Evolution of Radiological and Nuclear Threats: Intermediate Note for Task 3.1

Date: 31.05.2020

Contract No. 833573

This project has received funding from the European Union's Horizon 2020 research and innovation under grant agreement No. 833573

Document Information			
Contract No.	EC Contract 833573		
Coordinator	ENEA		
Document reference (file name)	INCLUDING_WP3_IAI_Intermediate Note_3.1		
Document status	Final		
Document Responsible Partner	IAI		
Document Type	Report		
Work - package No.	3		
Classification			
Lead author:	Ottavia Credi (IAI)	**Verification Panel**	Steering Board Security Board Project Security Officer
Co-authors:	Karolina Muti (IAI) Paola Tessari (IAI)		

Dissemination Level:

PU	Public	
PP	Project Private, restricted to other programme participants (including the Commission Services)	
RE	Restricted to a group specified by the consortium (including the Commission Services)	
CO	Confidential, only for members of the consortium (including the Commission Services)	
Restraint UE	Classified with the mention of the classification level restricted "Restraint UE"	
Confidential UE	Classified with the mention of the classification level confidential "Confidential UE"	

Partners Involved in the Document

No.	Partner	Short Name	Check if involved
1	AGENZIA NAZIONALE PER LE NUOVE TECNOLOGIE, L'ENERGIA E LO SVILUPPO ECONOMICO SOSTENIBILE	ENEA	
2	ASTRI POLSKA SPOLKA Z OGRANICZONA ODPOWIEDZIALNOSCIA	APL	
3	INSTITUTO DE ENGENHARIA DE SISTEMAS E COMPUTADORES, TECNOLOGIA E CIENCIA	INESC TEC	
4	ISTITUTO AFFARI INTERNAZIONALI	IAI	
5	UNIVERSITA CATTOLICA DEL SACRO CUORE	UCSC	**X**
6	INTERNATIONAL SECURITY COMPETENCE CENTRE	ISCC	**X**
7	FRAUNHOFER GESELLSCHAFT ZUR FOERDERUNG DER ANGEWANDTEN FORSCHUNG E.V.	FHG	
8	VALSTYBES SIENOS APSAUGOS TARNYBA PRIE VIDAUS REIKALU MINISTERIJOS	NSCOE	**X**
9	MAGYAR TUDOMANYOS AKADEMIA ENERGIATUDOMANYI KUTATOKOZPONT	MTA EK	**X**
10	ETHNIKO KAI KAPODISTRIAKO PANEPISTIMIO ATHINON	NKUA	
11	TEKEVER ASDS	TEK	
12	MINISTRY OF NATIONAL DEFENCE, GREECE	HMOD	**X**
13	COMMISSARIAT AL'ENERGIE ATOMIQUE ET AUX ENERGIES ALTERNATIVES	CEA	
14	MIKKELIN KAUPUNKI	SSAV	
15	MINISTERIO DA ADMINISTRACAO INTERNA	PSP	**X**

Executive summary

This report is the Intermediate Note of Task 3.1, "Evolution of RN threats". The Intermediate Note is an internal preliminary contribution to INCLUDING activities, and it will feed into the official Deliverable, D3.1 "Evolution of RN threats" due at M56. This analysis will focus on RN unconventional threats and how they are evolving, by investigating the trends which are likely to characterise radiological and nuclear (RN) events that might be conducted by criminal or terrorist actors in the future. By examining cases that have occurred in the past, the Note tries to assess the types of threats that continue to represent a risk today and might continue do so in the upcoming years. Accordingly, the Note also aims to provide inputs to Task 3.2 and Task 3.3, with the inclusion of some preliminary findings related to main strengths and weaknesses of the management of RN events.

The first part of the document is an overview of past RN events. More specifically, it takes into consideration cases that saw the involvement of RN material in the past few years. The analysis ranges from smuggling activities, such as the illicit trafficking of nuclear material that was recently discovered in Vienna (December 2019), to sabotage of nuclear facilities, like the attempted sabotage of the Doel Nuclear Power Station (August 2014).

Building upon the past events, the report outlines the evolution of RN events conducted by criminal or terrorist networks. Four types of dangerous activities involving RN material are identified as most likely to pose future threats – the smuggling of RN material, cyber-attacks to nuclear facilities, sabotage of nuclear installations or other facilities hosting RN material, and construction and employment of RN crude devices. New technologies, such as unmanned aerial systems (UASs) could have an impact on the development of future threats and are taken into consideration in the analysis. After having delineated such threats, some space is dedicated to an assessment of the perception of the community of RN experts on the matter. A final section briefly introduces a selection of existing weaknesses in the training activities meant to instruct those involved in RN emergencies. On this issue, special attention is given to the importance of effective collaboration between the civil and the military sectors.

CONTENTS

LIST OF FIGURES

1. Introduction

1.1 The INCLUDING project

INCLUDING connects 15 Partners from 10 EU Member States (MS), bringing together infrastructure, equipment and experts coming from Medical Organizations, Fire Corps, Government Department, Municipalities, Law Enforcement Agencies, Ministries, Governmental and Civilian Research Institutes and Industries operating in the field of radiological and nuclear emergencies. Far from being a simple aggregation of entities separated geographically and with complementary expertise, INCLUDING pursues to develop a Federation in which individual Members will cooperate together to provide a common framework to standardise access to their respective facilities, enhance interoperability and allow a more intensive use of expensive equipment. The operative tool to manage the Federation will be a web-based platform with a sophisticated architecture and whose functionality has been proven in a previous EU project. At the same time, the project aims to enhance practical know-how and to boost a European sustainable training and development framework for practitioners in the Radiological and Nuclear Security sector.

The INCLUDING project will be flexible in order to include new facilities and innovation in technology, organisations and procedures. The plurality of facilities and expertise in the INCLUDING Federation reflects the complex and intertwined structure of the prevention and response phases of RN threats and will provide to the practitioners a set of real or emulated scenarios where to test concept of operations in a controlled environment.

The Joint Actions will be the focal points of the project. They are multidisciplinary field exercises, table-top exercises, training, serious gaming and simulation organised at their premises by the project partners and with the objective of demonstrating the added value of the Federated scheme and of the use of an innovative tool like the INCLUDING web based Platform to manage a pan European network of training facilities and resources.

1.2 Scope of the project

The main objectives of INCLUDING are:

- To provide Practitioners in the RN security sector an Innovative European cluster pursuing a Pan-European Federated model to optimise sharing of resources and expertise and paving the way for a certified collective membership easing inter-facilities access to members of the Federation and smooth the way for equipment circulation;
- To develop a centralised improved management tool for remote booking and utilisation of resources in the Federation, joint engagement in training sessions development and post-event assessment;
- To contribute to the development of a common learning framework for RN training also to facilitate the uptake and integration of new technologies and methodologies for practitioners in the RN field;
- To capitalise results and training facilities developed in previously funded EU and national projects;
- To execute Joint Actions (drills, multidisciplinary field exercise, table top exercise, training sessions, instrument testing, etc…) to validate the Federated model and whose scenarios are developed following the reconnaissance of emerging RN unconventional threats and to bridge gaps in the specific exercise, simulation and training functions;
- To collaborate with other EU projects and Clusters and plan future developments enabling long-term cooperation and future Federation enlargement and sustainability.

1.3 Purpose of the document

The purpose of Work Package 3 is to conduct a review of RN events with a specific focus on intentional and terroristic (or potentially terroristic) activities. WP3 will study emerging unconventional threats with a focus on reported attempts to smuggle radiological and nuclear materials, dirty bombs fabrication, radiological poisoning, threatened attacks to nuclear installations, in order to assess strengths and weaknesses in the whole crisis management cycle (from Prevention to Recovery). In this context, this Intermediate Note of Task 3.1 is an internal note on RN unconventional threats and how they are evolving to provide an overall analysis of the state of the art of RN terroristic and intentional activities and the emerging key trends. The analysis is produced to serve also as a starting point for Task 3.2 and Task 3.3.

1.4 Research perimeter

The research conducted in this Intermediate Note focuses on past unconventional events that saw the employment of radiological or nuclear material and trends which might outline future criminal and terrorist activities. In line with INCLUDING definition, an unconventional RN scenario is "a threat that materializes as an abrupt and brutal event that evolves to a complex problem where every weakness comes to the forefront if proper measures are not taken in advance".[1] The first episode of radiological and nuclear terrorism dates back to 1995 in Moscow, when Chechen rebels alerted the international media threatening the possible detonation of a canister containing 137Cs. This event brought to public domain the concept of "dirty bomb". Since then, the RN unconventional scenarios have been evolving. For this reasons, types of events that will indeed be considered here and that belong to such new "scenarios " include the following: illegal trafficking and smuggling of RN material, detonation of a dirty bomb, intentional dispersal of RN material in the environment, sabotage of a nuclear facility. Both intentional/criminal acts and attempted terrorist attacks will be taken into account. Violent activities conducted by organised crime generally have profit as their final objective. Differently, terrorists normally act with the goal of intimidating the population or forcing governments or institutions to achieve their own political objectives.[2] All the examined cases and future threats have intentional causes, and are conducted by malicious actors, in line with the IAEA Glossary classification.[3] For the sake of this analysis, malicious actors are terrorist and criminal individuals or organisations. Accidental RN events related i.e. to natural disasters, military warfare, industrial accidents are not included in this report, being out of the scope of the Project.

