estimated 2,000 fissile transports are mainly for (1) fuel for the Belgian nuclear power plants of Doel and Tihange (about 10 transports), (2) fissile materials from industrial activities in the facilities of SCK•CEN and Belgoprocess (less than 1,000), and (3) more than 1,000 for transit from Borssele (Netherlands) to La Hague (France) and transport in and through the port of Antwerp (FANC, 2017c). The numbers in 2019 are of a similar size (FANC, email).

The BR2 nuclear reactor of the Belgian research facility SCK•CEN is fueled with high enriched uranium. The reactor produces 25% of all medical isotopes molybdenum-99 in the world, at peak moments up to 65% (SCK•CEN, 2013). It plays a vital role in the production of neutron transmutation doped silicon, a semi-conductor for high energy applications such as wind turbines, solar power installations, cars and trains (SCK•CEN, 2018b). Figure 1 shows the main directions of transport of transports group 2, 3 and 4 (cf. infra). The red arrows show UF\(_6\) transport directions, the blue arrows U-targets and the grey arrows fissile ores, uranium dioxide (UO\(_2\)), fuel elements, and waste and radiated fissile material (FANC, 2017a). Even after nuclear fade-out, radiological transports will remain.

Nuclear power plants will be decommissioned from 2025 onwards in Belgium (Law of 31 January 2003). Nuclear waste and spent fuel remain at site for at least 50 to 80 years before it can be stored underground. The reactors and other contaminated parts of plants will be dismantled, processed and stored (European Commission, 2018; Greenpeace, 2018). It is currently unclear whether radioactive waste and spent fuel will be processed at site or at the facilities of Belgoprocess (Greenpeace, 2018). This decision will have a profound impact on the number of transports. Greenpeace (2018) states that the dismantlement of nuclear power plants is still in its infancy. This is contradicted by SCK•CEN, which gained experience from dismantling the BR3 research reactor, the dismantlement and decontamination of the MOX-installation in Dessel and the research reactor Thetis of the University of Ghent (SCK•CEN, 2018a, 2018c).

2.2 Current Security Measures for Transports of Radioactive and Nuclear Materials in Belgium

Nuclear security covers ‘all technical and organizational measures taken to prevent and

---

\(^1\) Radioactive smoke detectors are prohibited in Belgium since January 1th, 2020 (FANC, 2019).
detect theft, sabotage, access by unauthorized persons, misappropriation and any malicious act. ... The aim is therefore to protect the population, workers and the environment against any radiological risk resulting from ... sabotage or a terrorist attack ... The protection of sensitive information ... also belongs to the domain of nuclear security’ (FANC, 2018a; our translation). Member states of IAEA have to meet these regulations and safety guarantees. IAEA offers tools to Member States to strengthen their nuclear security, e.g. transport security regulations, training, guidelines for international transport, and a transport security interface. IAEA follows up on current, evolving and future threats (IAEA, 2018d). ‘While both nuclear safety and nuclear security consider the risk of inadvertent human error, nuclear security places additional emphasis on deliberate acts that are intended to cause harm. Because security deals with deliberate acts, security culture requires different attitudes and behavior, such as confidentiality of information and efforts to deter malicious acts’ (IAEA, 2008a, p. 5).

The IAEA (2018 §2) describes nuclear transport security as ‘to guard nuclear and other radioactive material with locks, seals and other technologies and methods to ensure it does not fall into the wrong hands’. The IAEA assists ‘states with the development of a physical protection regime of the transport of nuclear and other radioactive material to help protect people, property and environment from malicious acts. This could include, for example, radioactive packages being intercepted and sabotaged during transport’ (IAEA, 2018 § 4). Once the packages arrive at their destination, they have to be placed in the correct part of the facility where they are safe and secure. Nuclear transport security limits its scope to the movement of the package between two facilities. Nuclear facilities have their own security systems in place. The security system of the transport and the facilities overlap each other at the moment of departure and arrival. This overlap is, however, not specified in Belgian legislation (FANC, 2018c). The Belgian legislation on the physical protection of nuclear material dates from 2011 and made security a top priority for FANC. The Radioactive Material Security Project, or RAMAS-project, aims to provide new legislation on the protection, prevention, detection and response to malicious acts in relation to radioactive materials (Dresselaers & Fanielle, 2016; FANC, 2018c).

A radioactive transport consists of the movement of radioactive or nuclear materials from point A to point B, including the preparation of the packages prepared for transport. A transport involves a consignor, carrier and consignee. Consignor (= sender) and consignee (= receiver) are considered safe and well-secured facilities. The term carrier refers to every company involved in the transportation of packages by rail, road, air, sea and inland waterways. According to the regulations of IAEA, the consignor is responsible that all regulations and guarantees of safety and security are met during the entire transport, including preparation, transport, and delivery to the consignee (FANC, 2018c). A transport can involve multiple modes of transport and companies, including handlers who shift packages from one mode to another. Their operations are regulated by international agreements, international regulations governing the transport of dangerous goods, and by Belgian national law. In Belgium, all stakeholders are inspected by FANC. There are some 120 carriers who are in possession of the required safety licenses (estimates given by FANC, 2018c). These licenses are granted if the safety requirements for transport of radioactive material comply, and if the security measures of the international agreements and regulations governing the transport of dangerous goods are respected. Additional
security licenses have to be obtained for nuclear material (FANC, 2018c). For nuclear transports, other actors are sometimes involved, e.g. police, and the Crisis center of the Ministry of Interior. FANC carries out inspections and can also demand a detailed report on the organization of the transport. Depending on the level of threat, the Crisis Center, police and FANC can request specific security measures. One of the measures can be to annul the transport.

Since January 1st, 2018 there is a graded approach system which pays more attention to sensitive transports than to routine transports with less dangerous products (FANC, 2018c). It recognizes 4 UN groups of transport of radioactive or nuclear material:

- **UN group 1** covers the class 7 dangerous goods in excepted packages (cf. infra), which carry little to no risk from the safety point of view;
- **UN group 2** covers the non-fissile or fissile excepted class 7 dangerous goods with the exception of those covered by the UN group 4, which carry a radiological risk from the safety point of view;
- **UN group 3** covers the fissile class 7 dangerous goods, with the exception of those covered by the UN group 4, which carry a radiological and ‘fissile’ risks from the safety point of view; and
- **UN group 4** covers uranium hexafluoride (UF₆), with the exception of those covered by the UN group 1, which carry a radiological, sometimes ‘fissile’, and corrosive risks from the safety point of view.

To obtain agreement and licenses for transports of radioactive and nuclear material, transport companies have to file an application at FANC. In addition to the review and assessment of the application, a system-inspection (compliance audit) is carried out. Inspectors of FANC verify whether the management system complies with international regulations for the safety and security of the transport of dangerous goods. For high consequence dangerous goods (class 7), nuclear material or UF₆, additional documents have to be submitted to the security department of FANC. The agreements and licenses are only obtained when the departments of Transport and Security of the FANC give permission. The security application requires a Transport Security Plan (TSP), respectively for UN group 2 transports, and for UN group 3 or 4 transports. The TSP is examined by FANC and if necessary amended. A license is valid for maximum five years. High risk transports have to be reported in advance and depending on the transported substance, specific permits must be submitted. This regulation, however, is only applicable since January 2018 (FANC, 2018c).