The research focuses on events occurred in the EU geographical area limited to the last ten years (namely, 2010-2020). The geographical and time perimeter is the foundation to provide an analysis that should reflect the recent evolution of RN related threats, specifically in the EU territory, so as to give a first input for the identification of gaps in training at an EU level and Joint Actions use cases/scenarios. RN events occurred outside the European geographical area or the aforementioned timeframe are mentioned only if particularly important, or when relevant for the aim of this study.

1.5 Methodology

The first part of this Note was drafted through in-depth desk research aimed at gaining a comprehensive picture of past RN criminal and terrorist events in Europe, in order to analyse how RN events have evolved in the last 10 years. The desk research was conducted by IAI as WP leader, and complemented by the contributions received from the WP partners. In particular, partners gave their input by sharing information on RN unconventional events

[1] INCLUDING Grant Agreement, Part B, p. 2.
[2] UNODC, University Module Series, https://www.unodc.org/e4j/en/organized-crime/module-1/key-issues/similarities-and-differences.html.
[3] Taking as point of reference the IAEA Glossary, the events and threats considered in this analysis are those incidents that have intentional causes, and that are unauthorized, malicious acts, e.g. sabotage, or theft. See: IAEA, "IAEA Safety Glossary. Terminology Used in Nuclear Safety and Radiation Protection", 2018, Table at p.86, https://www-pub.iaea.org/MTCD/Publications/PDF/PUB1830_web.pdf

occurred until 10 years in the past and by providing written contributions on their specific expertise.

In addition, IAI prepared a questionnaire that was distributed during the INCLUDING Workshop on 27th January 2020 in Frascati and completed by 20 stakeholders belonging to the RN community. The questionnaire's purpose was to gather feedbacks and inputs on stakeholders' perception regarding specific RN unconventional threats and on the likelihood for these events to happen in the future, as well as on gaps in training from Prevention to the Recovery phase. To this end, participants were asked to either respond with open answers to given questions or assign a value from 1 to 5 to given statements. Individuals with different backgrounds related to the RN sector, ranging from first responders to RN experts, participated to the survey. This allowed IAI to assess what these parties consider to be the most urgent issues to address, besides gathering a series of advice and recommendations on the matter. A detailed statistical analysis of answers delivered by stakeholders is reported in Annex I, that is the classified part of the document.

On this basis, the second part of the Note presents a forecast of potential future trends that may represent RN unconventional threats in the upcoming years. Throughout the report, different types of events that see the employment of RN material for malicious purpose are taken into account following an order of relevance. Priority is therefore given to cases that are likely to represent a threat in the future.

1.6 Glossary of Acronyms

Acronym	Description
CBRN	Chemical Biological Radiological Nuclear
CEPC	Civil Emergency Planning Committee
EDF	Électricité de France
GICNT	Global Initiatives to Counter Nuclear Terrorism
HEU	Highly Enriched Uranium
HMI	Human-Machine Interface
IAEA	International Atomic Energy Agency
IND	Improvised Nuclear Device
IS	Islamic State
ITDB	Incident and Trafficking Database
LEU	Low Enriched Uranium
MS	Member States
NC3	Nuclear Command, Control and Communication
NSS	Nuclear Security Summit

RN	Radiological and Nuclear
RDD	Radiological Dispersal Device
RED	Radiological Exposure Device
SAT	Systematic Approach to Training
SCADA	Supervisory Control And Data Acquisition
UAS	Unmanned Aerial System
UN	United Nations
UNODC	United Nations Office on Drugs and Crime
VPN	Virtual Private Network
WP	Work Package

2. RN UNCONVENTIONAL THREATS: AN OVERVIEW OF RN UNCONVENTIONAL EVENTS IN THE PAST

This section aims to present an overview of the RN unconventional threats in the past, by introducing the most relevant cases that happened in the last 10 years in the EU territory. This analysis will serve as a basis for the understanding of the evolution of the RN threat, from which it will then be possible to extrapolate current and future trends.

Before starting the review, it is essential to recall the regulatory framework for the prevention of nuclear terrorism at a global level. The most comprehensive Treaty in force is the *International Convention for the Suppression of Acts of Nuclear Terrorism (ICSANT)* adopted on April 13th, 2005, during the 91st plenary meeting of the General Assembly of the United Nations (UN).[4] The Convention is designed to criminalise acts of nuclear terrorism and promote police and judicial cooperation to prevent, investigate and punish such acts. So far, the Convention counts 115 signatories and 116 state parties. The main scope of the Convention is ensuring all State parties recognise the offences set forth in Art. 2 as criminal offences under their national law. This is important in order not to allow the existence of "safe islands" for individuals involved in acts of nuclear terrorism. The Convention does not apply to the activities conducted by armed forces during armed conflicts, as they are governed by international humanitarian law. Nor does it apply to the activities of military forces in the exercise of their official duties, which are governed by other rules of international law. Lastly, the Convention does not address the issue of the legality of the use or threat of use of nuclear weapons by States.

The other international legal instrument worth mentioning is the *Convention on the Physical Protection of Nuclear Material (CPPNM)*, signed in Vienna and New York on March 3rd, 1980.[5]

[4] UN, "International Convention for the Suppression of Acts of Nuclear Terrorism," 2005, https://treaties.un.org/doc/db/Terrorism/english-18-15.pdf.
[5] IAEA, "Convention on the Physical Protection of Nuclear Material," Legal Series No. 12, Vienna, Austria, 1982, https://www-pub.iaea.org/MTCD/Publications/PDF/Pub615web.pdf.

The CPPNM was amended in 2005, but these important amendments eventually came into force in 2016. The Convention with its amendments is the only international legally binding undertaking in the area of physical protection of nuclear material in international and domestic use, storage and transport. It establishes requirements to the Member States to develop, implement and maintain nuclear security regime comprising the measures related to the prevention, detection and response to the malicious and other intentional unauthorised activities involving nuclear material and related infrastructure. The CPPNM requires the Member States to set up the punishment for offenses related to unauthorised use, theft and ancillary offences, as well as for sabotage and smuggling of nuclear material.

Among the several international activities in the nuclear security sector*, the Global Initiatives to Counter Nuclear Terrorism (GICNT)* is worth noticing.[6] The GICNT is a voluntary international partnership of 89 nations and 6 international organisations (EU included) committed to enhancing global capacity to prevent, detect, and respond to nuclear terrorism. It works toward this goal by conducting multilateral activities that strengthen the plans, policies, procedures, and interoperability of partner nations.

In the past ten years, one of the most worrying activities concerning RN material has been its illicit trafficking and attempted smuggling. The International Atomic Energy Agency (IAEA) defines such practice as "the receipt, possession, use, transfer or disposal of radioactive material without authorization".[7] The substances being trafficked are both fissile materials which could potentially be used to produce nuclear devices, such as plutonium or highly enriched uranium (HEU), and other radiological materials that are typically used in civilian as well as military sectors, particularly in the industrial and medical fields.[8]

The IAEA manages the Incident and Trafficking Database (ITDB) system, meant to assist the Agency's Secretariat, participating States and selected international organisations to improve nuclear security.[9] The ITDB collates authoritative information reported on a voluntary basis by participating States on incidents involving illicit trafficking and other unauthorised activities involving nuclear and other radioactive materials. Information on reported incidents is only communicated via a network of Member States Point of Contacts, while the access to the complete database is limited to a small number of IAEA staff and governed by security rules.

An example of smuggling activities in the EU territory took place in December 2019. Three individuals belonging to a criminal network were arrested for attempting to sell a nuclear container, supposedly containing radiological material, to an army for 3 million euros.[10] The operation involved the Austrian Law Enforcement and the Moldovan General Police Inspectorate, coordinated by Europol.

---

[6] For more information, visit GICNT's official website: https://gicnt.org.
[7] IAEA, "Prevention of the inadvertent movement and illicit trafficking of radioactive materials," September 2002, https://www-pub.iaea.org/MTCD/Publications/PDF/te_1311_web.pdf.
[8] VERTIC, "Illicit Trafficking of Nuclear and other Radioactive Material - The Legislative Response," London, United Kingdom, April 2012, http://www.vertic.org/media/assets/Publications/ITR_WEB.pdf.
[9] IAEA, "Incident and Trafficking Database (ITDB)," https://www.iaea.org/resources/databases/itdb.
[10] Europol, "Crime group suspected of smuggling nuclear materials arrested in Vienna," 6th December 2019, https://www.europol.europa.eu/newsroom/news/crime-group-suspected-of-smuggling-nuclear-materials-arrested-in-vienna.

Between 2018 and 2019, there were several cases of suspected selling and delivery of scrap metals. In the Netherlands, four individuals were found to be involved in the illegal selling of radioactive scrap metal used in ballast blocks on ships, and were arrested by the authorities in June 2018.[11] In the following months (November 2018, January 2019 and March 2019), metal cylinders of approximately 1 cm radius and 10 cm length containing Cobalt-60 (Co-60) were found in the port of Rotterdam in three different shipments.[12] In the same period, in the port of Hamburg (Germany) a radioactive source of Co-60 was found in a container, which was part of a scrap metal delivery from Western Africa.[13] All of the aforementioned cases saw the involvement of a delivery shipping containing radioactive sources.

Besides the areas that were just mentioned, the former Soviet Union continues to represent a major junction for the smuggling of radioactive substances, with special regard to Ukraine, Russia, Georgia, and Belarus. Between 2010 and 2015, several individuals were arrested because they were involved in smuggling and trafficking activities of RN substances in Moldova, Georgia and Ukraine. Due to this area's proximity to the EU territory, it is important to be aware of possible smuggling networks that may result in threats for the Old Continent.

RN materials have also been used to harm people through poisoning. The most well-known case is the killing of the former Russian secret service agent Alexander Litvinenko, occurred in London in November 2006. Litvinenko was poisoned with Polonium-210 (Po-210), a radioactive substance particularly suited for direct irradiation, as it leaves the murderer completely unscathed.[14] Another relevant case of suspected radioactive poisoning is the death of the Moroccan model Imane Fadil. Her death was suspected to be caused by radioactive poisoning because her blood work revealed unusual levels of heavy metals such as Cobalt (Co), Chromium (Cr) and Molybdenum (Mo).[15] She was admitted at a hospital in Milan at the end of January 2019 claiming she had been poisoned, and died on March 1st, 2019. The results of the test taken on the woman's body then excluded the possibility that radioactive poisoning could have been the cause of death. Analysis on samples of Ms. Fadil's organ tissues were conducted by ENEA's Institute of Radioprotection (Italy).[16] Formerly, the Institute carried out a screening on biological samples of Italian citizens who, according to police

[11] James Martin Center for Nonproliferation Studies (CNS), "CNS Global Incidents and Trafficking Database," July 2019, https://media.nti.org/documents/global_incidents_trafficking_2018.pdf; DutchNews.nl, "Scrap metal dealers arrested for passing on radioactive metal waste," 20th June 2018, https://www.dutchnews.nl/news/2018/06/scrap-metal-dealers-arrested-for-passing-on-radioactive-metal-waste/.

[12] Laka - Documentation and research centre on nuclear energy, "Dangerous Co60 sources discovered in scrap metal containers," https://www.laka.org/docu/ines/event/1147.

[13] Laka - Documentation and research centre on nuclear energy, "Co60 source discovered in a scrap metal delivery," https://www.laka.org/docu/ines/event/1148.

[14] BBC News, "Alexander Litvinenko: Profile of murdered Russian spy," 21st January 2016, https://www.bbc.com/news/uk-19647226; The Economist, "The Litvinenko affair: Murder most opaque," 13th December 2006, https://www.economist.com/taxonomy/term/29/0?page=859.

[15] De Riccardis, S., "Imane: nessuna traccia di radioattività", La Repubblica, 21st March 2019, https://milano.repubblica.it/cronaca/2019/03/21/news/imane_fadil_ruby_ter_berlusconi_esami_radioattivita_-222159336/

[16] RaiNews, "Anche l'Enea esclude la presenza di radioattività nel corpo di Imane Fadil. Iniziata l'autopsia," 26th March 2019, http://www.rainews.it/dl/rainews/articoli/Morte-Imane-Fadil-radioattivita-anche-Enea-esclude-autopsia-da337c8e-446f-41cc-9ef1-49b249352fc3.html.

investigations. came into direct or indirect contact with the alleged perpetrators of the Litvinenko poisoning.[17]

Criminal or terrorist attacks involving RN material may also be directed against the very infrastructure where these substances are kept or produced. Nuclear facilities have long been recognised by experts as potential targets for terrorists willing to conduct at an attack or a sabotage.[18] Belgium experienced a few cases of attempted attacks and sabotage to nuclear facilities in recent years. In 2013, the nuclear research centre located in the Belgian city of Mol, was targeted by two individuals who managed to scale the fence, break into the laboratory and steal some equipment.[19] In August 2014, an employee of the Doel Nuclear Power Station (Belgium) caused a five months shut-down of a reactor turbine by intentionally draining 65.000 liters of the lubricant for the reactor turbine.[20] Lastly, in 2015, Belgian police found out that the terrorists who perpetrated the Paris terrorist attacks occurred in November of the same year were originally monitoring an official who worked in multiple Belgian nuclear research sites, where a wide range of nuclear and radiological materials, including HEU, were stored.[21]

Nuclear facilities have also been the target of cyber-attacks by violent non-state actors. In April 2016, the Gundremmingen Nuclear Power Plant in Bavaria (Germany) was infected by a malware aimed at stealing the facility's data.[22] Although the attack did not seem to cause serious damages to the operations of the power plant, the malware infected the computer system that managed the fuel rod-monitoring system in the plant's B unit, as well as 18 removable data drives linked to computers not connected to the plant's operating system. Two of the viruses found were Conficker, which is used to obtain login information and financial data, and W32. Ramnit, which targets Microsoft Windows software systems to steal files and allows the attacker to remotely control a system that is connected to the Internet.[23]

An alleged episode of cyber threat to a nuclear facility was the Stuxnet case. Stuxnet was a computer virus, which was first uncovered in 2010. Stuxnet did not simply target computers – it was meant to physically destroy the equipment controlled by computers. Nobody ever openly admitted the responsibility for its creation, however some analysts' reports claimed that the virus targeted five Iranian industrial facilities.[24] Even though Stuxnet apparently did not slow

[17] ENEA private communication.
[18] Pomper, M. and Tarini, G., "Nuclear terrorism – Threat or not?," AIP Conference Proceedings 1898, November 2017, https://aip.scitation.org/doi/abs/10.1063/1.5009230, p. 4.
[19] Rubin, A. and Schreuer, M., "Belgium Fears Nuclear Plants Are Vulnerable," *The New York Times*, 25th March 2016, https://www.nytimes.com/2016/03/26/world/europe/belgium-fears-nuclear-plants-are-vulnerable.html.
[20] Rosenbach, E. and Chorev, M., "Belgium Highlights the Nuclear Terrorism Threat and Security Measures to Stop it," HuffPost, 29th March 2016, https://www.huffpost.com/entry/belgium-nuclear-terrorism_b_9559006?guccounter=1; Rubin and Schreuer, "Belgium Fears Nuclear Plants Are Vulnerable."
[21] Pomper, M. and Tarini, G., "Nuclear terrorism," p. 3-4; The Conversation, "How to protect nuclear plants from terrorists," 13th April 2016, https://theconversation.com/how-to-protect-nuclear-plants-from-terrorists-57094.
[22] Van Dine, A., Assante, M. and Stoutland, P., "Outpacing cyber threats. Priorities for cybersecurity at nuclear facilities," Nuclear Threat Initiative (NTI), 2016, https://media.nti.org/documents/nti_cyberthreats__final.pdf, p. 29.
[23] *Ibid.*
[24] Albright, D., Brannan, P. and Walrond, C., "Stuxnet Malware and Natanz: Update of ISIS December 22, 2010 Report," ISIS Report, 15th February 2011, pg 2 in Kesler B., "The Vulnerability of Nuclear

down Iran's accumulation of low-enriched uranium (LEU), it may have successfully disrupted the Iranian centrifuge programme.[25] Although this cyber-attack has never been officially proven and remains a disputed reconstruction, it still represents an instructive exercise in assessing the impact a highly sophisticated virus may have on nuclear facilities, therefore demonstrating how similar conceived attacks represent a possible scenario.

Viruses like Stuxnet represent high-quality means that can be employed to perpetrate attacks resulting in major consequences. However, cyber-attacks can also occur through a simple computer intrusion. An example is offered by the attack suffered by the Areva group in France, in September 2011.[26] The attack consisted in a large-scale network intrusion that forced the group to increase security measures for three days around in September 2011.[27]

3. RN UNCONVENTIONAL THREATS: EVOLUTION AND RECENT TRENDS

The first section provided an overview of RN events that happened between 2010-2020, to demonstrate their relevance and occurrence. In the following section, we will bring the analysis further to attempt an assessment of how the RN threat can evolve in the future and what are likely to be its most relevant trends.

In brief…

- The illicit trafficking and smuggling of RN material continue to be a serious source of concern. Particularly worrying is the threat of contraband of RN agents through maritime shipping. Regarding the geographical distribution of smuggling activities, special attention should be placed on the Eastern European region. To counter the continued threat of illicit trafficking of RN material, the international community could consider adopting a set of common security standards, as well as enhancing the detection technologies that are currently in place.

- Due to the new and widespread availability of technologies and know-how, cyber-attacks represent a particularly threatening type of operation through which malicious actors might target a nuclear installation. It is crucial to enhance cybersecurity measures that need to encompass both minor negligence such as the admission of guests' computers and USB flash drives inside nuclear facilities, and more substantial threats like the risk of malwares infecting a facility's informatic system.

- A potentially new threat consists in the possible employment of unmanned aerial systems to conduct RN attacks. More specifically, experts are showing concern about the risk of drones flying over nuclear facilities gathering sensitive information that might prove useful in the planning of a future attack, as well as drones being used as dirty bomb-carriers.

Facilities to Cyber Attack," *Strategic Insights*. Volume 10, Issue 1, Spring 2011, http://large.stanford.edu/courses/2015/ph241/holloway1/docs/SI-v10-I1_Kesler.pdf, p. 21-22.

[25] *Ibid*.