FANC organizes follow-up inspections. Punctual inspections are carried out three or four times per year for high-risk transport companies. During transport, inspectors check compliance with the regulations on site. System inspections are comparable to a compliance audit. Transport companies are subject to system inspections before issuing the initial license, and afterwards every three years for group 3 and 4, and every five years for group 2 (FANC, 2018c). The regulations concerning transport of dangerous and radioactive products are bundled in the Orange Book, and then split by transport mode in a specific set of rules that consignor, transporter and consignee have to comply with: the European
Agreement concerning the International Carriage of Dangerous Goods by Road (ADR), the Règlement concernant le Transport International Ferroviaire des Marchandises Dangereuses [Regulation concerning the International Transport by Rail of Dangerous Goods] (RID), the International Maritime Dangerous Goods Code (IMDG), the Technical Instructions for the Safe Transport of Dangerous Goods by Air (ICAO), and the European Agreement concerning the International Carriage of Dangerous Goods by Inland Waterways (ADN) (FANC, 2018b). Companies have to use the template supplied by FANC per transport mode to comply with the demands regarding safety, security and trustworthiness. Companies that already perform other transports of UN groups 1 and 2 are not required to comply with legislation on the physical protection of fissile material and clearances due to the graded approach (FANC, 2018c).

According to FANC (2018c), the safety and security of all transports of radioactive and nuclear material in Belgium is based on the principle of Defense in Depth and consists of (1) technical performance of the packages, (2) limitations during transport, which refer to the maximum weight of the transport, speed, possible itineraries (3) trustworthiness of the transport, and (4) prevention and management of incidents and accidents.

Nuclear safety (that is related to accidents, in contrast to the concept of nuclear security that is related to terrorism) increases the level of protection of the packages, and simultaneously advances certain security measures, so-called ‘collateral advantages’. Security is further enhanced by the trustworthiness of personnel involved, an engaged security management, and in some cases armed escorts.

2.2.1 Collateral advantages of nuclear safety for nuclear security

Packages used to transport radioactive materials are designed to protect individuals–and the environment under all circumstances, irrespective of the mode of transport (FANC, 2018c). Safety protection is obtained by (1) containment of the radioactive content, (2) control of the intensity of external radiation, (3) prevention of criticality\(^2\), and (4) prevention of damage caused by heat (FANC, 2018a).

Transports containing UN group 4 materials are considered international events, even if they do not cross national borders (FANC, 2018d). The rules of international agreements, regulations governing the transport of dangerous goods, and the Basic Safety Standards (European Directive 2013/59/Euratom) have been transposed by the Belgian authorities in 2017 and entered into force by Royal Decree on January 1\(^{st}\), 2018 (FANC, 2018d). As every UN group 4 transport is considered an international event, an international standard is needed to classify the risk level of the transported material.

---

1. Criticality refers to the environment in which enough neutrons are present to sustain a nuclear chain reaction.
The IAEA developed a system to calculate a threshold for every radioactive material. These thresholds refer to the activity that, in case of an incident, would expose the population or emergency services to an actual dose of 50 mSv in 30 minutes, measured 1 meter from the package. The model focuses on external exposure resulting from (1) photons, (2) beta radiation, and internal exposure resulting from (3) inhalation, (4) immersion and (5) ingestion (FANC, 2015). The threshold determines the type of package that has to be used. The safety level ranges from very low to significant radioactivity. The lowest protection grade, the excepted packages, has to be ‘shock and vibrations resistant, water resistant, resistant against radiation, and the chemical damage determined by the characteristics of the content’ (FANC, 2015, p. 20; our translation). They carry small amounts of low radioactive materials (FANC, 2018c). The highest protection grade, type C, has to be resistant against accidental conditions including airplane accident (FANC, 2015, p. 20).

While packaging offering a lower grade of protection may be certified by recognized operators, packages offering a higher grade of protection have to be certified by the appropriate authorities (FANC, 2015).

The mode of transport is decided by the carrier, using the ALARA-principle (As Low as Reasonably Achievable), taking into account the locations of the consignor and consignee, and the possible routes. Safety and security measures are the main parameters to opt for a certain mode of transport (FANC, 2018c). But, although maritime shipping would be safer than transport over land, FANC (2018c) only allows maritime shipping when a sea has to be crossed. If there are other modes of transport available, these are preferred.

According to Greenpeace (2018), for the risk to be as low as possible, the transport mode that passes the least number of urban areas must be used. For transports from the nuclear power plant of Borssele to La Hague, maritime shipment would pass fewer urban areas than the current railway route.