[26] Areva was a French corporation specialising in nuclear power and renewable energy.

[27] Amiard, J-C., "Nuclear Accidents: Prevention and Management of an Accidental Crisis," February 2020.

- The risk of insider threats in nuclear facilities is to be taken into serious consideration. This applies to different categories of potential attackers: for example, individuals who do not have specialised skills but have access to critical areas of a facility hosting RN material, people who may not have direct access to such areas but possess advanced technical competences (e.g. in the cyber realm) and also blackmailing of an employee with access to a nuclear safety-sensitive area to force him to carry out a damaging attack.

- With specific reference to the use of RN material for an attack by terrorists, the main source of worry seems to be a possible significant improvement in the technological competencies of terrorists interested in conducting a RN attack. For this reason, stakeholders wish for meaningful advancements in the counter-action to technological and cyber-attacks on behalf of the appointed authorities.

3.1 Intentional RN acts with malicious purpose

The risk of criminal or terrorist organisations conducting an attack with RN weapons or material has always been considered threatening. However, this worry became more heightened after the events of September 11th, 2001, which showed how violent non-state actors might be intentioned to resort to means of attack able to provoke hundreds, if not thousands, of victims. In such context, RN materials pose a particularly worrying threat, as just a few grams of some RN agents have the potential of causing significant harm.[28]

Some terrorist groups have been trying to obtain RN know-how and material for some time.[29] The Islamic State (IS) made public declarations about its ability to acquire and smuggle nuclear weapons.[30] The IS also seems capable of inspiring and radicalising individuals who already possess knowledge on RN weapons and materials.[31] A representative case is that of Ilyass Boughalab, who became an IS militant after having worked for three years as a welding technician at a Belgian inspection and certification organisation, which granted him regular access to the Doel Nuclear Power Plant.[32] In Syria, Boughalab became a member of a brigade composed of dozens of Belgians nationals, including Abdelhamid Abaaoud, who is considered to be the leader of the 2015 Paris attacks.[33]

[28] Downes, R., Hobbs, C. and Salisbury, D., "Combating nuclear smuggling? Exploring drivers and challenges to detecting nuclear and radiological materials at maritime facilities," *The Nonproliferation Review* Vol. 26 No. 1-2, 2019.
[29] Rühle, M., "Analysis - The nuclear dimensions of jihadist terrorism," NATO Review, October 2017, https://www.nato.int/docu/review/articles/2007/10/01/analysis-the-nuclear-dimensions-of-jihadist-terrorism/index.html.
[30] Ackerman, G. and Jacome, M., "WMD Terrorism - The Once and Future Threat," *PRISM: A Journal of the Center for Complex Operations* Vol. 7 No. 3, May 2018, p. 29.
[31] Bunn, M. *et al.*, "Preventing Nuclear Terrorism – Continuous Improvement or Dangerous Decline?," Harvard Kennedy School, Belfer Center for Science and International Affairs, Cambridge, Massachusetts, March 2016, p. 17.
[32] Bunn, M. and Sagan, S., *Insider Threats*, Cornell University Press, 2017, p. 35.
[33] Rubin and Schreuer, "Belgium Fears Nuclear Plants Are Vulnerable."

Despite the fact that there is no publicly available evidence of a concrete effort on behalf of the IS to obtain a nuclear weapon,[34] the trafficking of RN material is more within the reach of a criminal or terrorist network than one might initially realise.[35] Advances in information technologies, coupled with the increasing availability of radioactive material, are making experts worrying about a potential increment of criminal and/or terrorist activities involving RN material.[36]

When it comes to the availability of the RN substances used for commercial or medical activities, the one still representing the bigger source of concern is probably Caesium-137 (Cs-137), as it is found in the form of powder and it is particularly easy to disperse in the environment.[37] Cobalt-60 (Co-60) and Iridium-192 (Ir-192) are immediate seconds because, as hard metals, they could be smuggled or dispersed in the form of pellets. The level of attractiveness of a given RN material is subjective, and depends on the value the criminal or terrorist group at issue assigns to it.[38]

The control of RN sources poses challenges both on national and international scales.[39] Flaws in the regulatory systems contribute to an increased risk perception when it comes to RN material. The legal architecture, as well as the cradle-to-grave control of the RN material, remains too weak to face modern threats.[40] There are still relevant weaknesses in the regulations on the safety and control of radioactive sources in some countries where RN smuggling activities originate.[41] In addition, because these substances are often transported across countries, it is difficult to keep track of their movement. This is why the transport of the RN material represents a critical step for a potential seizure. In 2018, for instance, 41% of the total incidents that saw the theft of radioactive material happened during transit.[42]

In order to make a balanced assessment of criminal and terrorist acts conducted with RN material, it might be useful to refer to the model proposed by Bunn *et al.*, which suggests to consider a given threat as the product of someone's intention and their capability, minus the efforts put by those who are countering their actions.[43]

What follows is an overview of the most relevant trends that are likely to characterise future malicious employment of RN agents.

---

[34] Bunn *et al.*, "Preventing Nuclear Terrorism," p. 18.
[35] VERTIC, "Illicit Trafficking of Nuclear and other Radioactive Material," p. 11.
[36] IAEA, "Combating Illicit Trafficking in Nuclear and other Radioactive Material," IAEA Nuclear Security Series No. 6, Vienna, Austria, 2007, p. 4.
[37] Bieniawski, A., "The Radiological Risk and Comparison with an Improvised Nuclear Device (IND)," Nuclear Threat Initiative (NTI)/Pool Re Conference, 6 April 2017.
[38] VERTIC, "Illicit Trafficking of Nuclear and other Radioactive Material," p. 12.
[39] Rossetti, P. *et al.*, "Dirty Bomb Drones, Physical-Logical Urban Protection Systems and Explosive/Radiological Materials regulation's challenges in the Age of Globalization," *Biomedicine & Prevention*, Vol. 3, 2017, p. 136.
[40] Bieniawski, A., Iliopulos, I. and Nalabandian, M., "Radiological Security Progress Report: Preventing Dirty Bombs – Fighting Weapons of Mass Destruction," Nuclear Threat Initiative (NTI), March 2016, https://media.nti.org/pdfs/NTI_Rad_Security_Report_final.pdf, pp. 9-10.
[41] VERTIC, "Illicit Trafficking of Nuclear and other Radioactive Material," p. 11; Bieniawski, Iliopulos and Nalabandian, "Radiological Security Progress Report", p. 11.
[42] CNS, "CNS Global Incidents and Trafficking Database," p. 5.
[43] Bunn *et al.*, "Preventing Nuclear Terrorism," p. 26.

Smuggling of RN material

There is a variety of actors interested in smuggling RN material. The range varies from traffickers who, besides smuggling the material, are also the end-users, and are therefore highly invested in such operation, to mere mules contracted for the only end of smuggling the material, but who are otherwise uninterested in the latter.[44]

Overall, the feasibility of a given RN substance to be smuggled depends on a series of factors, including the concerned actors' commitment to conducting the trafficking, the properties of the specific substance that is being smuggled, and the actors' willingness to smuggle the material in person rather than resorting to a clandestine courier.[45]

Depending on the type of perpetrators attempting to conduct a RN attack, their risk-aversion level might be very different. In some cases, the attackers might prioritise the success of the operation to their physical safety[46] (for example, suicide bombers represent the highest risk component in this scenario, since they may carry an RDD - see below - without any concern about their own safety). In this context, it might be worth keeping in mind the risk-assessment model that was previously mentioned, as it considers the actor's intention as a key element to make a realistic estimate of the probability of a RN event.

Despite the thorough work done by law enforcement agencies, the risk of RN illicit trafficking remains a potential threat to European security.[47] This is mainly due to the constant flow of these materials from conflict zones, which implies an increased availability, thus a continued threat of contraband. Other experts believe that lately we have actually witnessed a scarcity of available nuclear material, but nonetheless agree on the continued threat represented by attempted smuggling of RN substances.[48]

While nuclear material is generally stored in government-owned and secured facilities, radiological material can also be found in facilities belonging to the private sector, which are often characterised by insufficient security measures.[49] Not to mention medical, academic, and research facilities, which are even accessible to the public.

Numerous civilian storages hosting said substances are not protected with sufficient security measures.[50] Out of the 23 countries (7 of them are EU Member States) that committed to securing their most dangerous radiological sources during the 2014 Nuclear Security Summit (NSS), only 19 had, by March 2016, implemented a national strategy aimed at re-gaining

[44] VERTIC, "Illicit Trafficking of Nuclear and other Radioactive Material," p. 8.
[45] *Ivi*, pp. 13-14.
[46] *Ivi*, p. 12.
[47] Europol, "Crime group suspected of smuggling nuclear materials arrested in Vienna."
[48] Zaitseva, L. and Steinhäusler, F., "Nuclear Trafficking Issues in the Black Sea Region," *Non-Proliferation Papers* No. 39, April 2014.
[49] Bieniawski, Iliopulos and Nalabandian, "Radiological Security Progress Report," p. 10.
[50] Jiménez García, E., "Radiological and nuclear terrorism: definition, nature, scenarios and deterrence," Instituto Español de Estudios Estratégicos (IEEE), February 2019, http://www.ieee.es/Galerias/fichero/docs_opinion/2019/DIEEEO17_209EDGJIM-TerrorNuclear_ENG.pdf, p. 7.

control over their orphan sources and improve control over those that are considered as vulnerable.[51]

Ninety percent of international trade happens through maritime shipping.[52] Direct maritime routes represent a particularly attractive option for those attempting to smuggle radioactive material, especially because the existing difficulties in its detection make it possible to carry higher amounts of smuggled material.[53] The maritime supply chain therefore represents a crucially important factor for the identification of RN contraband.[54] Due to the presence of both land and maritime routes, the Black Sea region is particularly suitable for trafficking operations.[55] The majority of attempted RN smuggling operations occurring in this area are profit-motivated.[56] As previously mentioned, the latest reported attempt of illicit trafficking took place less than an year ago, with a criminal network trying to smuggle nuclear material.

According to authorities and experts, the most common routes for nuclear smuggling in that region is the one crossing the Ossetia region from North to South.[57] Materials destined to Turkey are taken across the Georgian region of Adjara, while those headed to Iran go through Armenia. Turkey is also one of the favoured area of destination for RN material smuggled from the former Soviet Union.[58] However, Turkish authorities have not acknowledge that such substances are directed to their country,[59] and it is therefore impossible to state with certainty their true destination.

When it comes to maritime routes, some of the most popular ones are from Odessa towards Turkey and the Middle East, and through Moldova.[60] Following an attempted case of HEU smuggling in the Moldovan capital of Chișinău, even local officials had to acknowledge their country's role in non-state actors' nuclear smuggling activities.[61]

---

[51] Bieniawski, Iliopulos and Nalabandian, "Radiological Security Progress Report," p. 6. The 23 signatory countries are the following: Algeria, Armenia, Australia, Canada, Czech Republic, Denmark, Georgia, Germany, Hungary, Italy, Japan, Kazakhstan, Lithuania, Morocco, Netherlands, New Zealand, Norway, Republic of Korea, Sweden, Turkey, United Arab Emirates, United Kingdom, United States.

[52] International Chamber of Shipping, "Shipping and World Trade," https://www.ics-shipping.org/shipping-facts/shipping-and-world-trade.

[53] Zaitseva and Steinhäusler, "Nuclear Trafficking Issues in the Black Sea Region."

[54] Downes, Hobbs, and Salisbury, "Combating nuclear smuggling?".

[55] Zaitseva and Steinhäusler, "Nuclear Trafficking Issues in the Black Sea Region."

[56] *Ibid.*

[57] *Ibid.*

Ossetia is a region located in the Northern Caucasus, at the border between Russia and Georgia. Administratively, Ossetia is divided in North Ossetia–Alania (North) and South Ossetia (South).

[58] *Ibid.*

[59] Turkish Ministry of Interior and Turkish National Police, Department of Anti-Smuggling and Organized Crime (KOM), "Turkish Report of anti-smuggling and organized crime 2011," March 2012, http://www.tadoc.gov.tr/Dosyalar/Raporlar/2011eng/index.html.

[60] Zaitseva and Steinhäusler, "Nuclear Trafficking Issues in the Black Sea Region."

[61] Moldovan representative, Presentation at the "International Conference on Illicit Trafficking Issues in the Black Sea Region," Chișinău, Moldova, November 2013.

Figure 1 Smuggling activities in Europe and the Black Sea region, 2013-2018, CNS Global Incidents and Trafficking Database [62]

The growing industrialisation of developing countries which might not yet have robust security measures in place, coupled with the globalisation process, might be influencing illicit RN smuggling activities. There is a need to adapt export controls to the growing industrialisation of countries involved in the transferring of dual-use radiological material.[63] Globalisation brought along the need to re-evaluate security strategies,[64] and the black market based on RN illicit trafficking makes no exception.

In order to counter the smuggling of RN material, the IAEA considers the "detection of the transfer of significant quantities of plutonium or enriched uranium" to be the primary objective of nuclear security measures.[65] Detecting trafficking involving uranium, plutonium or other alpha-particle radiation emitting isotopes, is particularly difficult due to the fact that these

[62] The data were retrieved from "The CNS Global Incidents and Trafficking Database" (Last Update 4 October 2019, https://www.nti.org/analysis/articles/cns-global-incidents-and-trafficking-database/).
The map considers episodes of theft and unauthorised possession of radioactive material occurred in Europe and the Black Sea region, between 2013 and 2018. In total, 68 case were reported among the following countries: Belarus, France, Georgia, Ireland, Moldova, Poland, Slovakia, Spain, The Netherlands, Turkey, United Kingdom, Ukraine.
[63] European Commission and European Union External Action, " EU efforts to strengthen nuclear security," Joint Staff Working Document - SWD(2016)98 final, 16th March 2016, https://ec.europa.eu/jrc/sites/jrcsh/files/eu-efforts-to-strengthen-nuclear-security_en.pdf, p. 40.
[64] IAEA, "Nuclear Proliferation and the Potential Threat of Nuclear Terrorism", November 2004, https://www.iaea.org/newscenter/statements/nuclear-proliferation-and-potential-threat-nuclear-terrorism.
[65] IAEA, "Combating Illicit Trafficking in Nuclear and other Radioactive Material," p. 6.

materials can be easily shielded.[66] However, the likelihood of cases of attempted smuggling of substances like Co-60 though scrap metal deliveries remains high.[67]

By one estimate, over 13.000 buildings in more than 100 countries worldwide are hosting quantities of radiological sources sufficient to pose a serious RN threat.[68] There is a need to build a comprehensive system able to find and recover stolen RN material. The system should include, to name a few, a legal architecture, intelligence services, and radiation detectors. Building a similar framework will prove a very complex task.[69]

a) Cyber-attack to nuclear installations

Nuclear facilities are more vulnerable to cyber-attacks today than they were in the past. Cyber-criminal operations are becoming easier to conduct, and the number of activities of this kind is increasing rapidly.[70]

Criminal or terrorist groups may attempt to conduct a cyber-attack against a nuclear facility to compromise the security of RN materials and the execution of operations, thus endangering the nuclear command and control system.[71] A successful cyber-attack to a nuclear installation could have consequences ranging from minor to potentially catastrophic. Examples include interruption of critical communications or access to information and imperilment of nuclear planning or delivery systems; but they might go as far as allowing an adversary to take control of a nuclear weapon.[72]

Nuclear facilities were not constructed at a time when cyber-attacks represented a serious threat. This makes them "insecure by design" when it comes to cybersecurity.[73] Unfortunately, it cannot be assumed that the more a system is technically complex, the more it is secure – rather, the opposite is true.[74] Sophisticated technical system normally entail some degree of automation and connectivity which, although granting more efficiency and cost-saving benefits,[75] inevitably lead to increased vulnerability to cyber-attacks.[76] A cyber-attack could be conducted, for instance, with the aim of causing the conditions to then lead a physical theft or

[66] Zaitseva and Steinhäusler, "Nuclear Trafficking Issues in the Black Sea Region."
[67] Laka, "Co60 source discovered in a scrap metal delivery."
[68] Bunn *et al.*, "Preventing Nuclear Terrorism," p. 98.
[69] Bunn, M., "Securing the Bomb 2010 – Securing All Nuclear Materials in Four Years," Nuclear Threat Initiative (NTI) , April 2010, https://media.nti.org/pdfs/Securing_The_Bomb_2010.pdf, p. 22.
[70] Baylon, C., Brunt, R. and Livingstone, D., "Cyber Security at Civil Nuclear Facilities - Understanding the Risks," Chatham House Report, Chatham House, London, United Kingdom, September 2015, p. 1.
[71] NTI, "Addressing Cyber-Nuclear Security Threats", Nuclear Threat Initiative, https://www.nti.org/about/projects/addressing-cyber-nuclear-security-threats/.
[72] Stoutland, P. and Pitts-Kiefer, S., "Nuclear weapons in the new cyber age. Report of cyber-nuclear weapons study group," Nuclear Threat Initiative (NTI), September 2018, https://media.nti.org/documents/Cyber_report_finalsmall.pdf, p. 9.
[73] *Ivi*, p. ix.
[74] Berghofer, J., "Apocalypse now? Cyber threats and nuclear weapons systems," European Leadership Network, May 2019, https://www.europeanleadershipnetwork.org/commentary/understanding-and-addressing-cyber-threats-to-nuclear-weapons-systems/.
[75] Baylon, Brunt and Livingstone, "Cyber Security at Civil Nuclear Facilities," p. 1.
[76] Berghofer, "Apocalypse now?".

sabotage of a nuclear facility. Moreover, it could be meant to get access to sensitive information (e.g. nuclear weapon design).[77]

Nuclear facilities can be subject to numerous types of cyber-attacks, ranging from data theft, to infiltration in the nuclear command, control and communication (NC3) system, to cyber espionage. Nuclear supply chains and NC3 systems represent potential targets for cyber-attacks.[78]