The maximum radiation outside the package is limited to a maximum of 0.1 mSv/h at a distance of two meters. Highly active materials therefore necessitate a larger level of protection against radiation than low-risk materials. To limit radiation of medical isotopes outside the package to the maximum of 0.1 mSv/h, two or three millimeters of lead is sufficient. In contrast, one ton of spent fuel will require a package that weighs 100 tons or more. The weight is an important determinant of the mode of transport (FANC, 2018c).

2.2.2 Trustworthiness

Special attention is paid to trustworthiness of companies and people. They have to comply to a set of regulations before a security clearance can be obtained. All applicants for a security clearance, either Facility Security Clearance (FSC) or Personal Security Clearance (PSC), are screened by the National Security Authority (NSA). Only after the company received the FSC, its employees may apply for a PSC. A PSC must always be linked to a FSC company which must be registered with the NSA (2016).

FANC encourages companies to set up a trustworthiness program and to pay special attention to insider threat. Since the Charlie Hebdo attack the Belgian rail network administrator Infrabel has set up a trustworthiness program (Decelle, 2018). Transport
companies are provided with a Design Basis Threat (DBT), a tool that allows organizations and agencies to plan, design and evaluate a physical protection system. It has to assess the threat and characteristics of insider and outsider threat. The IAEA (2008b) recommends its member states to attribute the characteristics of potential insiders in the DBT and to evaluate the threat. Physical protection systems have to be designed based upon the DBT, which includes countermeasures for the unauthorized removal, sabotage or attack on radiological and fissile materials. Motivations, intentions and capabilities have to be described (Dresselaers & Fanielle, 2016; IAEA, 2008b). Companies tasked with UN group 2 transports have to comply with international regulation for dangerous goods (FANC, 2018c). The RID obliges railway transporters to organize extensive initial and periodical security training. These awareness trainings have to pay attention to changes in regulation, the Transport Security Plan (TSP), the nature of threats and risks, ways to recognize them and how to steer away from them. The company has to present records of these trainings to government agents when asked (RID, 2019). The highest categories of dangerous transports are given guidelines for the minimal content of a TSP, including trustworthiness of personnel (FANC, 2018c; RID, 2019).

2.2.3 Security measures

Safety measures have an important influence on security, known as collateral advantages or disadvantages. When assessing a terrorist threat, we need to take into account the attractiveness of the target, whether the material is targeted for theft or attack, and in case of theft, if the material is usable in a RED, RDD (FANC, 2018c) or IND. Industrial radiography devices for instance are small and light-weight and could therefore constitute easy targets. Due to the low radiation levels and small amounts of material in these devices, the attractiveness of the target is considered low. When radiation levels are high, the attractiveness of the target is high. Safety standards require nuclear materials to be transported in heavy packages. The theft of a 100-ton package is quite a challenge for any organization (FANC, 2018c). Most, if not all vehicles for nuclear transports have tracker systems and, in a country so densely populated as Belgium and such an elaborate camera network along roads, airports and waterways, a vehicle that can carry such load cannot be moved unnoticed (Greenpeace, 2018).

The regulations of FANC and the specific regulations for nuclear transport of the IAEA and Euratom include the training of staff, as well as the chosen mode of transport and the safety equipment on board. Marks on the packages include consignor and consignee, brute mass, type of package and when necessary, identification marks such as the UN-number and the identification number of the content. Depending on the category of the packages, labels have to be placed outside the packages. Road transports of radioactive and nuclear material (with exception of excepted packages) carry orange placards in front and back of the vehicle, and labels on the sides and the back. These placards and labels are designed to inform intervening personnel about the radiological activity and the specific substance on board. The transport documents have to contain the UN-number and identification number of the content, important radio-isotopes, the physical condition and chemical form, and other vital information (FANC, 2018c).
3  **Radiological and Nuclear Transport Terrorism**

Assessing the parameters proposed by Volders (2016) - *motivation, knowledge, availability* - and a cost-benefit analysis of an attack, we hypothesize three possible modi operandi for terrorist organizations:

1. **Theft:** Only UN group 1 and 2 transports are prone to theft as the packages are small enough to disappear. They can be used to develop an RED or RDD.