Conducting a cyber-attack against a nuclear power plant is neither as risky nor as expensive as physically attacking one.[79] But the main reason for nuclear facilities' vulnerability to cyber-attacks is an increased use of digital systems.[80] Digitalisation introduces a new degree of flexibility that allows criminals/terrorists to potentially hack a system by merely changing a programmable code. Firstly, it can potentially decrease the level or redundancy, which provided backup in case of system failure, through the addition of extra critical components or functions.[81] Secondly, the increased use of commercial off-the-shelf systems (e.g. Windows) took away the "obscurity" that characterised older plants, making it much easier for potential hackers to familiarise with a given system.[82] At the time most nuclear facilities were built (i.e. 1960s, '70s, and '80s), carrying out a cyber attack against them would not have been feasible, as they were built on hardwired system which could not be hacked unless a criminal/terrorist physically altered the circuit. Thirdly, the higher degree of connectivity within nuclear power plants resulted in the decline of "air gaps", which used to grant additional protection against cyber-attacks.[83] These "gaps" serve to physically isolate a computer or network from the Internet, making them inaccessible to those who do not personally work in the infrastructure.[84] Today, not only is it possible to break into these networks using a simple USB flash drive, but several nuclear facilities even have virtual private networks (VPNs) that can be breached by experts users.[85] Lastly, the increased use of digital systems for nuclear facilities also led to increased vulnerabilities in the supply chain. The nuclear supply chain consists in a series of different companies and providers, all located in different regions of the world and presenting different cybersecurity measures and regulations. A potential terrorist or criminal network interested in conducting a cyber-attack could hit just one element of the supply chain, perhaps taking advantage of comparably mild cybersecurity standards, then use this new vulnerability to affect the rest of the chain. A facility's components and equipment could potentially be compromised by an attacker at any stage, for instance during the phases of design and assembly.[86]

All of the aforementioned vulnerabilities make it possible, for some particularly skilled criminal or terrorist groups, to develop the capabilities needed for carrying out a cyber-attack on a

[77] Bunn *et al*., "Preventing Nuclear Terrorism," p. 20.
[78] Berghofer, "Apocalypse now?".
[79] Mortera-Martinez, C., "Game over? Europe's cyber problem," Centre for European Reform, July 2018, https://www.cer.eu/publications/archive/policy-brief/2018/game-over-europes-cyber-problem.
[80] Baylon, Brunt and Livingstone, "Cyber Security at Civil Nuclear Facilities," p. 9.
[81] *Ibid.*
[82] *Ibid.*
[83] *Ibid.*
[84] *Ivi*, p. 1.
[85] *Ibid.*
[86] Traynham Morrison and Walcroft, "Cyber security in the nuclear industry: Growing threats and evolving practices."

nuclear facility.[87] Some fear this could be the case of the IS, which has proved to be fairly capable when it comes to new technologies.[88] A criminal or terrorist group aiming to hit a nuclear facility might consider different targets, ranging from business networks, for the theft of confidential corporate data that could be used for financial gains, to reconnaissance systems, in order to obtain information that could then be used at a later time to conduct an attack.[89]

A cyber-attack against a nuclear facility could target its industrial control system, namely computers, field devices, and the human-machine interface (HMI). This is especially true for Supervisory Control And Data Acquisition (SCADA) systems.[90] Such an attack could cause loss of power thus taking the whole facility offline. What is more, several specialised search engines which show all SCADA systems connected to the internet exist.[91]

A cyber-attack could also occur by taking advantage of a nuclear facility that allows third-party remote access, as hackers could potentially exploit corporate business networks to gain access to a facility's industrial control system.[92] Similarly, if a facility lets its vendors to connect to it through a Virtual Private Network (VPN), the latter could potentially be hacked and used to introduce a malware into the industrial control network.[93] The same could happen if a facility has an undocumented connection to the internet which, for instance, might be set up by an employee.[94]

An additional potential vulnerability is represented by the necessity to constantly upload and download data. If members of staff use their own USB flash drive, for instance, they might risk introducing a malware into the system.[95]

Simultaneous attacks could also happen. This could be the case of a highly-organised criminal or terrorist group which manages to plan a cyber and a physical attack to a nuclear facility at the same time. Similarly, a group might be able to conduct multiple cyber attacks against different public infrastructures, including a nuclear power plant.[96]

Today, potential attackers are also advantaged by the increased availability of automated exploit toolkits.[97] This equipment allows the user to test a system for vulnerabilities by combining a computer programme with a payload – if put in the hands of a criminal or terrorist organisation, the latter could employ it to conduct a cyber-attack against the industrial control system of nuclear facility.

[87] Baylon, Brunt and Livingstone, "Cyber Security at Civil Nuclear Facilities," p. 5.
[88] *Ibid.*
[89] *Ivi*, p. 6.
[90] SCADA systems are systems of software and hardware elements that allow industrial organisations to monitor and control their equipment.
[91] Baylon, Brunt and Livingstone, "Cyber Security at Civil Nuclear Facilities," p. 8.
[92] *Ivi*, p. 10.
[93] *Ibid.*
[94] *Ivi*, pp. 10-11.
[95] *Ivi*, p. 12.
[96] *Ivi*, p. 6.
[97] *Ivi*, p. 8.

The risk of insider threat is just as real in the cyber sphere as it is in the physical realm.[98] Someone working inside a nuclear installation could, potentially, perpetrate a cyber-attack. The attackers at issue would not even need to have a particularly sophisticated understanding of hackers techniques since, as it was previously mentioned, something as easy as inserting a USB flash drive carrying a dangerous virus could be more than enough to cause a cyber-attack.

The consequences of a cyber-attack on a nuclear power plant could be as serious as the uncontrolled release of ionising radiation.[99] The effects of such an attack could be similar to those of the Fukushima Daiichi incident of 2011, when all the power lines of the nuclear reactors were destroyed, leading to their complete meltdown. What would have happened, for instance, if the "WannaCry"[100] virus of 2017 had hit informatic systems of nuclear infrastructures such as the UK Trident system?[101]

Overall, the amount of consideration and thoroughness dedicated to the physical security of nuclear facilities does not seem to be matched with a comparable level of cybersecurity.[102] Some may consider the risk of a cyber-attack to a nuclear facility as an unrealistic possibility.[103] In the past, there may have been cyber-attacks to nuclear facilities which, however, were never disclosed. This might have contributed to making such occurrences perceived as sporadic and improbable. A non-exhaustive collaboration within industries and a lack of intelligence-sharing makes it especially difficult for the nuclear industry to learn how to protect its cyber systems from cyber-attacks.[104]

An incorrect risk assessment may cause the implementation of inadequate security measures. The personnel working in a nuclear facility may not have a comprehensive understanding of cybersecurity procedures and, even when that is not the case, there might be communication problems. It is therefore necessary that the people who operate directly within these infrastructures are able not only to identify gaps in cybersecurity measures, but to report them to those appointed at enforcing standards and regulations. This could be done by ensuring all the staff working in a nuclear facility receives an appropriate cybersecurity training. Security culture plays a crucial role in the protection and well-functioning of all nuclear installations,[105] which should promptly include cybersecurity standards in their code of conduct.

---

[98] *Ivi*, p. 13.
[99] *Ivi*, p. 6.
[100] WannaCry is a ransomware virus that, in May 2017, infected numerous computers making their users' access impossible. For more information, see: Fruhlinger, J., "What is WannaCry ransomware, how does it infect, and who was responsible?," CSO online, 30th August 2018, https://www.csoonline.com/article/3227906/what-is-wannacry-ransomware-how-does-it-infect-and-who-was-responsible.html.
[101] The UK Trident system consists in the country's nuclear deterrent. The system includes four nuclear submarines carrying Trident II D-5 ballistic missiles.
[102] Baylon, Brunt and Livingstone, "Cyber Security at Civil Nuclear Facilities," p. 13.
[103] *Ivi*, p. viii.
[104] *Ibid*.
[105] IAEA, "Nuclear Security Recommendations on Radioactive Material and Associated Facilities," IAEA Nuclear Security Series No. 14, 2011, https://www.iaea.org/publications/8616/nuclear-security-recommendations-on-radioactive-material-and-associated-facilities, p. 12.

b) Attack or sabotage of nuclear facilities and other facilities containing RN material

The risk of a physical attack or sabotage of a nuclear installation or another type of facility hosting radioactive material is another type of RN event which seems to continue to worry experts of the RN community.

There are two main reasons why criminals or terrorists would attack a facility hosting RN material: either an attempt to steal the material, or physically damage the facility.[106] While, in the case of a civilian facility, the latter case would be limited to the dispersal of radioactive material into the environment, a physical attack to a nuclear installation might result in the meltdown of the nuclear reactor, provoking a release of ionising radiation.

There have been hints that extremist Islamic militants might be turning their attention to the nuclear industry.[107] Some well-known terrorist groups like Al Qaeda have publicly declared their intention to target nuclear power plants through sabotage operations.[108] The IS, too, has been reported to be actively trying to attack, infiltrate or sabotage nuclear facilities.[109] After the terrorist attacks that took place in Brussels in March 2016, Belgian media reported that the perpetrators originally considered attacking a nuclear installation.[110] Overall, there is a growing concern amongst experts that radicalised individuals might gain access to nuclear installations.[111]

A new threat that has only recently started to be taken in serious consideration is that posed by UASs, commonly known as drones.[112] There is more than one way these systems could be used to cause harm to nuclear installation. For instance, they could be packed with explosive material and be crushed against the facility, to physically damage it.[113] Drones could be also employed during a reconnaissance operation, through a flyover conducted to gather intelligence on a nuclear facility.[114] They could collect photos and video footage documenting, for instance, the site layout or the movement scheme of the facility's guards.

Besides new technological devices that could be used to attack a nuclear installation, potential attackers could still resort to simple trucks or other vehicles filled with explosive material, which they could drive inside the facility.[115] The risk of an insider threat in a nuclear facility has also

[106] Pomper and Tarini, "Nuclear terrorism," p. 4.
[107] De Clercq, G. and Steitz, C., "Militant interest in attacking nuclear sites stirs concern in Europe," Reuters, 10th October 2016, https://www.reuters.com/article/us-belgium-blast-nuclear/militant-interest-in-attacking-nuclear-sites-stirs-concern-in-europe-idUSKCN12A1PF.
[108] Joyner, C., "Countering Nuclear Terrorism: A Conventional Response," The European Journal of International Law Vol. 18, No. 2, 2007, p. 227.
[109] Rubin and Schreuer, "Belgium Fears Nuclear Plants Are Vulnerable."
[110] De Clercq and Steitz, "Militant interest in attacking nuclear sites stirs concern in Europe."
[111] *Ibid.*
[112] Pomper and Tarini, "Nuclear terrorism," p. 5.
[113] *Ibid.*
It is important to notice how, for a UAV to cause serious damage to a nuclear facility, it would need to be in the category of military drones and would have to be carrying the adequate explosive payload.
[114] Baylon, C., "Drones are an Increasing Security Issue for the Nuclear Industry", 18th December 2014, https://www.chathamhouse.org/expert/comment/drones-are-increasing-security-issue-nuclear-industry
[115] Pomper and Tarini, "Nuclear terrorism," p. 5.

been outlined as a worrisome possibility, but to result in a major safety-related incident it necessitates the knowledge of safety-sensitive areas.[116]

The security measures adopted by each nuclear installation are different, as there are no global standards. Surely enough, triggering an actual meltdown of a nuclear reactors would be very difficult, since there are normally at least four operators present in the control room at all times

c) RDDs, REDs and INDs

Although in recent years there have not been successful reported cases of this sort, criminal or terrorist groups who manage to obtain RN material could potentially manufacture a RN device, such as a Radiological Dispersal Device (RDD), a Radiological Exposure Device (RED) or an Improvised Nuclear Device (IND).

RDDs are the simplest and most primitive terrorist nuclear devices. They are made by combining conventional explosive (e.g. plastic explosive) and radioactive material (e.g. Ces-137). Numerous radioactive substances commonly used for civilian applications such as medicine, industry and agriculture could potentially be used to craft an RDD. However, for some of them, the quantity that would be needed to carry out a successful attack is simply not available on the civilian market.[117]

Regulatory (as well as physical) security varies depending on the country and, in some cases, even among institutions within the same country.[118] Some radiological materials are defined "orphan sources", namely substances which are not under regulatory control, e.g. because they have been abandoned, lost, misplaced, stolen or transferred without proper authorization.[119] These sources are particularly accessible for criminals and terrorists aiming to use them for building a dirty bomb.[120]

In 2005, the IAEA conference on nuclear security identified RDDs as a "major threat".[121] Desk research and perceptions of questionnaire respondents suggest that the risk of an RDD is not as likely as it was back then. Yet, some experts deem the risk of an attack conducted with an RDD is to be higher in Europe than it is in the US.[122] In particular, an analysis from the Washington Institute emphasises the peril of extremist jihadist groups successfully manufacturing such a weapon, and consider most European countries less prepared than the US to face such a threat.[123]

---

[116] Stoutland, P. (Nuclear Threat Initiative - NTI), in De Clercq and Steitz, "Militant interest in attacking nuclear sites stirs concern in Europe."
[117] IAEA, "Combating Illicit Trafficking in Nuclear and other Radioactive Material," p. 5.
[118] Pomper and Tarini, "Nuclear terrorism," p. 3.
[119] IAEA, "Code of Conduct on the Safety and Security of Radioactive Sources," Vienna, Austria, 2004, p. 3.
[120] IAEA, "Combating Illicit Trafficking in Nuclear and other Radioactive Material," p. 5.
[121] *Ibid.*
[122] Eisenstadt, M. and Mukhlis, O., "The Potential for Radiological Terrorism by al-Qaeda and the Islamic State," The Washington Institute, August 2016, https://www.washingtoninstitute.org/policy-analysis/view/the-potential-for-radiological-terrorism-by-al-qaeda-and-the-islamic-state.
[123] *Ibid.*

One reason why it is likely dirty bombs will continue to represent a threat in the forthcoming future consists in the introduction of UASs.[124] If placed in technically capable hands, a drone might become an RDD carrier. There is a variety of commercial drones that would be equipped to carry such a device.[125] During an interview conducted in 2017, Friedrich Grommes, Head for International Terrorism and Organized Crime in Germany's Federal Intelligence Service, expressed his concern about the possibility of terrorists using a commercial drone to drop a dirty bomb.[126]

Just four years ago, the IS threatened the United Kingdom claiming it was seriously intentioned to conduct a mass-casualty attack either through a chemical weapon or a dirty bomb, possibly employing a drone to carry out the attack.[127] In November 2016, a "drone factory" was discovered in Mosul (Northern Iraq).

Sophisticated and anti-Western terrorist networks like the IS are not the only type of actor who showed an interest in radiological terrorism. Despite it dates back to more than 10 years ago, an example that is worth to report, is the case of James Cummings. Cummings was a white supremacist who, angered by the election of President Obama in 2008, decided to plan an RDD attack during a presidential public event.[128] At the crime scene (i.e. Cummings' home in Belfast, Maine) the police found radiological material and literature on methods to construct a dirty bomb. Cummings collected the radioactive isotope thorium-232 (Th-232) and depleted uranium; he was able to buy the latter online, along with the material necessary to build a conventional explosive. This was a clear "alarm bell" that motivations for radiological terrorism may also from domestic extremisms in developed countries.

In July 2018, Greenpeace France carried out a demonstrative action aimed at exposing the vulnerabilities of nuclear power plants.[129] More specifically, the organisation wanted to raise awareness about the possible use of drones against these facilities on behalf of a malicious non-state actor. The organisation flew a Superman-shaped drone over the Bugey Nuclear Power Plant, located about 25 kilometers from the city of Lyon (France), then crashed it against the wall of the plant's spent fuel pool building. As it emerges from statements released by officials of the Électricité de France (EDF), the drone did not affect the safety of the installation.[130] The operation did, however, prove successful in its intent, as it was aimed at proving how these installations are "easily accessible and extremely exposed to outside attacks".[131]

---

[124] Rossetti *et al.*, "Dirty Bomb Drones, Physical-Logical Urban Protection Systems and Explosive/Radiological Materials regulation's challenges in the Age of Globalization," p. 136.
[125] *Ivi,* p. 137.
[126] Friedrich Grommes in Johnson, T., "ISIS may mount dirty bombs on drones," *Greenfield Recorder*, 8th September 2017, https://www.recorder.com/Something-else-to-fret-about-ISIS-mounting-dirty-bombs-on-drones-12382135.
[127] Gadher, D., "Isis plots drone chemical strike on UK," *The Sunday Times*, 4th December 2016, https://www.thetimes.co.uk/article/isis-plots-drone-chemical-strike-on-uk-9vwzm38s7.
[128] Cathcart, W. and Epstein, J. A., "White Supremacists Want a Dirty Bomb," *Foreign Policy*, 16th August 2019, https://foreignpolicy.com/2019/08/16/white-supremacists-want-a-nuclear-weapon/.
[129] Pradier P., "Greenpeace intentionally crashes drone into French nuclear power plant to reveal security vulnerability," ABC News, 3rd July 2018, https://abcnews.go.com/International/greenpeace-intentionally-crashes-drone-french-nuclear-power-plant/story?id=56343027.
[130] *Ibid.*
[131] *Ibid.*

The demonstration over Bugey Nuclear Power Plant was not the only event which saw the employment of drones in proximity of nuclear installations. Between October 5th and November 2nd, 2014, guards working in 13 different French nuclear plants spotted around 20 unaccounted drone overflights.[132] In the same year, a similar UAS was spotted flying over the Doel Nuclear Power Station.[133] For the time being, commercially available drones are not able to reach the reactor located in the core of a nuclear facility. This is why the likelihood of having criminals or terrorists causing a major radiological event by flying a drone against a nuclear installation is not very high.[134] On the other hand, drone do pose a serious threat as weapons carriers.[135]

Another example of radiological device is the RED. An RED is an object containing radioactive material which exposes potential victims to radiation. Because such device does not emit any noise, it could be hidden in a location (e.g. under a subway seat) where it can release radiation without being noticed.[136] The absence of sound or a blast makes REDs especially difficult to detect, and implies a lack of public reaction during its use.[137] While no terrorist act using REDs is documented, reported events show that such devices have been used in the past to carry out attempted targeted killings, where the victim is known to the perpetrator.[138] An example is represented by a Chinese nuclear researcher's unsuccessful attempt, in 2003, to murder a colleague with an RED made up with an industrial radiography camera containing pellets of Iridium-192 (Ir-192).[139]