2. **Conventional attack on a radiological transport:** with the use of explosives, the transport may be used as a RDD.

These two types of attack have the highest chance of success, but the attractiveness is low. They are socially disruptive and economically devastating but cost no human life, unless lives are lost in the initial attack. The consequences for health, environment and property are close to none (FANC, 2018c; Greenpeace, 2018; Sauer & Volders, 2016).

3. **A conventional attack on a fissile materials transport.**

In Belgium there are UN group 2 radiological railway transports, consisting of uranium ores, and group 3 fissile materials transports, consisting of nuclear waste and spent fuel (Decelle, 2018; FANC, 2018c). Railway transports of groups 3 and 4 in Belgium have to comply with RID category 7 regulations (RID, 2019). Along the route, there are safe zones where the convoy can be diverted to. These places are shielded from public sight by screens. The security is assured by railway security staff (Securail) and police. Platforms in railway stations adjacent to the railway tracks used by the convoy are evacuated in case of maneuvers. All drivers and security personnel are in immediate contact with Securail, police, and Infrabel. They can alert the national Rail Operation Center in Brussels, and the nearest signal house. Transports are vulnerable when standing still or passing under bridges or other vantage points (Greenpeace, 2018). Any type of transport vehicle or vessel becomes a target when it passes a vantage point. Even more so if it is slowed down or comes to a complete halt. It gives terrorists time to charge and steal or explode the package. Well-funded and well-organized terrorist organizations can revert to different methods to slow down or stop the transport using insider knowledge. Terrorists can sabotage rails, but this will trigger an automatic alarm, giving them only a matter of minutes before Securail and police services will be on scene. The train will be halted automatically, after which it will be evacuated to the nearest safe zone. Road blocks can be raised in a matter of seconds, safeguarding the surprise element of the attack. According to Greenpeace (2018), certain weapons that can be bought on the international black market can penetrate reinforced packages before exploding inside.

This type of attack will necessitate extensive planning, funding and insider knowledge. Time tables, routes and security measures have to be mapped. If a transport can be slowed or halted, this can give terrorists enough time to fire upon the package and cause massive damage. Fissile material may be spread over a wide area, contaminating it, with devastating consequences for environment, human health and property. Extreme heat (such as from phosphor ammunition or deliberate crash with fuel trucks) may aerosolize the fissile material and create a dangerous nuclear cloud. If criticality is reached, a nuclear explosion
may occur (Greenpeace, 2018). To prevent criticality, the fissile materials are transported with sufficient distance between them. The package are tested to withstand heat of 800°C during 30 minutes (FANC, 2015, 2017a, 2018c, 2018d), but if an attack occurs at a specific spot (e.g. inside a tunnel) or with a certain type of weapon (phosphor ammunition), the package may be exposed to higher temperatures over a prolonged period of time (Greenpeace, 2018).

4 COUNTERING THE CBRN THREAT

In the following, we will try to shed some light on the external and internal CBRN threats and adequate means to counter them.

4.1 COUNTERING EXTERNAL CBRN THREAT

Countermeasures have to be taken against terrorist attacks, but any countermeasure can be countered in turn. Security forces can be overwhelmed, bribed, coerced or killed. The protection of the vehicle and the package can be countered by creating larger explosions, with possibly devastating collateral damage (Van Hauwe, 2018a).

One should not focus on one’s own strengths and weaknesses, but the threat must be assessed from the viewpoint of the terrorists. The question is: if you plan an attack, what weaknesses would you exploit and where would you strike? ‘Begin with the end in mind. Increase awareness and understanding about modus operandi used by hostiles … prior to attack’ (Van Hauwe, 2018a; slide 5 [ppt]).

If a malicious act is successful, an emergency plan should mitigate and minimize the effects of sabotage and contamination. Such a plan describes communication, provisions and countermeasures in case of emergency, personnel training for operational, guard and response units, and should contain a segment on how to retrieve stolen radioactive material (IAEA, 2008b). The emergency plan and Management Control & Accounting system (MC&A) should be interlinked. MC&A is a tool that controls which materials are used, stored or transported and in what quantity at any given time. It consists of an inventory that allows a profound follow-up of radiological and nuclear materials. Any material gone missing is immediately detected (Annual Report to Congress on Combating Terrorism, 2001).

Special attention needs to be paid to information security and the correct application of procedures (IAEA, 2008c). The IAEA (2008c) recommends as best practices:

1. Avoid similar transport schedules;
2. Plan routes away from sensitive areas. Plan alternative routes in case of anomalies;
3. The time between facilities should be kept to an absolute minimum;
4. Confidentiality; the number of staff should be kept at a minimum and information should be shared on a need-to-know basis;
5. Do not leave packages unattended;
6. During transport and intermodal transfers, the security measures should be consistent with those of the facilities (IAEA, 2008c). In 2013, a truck carrying radioactive cobalt was stolen in Mexico. The truck was discovered a few days later, the package was found in the neighborhood. No material was stolen. Similar incidents have occurred in Belgium twice. In every case, the radioactive material was recovered. Thieves targeted the trucks and found more than they bargained for. Every time, the truck was left unattended (FANC, 2018c; Sauer, 2017).

4.2 Countering Insider Threat

Assessing insider threat should be done for every transport and transport company individually (IAEA, 2008b). If every organization and every transport was secured the same way, it would constitute a weakness as an employee of one company would know the security procedures of the other (FANC, 2018c; Van Hauwe, 2018a, 2018b). Design criteria are important for security. Among others, this includes the physical and geographical separation of the transport and a strong diversity in systems. It would mitigate consequences if an attack is successful (IAEA, 2008b). To counter sabotage, the four eyes principle is of vital importance. But since two co-workers can corroborate in a malicious act, or the one can coerce the other, it is recommended to change partners on a regular basis. The IAEA (2008b) advises member states to raise security by employing more personnel. Additional security personnel can rapidly increase the security of a transport and knowledge can be split over more people, making it impossible for one person to obtain all information needed to commit a malicious act (Sagan, 2004). This measure contradicts the principle of minimal staff as stated in other IAEA recommendations (2008c). When more people operate in sensitive environments, more people may be targeted by terrorists. Sagan (2004) compares the security level to the safety level of an aircraft. Additional engines keep the aircraft in the air when an engine fails. Each engine serves as backup. But every engine is as prone to failure as the other. One engine can therefore fail and damage the other engines. The more engines on an aircraft, the higher the chance that the aircraft survives failure, but also the higher the chance an engine will fail and damage others. High numbers of security personnel may create new threats. Security should not depend on the amounts of resources and personnel, but on a thoroughly investigated and executed DBT, which combines technical and software engineering and social science perspectives (Sagan, 2004).

A multilayer defense system of security procedures, inventories (MC&A), access control rules, four eyes principle, and a trustworthiness screening of staff constitute important administrative barriers. Any measure, whether preventive or protective, has to be subject of periodical reassessment (IAEA, 2008b).

Security culture is the most valuable asset in countering any threat. IAEA (2008a) emphasizes ‘that nuclear security is ultimately dependent on individuals: policy makers, regulators, managers, individual employees and — to a certain extent — members of the public’ (p. 2). Nuclear security culture is ‘the assembly of characteristics, attitudes and behavior of individuals, organizations and institutions which serves as a means to support and enhance nuclear security. An appropriate security culture aims to ensure that the implementation of nuclear security measures receives the attention warranted by their
Companies should have contingency plans built into their safety and security strategy. It encompasses the mitigation and minimization of consequences in case of (possible) radioactive release, and the recovery of stolen materials (IAEA, 2008c). Aspects of personal life can be used to coerce an employee to collaborate or give up professional secrets. Staff should be trained to notice when a co-worker becomes a liability (e.g. depression, debts) and the company should have a system in place where such problems can be reported and investigated with regard to the charge and discharge of the accused employee (Decelle, 2018; Van Hauwe, 2018b). Decelle (2018) describes how the Belgian railway network operator Infrabel has set up a network of Local Security Officers (LSO). These LSO operate within local branches of Infrabel as security coaches for personnel. They collaborate with the responsible leader and the confidential counsellor of the local branch. When an employee is accused of being a liability to the security of the company or railway traffic, an investigation is conducted with regard to charge and discharge. First, the accused employee is invited to an interview with the leader and the confidential counsellor. No security officers are present at the time, so that the employee does not feel threatened. When there are signs of external forces (blackmail, etc.), police services are alerted. In a second phase, another interview is organized in the presence of security officers. If problems are found, the employee can be moved to another post where he cannot do any harm, or is fired (Decelle, 2018). Van Hauwe (2018b) warns that firing personnel can only be the very last step of the process. When the employee leaves the company, he leaves with profound knowledge of security measures, procedures, befriended coworkers, etc. Van Hauwe (2018b) advises to move the employee to a post where he cannot do any harm, but where he remains under control of the security officer and can be helped by training, and deradicalisation programs.

In December 2017, ARTE TV broadcasted the documentary Sécurité Nucléaire: le grand mensonge (Nuclear Security: the big lie) (Guéret, 2017). Activists showed a map of France, showing the most used transportation modes, the classic route and often used alternative routes. Although the documentary was intended to denounce holes in the security of such transports, sensitive information was shared on television. The activists explained how they obtained this information and showed good vantage points from where the transport could be attacked. There is always a risk that the actions of pacifists become self-fulfilling prophecies.

After the 2016 Paris attacks, detectives found footage of the home of a top executive of the Belgian nuclear research center (Van Dooren, 2016, February 17th). The Belgian Parliamentary Papers show that the Chamber of Representatives paid little attention to the matter. The Minister of Interior did undertake measures by his own initiative. A special corps within Federal Police services will be founded for the protection of six nuclear facilities and Brussels Airport as an armed unit on site. The teams will be trained to counter drone attacks, suspicious packages and other external threats, to test nuclear security...
measures and to control potential violent situations. A fast response team will be formed (Chamber of Representatives, 2016, April 13th, 2016, December 7th). The plans of the Minister of Interior do not address security of transport of radioactive material. It is unclear whether the fast response team is trained to intervene in terrorist incidents involving radioactive transports, neither if they are part of the escort. A special unit within the Federal Police service is already tasked with these escorts (Dresselaers, personal communication, 2020). To this date, the special corps and the fast response team of the Federal Police are yet to be created. Since December 21st, 2018, Belgium has not had a government with full powers capable of creating such police divisions and the Police services are confronted with a large shortage of staff. Meanwhile, some security duties are performed by the military (Chamber or Representatives, 2018, November 7th).

FANC and the National Security Administration of the United States (NNSA) stress the importance of insider threat mitigation (FANC, & NNSA, 2020). Therefore, they founded an international work group to address insider threat (FANC, 2020), based on the 2016 IAEA Information Circular concerning the mitigation of insider threat, which is endorsed by 31 countries and Interpol (Fanc, & NNSA, 2020).

5 CONCLUSION & RECOMMENDATIONS

FANC widened its focus from safety of Belgian radioactive transports to include security. According to Decelle (2018), railway security (including nuclear transports) has been boosted after the 2015 Charlie Hebdo attacks. Plans are to screen employees by the NSA (Infrabel, personal correspondence, 2019). The division of radioactive transports in four groups with a graded safety approach has only been set up since January 1st, 2018. Additional security permits are since 2011 required for UN groups 3 and 4 transports (FANC, 2018c). This might prove a liability as radiological terrorism of UN groups 1 and 2 transports can cause social and economic disruption. As we have shown, there are three plausible attack modes, depending on motivation, knowledge and availability (Volders, 2016). Terrorists could steal or detonate the packages for UN groups 1 and 2 transports, or they could detonate UN group 3 or 4 transport packages. Materials of UN groups 1 and 2 transports used in RDD or RED will have low or no effects on health and environment. The psychological effect will be dire; social and economic damage vast. Theft of UN group 3 or 4 transport packages is near to impossible in Belgium due to the weight and size of the packages. In a small and densely populated country with high-tech tracking devises in the vehicles and an elaborate camera network, it is impossible to get away unnoticed. An explosion of a UN group 3 or 4 transport packages will have massive health and environmental consequences. A large area will be contaminated and may be uninhabitable for years.

Theft of UN group 1 or 2 transport packages or an explosion will have less dire consequences, but is easier to plan and will necessitate far less funding and preparation. The attractiveness of detonating a UN group 3 or 4 package is much higher but necessitates a longer preparation and more funding. These packages are built in such a way that they can withstand external pressures and heath. Greenpeace (2018) states that weapons can be bought on the international black market that penetrate these packages and detonate inside.
There is no evidence of such weapons being smuggled or sold in Belgium. But neither is there any evidence against it. The Belgian Ministry of Interior and the Belgian intelligence services should map smuggling routes in Europe. The EU should boost border security in an effort to prevent the smuggling of weapons and radioactive materials.

FANC focusses on insider threat and on how to prevent sensitive information from falling into malicious hands. No matter how high-tech a security system is, the strongest and weakest link of any security system is the staff. A trustworthiness-investigation is recommended, even for UN groups 1 and 2 transports. It is recommendable to check references of new applicants to see whether they are considered trustworthy by their previous employer. To counter insider threat, a multilayer defense system is recommended. Security procedures, inventories (MC&A), access control rules, four eyes principle, and a trustworthiness screening of current personnel and applicants constitute important administrative barriers. All people carrying cameras, scouting sites or vantage points, should be kept at close eye and their identities checked. Routes and security routines should be altered as often as possible and as is reasonably acceptable. The four eyes principle is based on the idea that one employee is the controlling factor of another employee. This principle should reduce the risks of insider threat. It could be recommendable to invoke the four eyes principle in UN groups 1 and 2 transports, but further research is needed to show whether this is economically viable. It is recommendable to change partners on a regular basis (Van Hauwe, 2018a).

The IAEA (2008b) emergency plans make no distinction between insider and outsider threat. This is a liability if it results in lack of attention or specialization in either threat. The measures needed to counter these threats can produce infringements and interference in the market economy, personal liberty, privacy (Sauer & Volders, 2016) and human rights. The tension between the necessity for more security and safeguarding privacy and liberty, is a conundrum for which a wide range political and social discussion is needed.

Terrorist organizations have evolved over the past 25 years. Security has to be updated, based on a DBT and TSP. Boasting security staff may be a necessary measure, but one should beware of redundancy. The most important factor in designing a new strategic security plan for nuclear transport is changing the viewpoint of the designer on security strategies. Rather than designing a security strategy from the viewpoint of the defender, it should be designed from the viewpoint of the attacker.

We found no evidence of major improvements against outsider threat during transport. However, the Belgian Ministry of Interior has upgraded facility security, which included major improvements in the security procedures and updates of protective measures against insider threat in the transportation of radioactive and nuclear materials.

6 References

6.1 Articles and Books


6.2 WEBSITES AND MEDIA


6.3 Interviews and Presentations


FANC. (2018, June 14th). Service Importation & Transport - Dienst Invoer & Vervoer [Import & Transport Office] [presentation].
6.4 **Legislation and Judicial Documents**


**RID Hoofdstuk 1.10 - Bepalingen betreffende de beveiliging [RID Chapter 1.10 - Provisions concerning security], (2019).**