One last device that may be crafted by a particularly technically capable non-state actor is the IND, defined by the IAEA as "a device incorporating radioactive materials designed to result in the formation of a nuclear-yield reaction".[140] Differently from an RDD or an RED, an IND is made with materials able to cause a nuclear explosion (i.e. uranium and plutonium). It is important to consider that it requires a minimum know-how and infrastructure to even build a crude gun-type nuclear device, whilst the probability to build a crude implosion nuclear device is extremely low. If a criminal or terrorist group intended to produce its own weapon-grade fissile material, it would only have two options: either enriching uranium or attempt the

[132] De la Baume, M., "Unidentified Drones Are Seen Above French Nuclear Plants," *The New York Times*, 3rd November 2014, https://www.nytimes.com/2014/11/04/world/europe/unidentified-drones-are-spotted-above-french-nuclear-plants.html.
[133] Pomper and Tarini, "Nuclear terrorism," p. 5.
[134] Jae, S. K., "A Study on the Possibility of Unmanned Aerial Vehicles (UAV)' Threat in Nuclear Facilities," Transactions of the Korean Nuclear Society Autumn Meeting, Goyang, Korea, 24-25 October 2019, https://www.kns.org/files/pre_paper/42/19A-202-%EA%B9%80%EC%9E%AC%EC%82%B0.pdf.
[135] Hersh, M., "Commentary: Drone Threat to Nuclear Plants," *Defense News*, 30 January 2015, https://www.defensenews.com/opinion/commentary/2015/01/30/commentary-drone-threat-to-nuclear-plants/.
[136] Colella, M. *et al.*, "An introduction to radiological terrorism," *The Australian Journal of Emergency Management*, Vol. 20 No. 2, May 2005, http://www.austlii.edu.au/au/journals/AUJlEmMgmt/2005/16.pdf, p.9.
[137] Gale, R. and Armitage, J., "Are We Prepared for Nuclear Terrorism?," *The New England Journal of Medicine*, Vol. 378, 29 March 2018, https://www.nejm.org/doi/full/10.1056/NEJMsr1714289, p. 1248.
[138] Bland, J., Potter, S., and Homann, S., "Radiological Exposure Devices (RED) - Technical Basis for Threat Profile," Sandia National Laboratories, June 2018, https://prod-ng.sandia.gov/techlib-noauth/access-control.cgi/2018/186003.pdf, p. 13.
[139] *Ibid.*
[140] IAEA, "Nuclear Security Series Glossary Version 1.3," November 2015, https://www-ns.iaea.org/downloads/security/nuclear-security-series-glossary-v1-3.pdf.

chemical separation of plutonium. Both techniques are extremely complex, let alone expensive and very difficult to accomplish without being detected.[141]

So far, there has never been a reported case of construction and use of either RDDs, REDs or INDs by criminals or terrorists in the EU in the last 10 years. More specifically, the recorded quantity of stolen nuclear material in the past few years is not enough to construct a crude nuclear device.[142] However, especially given the new threat represented by weapon carrier-drones, the risk represented by such RN devices should not be underestimated.

3.2 Threats assessment and perception[143]

People and organisations in the security realm, some of them directly or indirectly involved in the management of RN events, identify a set of critical issues they have encountered in such process.

The feeling that malevolent actors have acquired a renewed interest in RN material in the last few years is shared among many – yet, there seems to be a common agreement that these types of substances are still particularly difficult to acquire, when compared to other "conventional" means.

Depending on the party involved, there are different perceptions concerning the type of potential RN threats that might present themselves in the future. Some types of attacks are generally seen as more likely in present or future times than others. Attacks conducted with nuclear material, such as the detonation of an IND, are not considered realistic, possibly due to the well-known difficulty of acquisition of such substances in sufficient amount and weapon-grade quality. However, the mere smuggling of these materials, as well as other radiological (non-nuclear) agents, is still considered a practice that continues and will continue to occur in the future.

The majority of respondents found it impossible to assess whether RN attacks are more likely today than they were in the past. This might suggest an inherent difficulty in the identification of current trends in the RN threat. Differently, some of the experts proved ready to pinpoint some significant changes in RN events that occurred in recent times. For one thing, by resorting to some of the new technologies, perpetrators are able to conduct attacks with RN agents without personally having to handle them. This is, for instance, the case of cyber-attacks against nuclear facilities. Similar modes of actions allow the attackers to remain in a completely safe physical state for the entire duration of the attack. In addition, the diffusion of information concerning RN agents has allowed malicious non-state actors to acquire a higher level of know-how, therefore increasing the chances of having highly skilled people in the criminal or terrorist network at issue.

Besides factors strictly connected to the RN material itself, interviewees also pointed out how socio-economic changes and political instabilities characterising some geographical areas

[141] Ackerman and Jacome, "WMD Terrorism," p. 25.
[142] INCLUDING, Lithuanian Nuclear Security Centre of Excellence (NSCOE), "Evolution of RN threats."
[143] The statements of this sections are supported by the responses to the questionnaire that IAI distributed to a group of RN experts during the INCLUDING Workshop held on 27th January 2020.

have contributed to the evolution of the RN threat over time. With regard to future developments, the main factor that will determine a possible increase in RN events consists in technological development and criminals/terrorists' access to software and hardware they could possibly employ to conduct a RN attack.

4. RN UNCONVENTIONAL EVENTS MANAGEMENT

The section below is related to the RN training domain, which were produced with the contribution from the partners and from the findings collected through the dedicated questionnaire.

4.1 Strengths and weaknesses in training[144]

In brief…

- Each organisation, based on the responsibilities assigned and functions performed, has specific needs and requires its staff to gain different competences (a set of skills, attitudes and knowledge). Besides these specific training needs, all organisations should have trainings aimed at the basics in radiation protection and understanding how to protect the public from radiological hazard.

- A Systematic Approach to Training (SAT) is an optimal tool granting a gradual implementation of the tailored training programme, designed as a logical progression from the identification of the knowledge, skills and attitudes required to perform a job to the development and implementation of training to achieve these competencies, and subsequent evaluation of this training.

- A desire of more extensive use of technology in training has been expressed by interviewees, involving new equipment and modelling techniques that can help a more realistic simulation, with the ultimate aim of ensuring a comprehensive understanding of the risk posed by radioactive material.

- Simulations and field exercises should be included in the training programmes: they define gaps in legal framework, test effectiveness of the coordination and collaboration mechanisms, procedures, concept of operations as well as test a team's competences in a given phase of RN events, showing potential gaps in its skills and knowledge. In addition, they allow the workforce to operate in a close-to-real environment – something that proves quite useful, given the extraordinary circumstances that characterise a RN event.

- Basic knowledge of civil population protection and personal safety requirements in case of a RN emergency could be instilled in the wider public. This way, everyone could not only know how to practically behave to a RN event but would also know how to manage stress should such an occurrence present itself.

[144] *Ibid.*

- Further cooperation among authorities and RN professionals could grant a quicker and more efficient response to a RN attack. The inclusion of experts coming not only from the field of RN materials, but also public health allows a wider view over the issue.

For an organisation to meet its nuclear security responsibilities and be able to effectively contribute to an efficient nuclear security regime, it is essential to conduct a precise and comprehensive training educating its workforce about the risks posed by RN materials.[145] Through the tailored training, the personnel working in the field of RN emergencies can develop numerous capabilities, including developing practical and operational knowledge and skills, improving operational readiness, and clarifying roles and responsibilities within a given organisation.[146]

Each organisation has different needs and requires its staff to obtain a different set of skills and capabilities. A Systematic Approach to Training (SAT) is an optimal tool to develop and implement the training program that correspond specific needs of the organisation. Within its initial phase, SAT identifies the training needs that later will provide the basis for development of comprehensive and tailored training program for respective organization. Identifying the training needs, SAT employs analysis of different organizational documentations – job descriptions, lists of typical duties and activities performed, statistics, as well as past events records, compliance evaluation reports and other relevant information.[147]

Among the numerous objectives of RN-training courses, two are considered to be most significant by the large majority of respondents - understanding the basics in radiation protection, and understanding how to protect themselves and the public from radiological hazards, including contamination. It has also been highlighted that detection is crucial whenever dealing with a radiological hazard.

Besides trainings, practical exercises can prove a very useful element for the workforce's readiness to RN events.[148] Such activities test the effectiveness of the related response infrastructure as well as the team's competences in a given phase of RN events management, showing potential gaps in its skills and knowledge.[149] In addition, participation in the exercise allows the workforce to operate in a close-to-real environment – something that proves quite useful, given the extraordinary circumstances that a RN emergency scenario implies.

According to some respondents, thanks to applications allowed by new technologies RN training has been enhanced. A few respondents pointed out that the practical training with emphasis on utilisation of effective and advanced equipment and instrumentation significantly contribute to development of the competences that are necessary to respond to RN events. At the same time, it is important that the same equipment types and modifications that have been used for real operations are available for the training.

[145] INCLUDING, NSCOE, "Evolution of RN threats."
[146] *Ibid.*
[147] *Ibid.*
[148] *Ibid.*
[149] *Ibid.*

Furthermore, the inclusion of experts coming not only from the field of RN materials but also public health allowed a wider view over the issue.

There is, however, a lot of space for improvement. For one, basic knowledge of civil protection arrangements and personal safety requirements in case of RN emergency could be instilled in the wider public. This way, everyone could not only know how to practically behave in case of a RN event, but would also know how to manage stress should such an occurrence present itself. Then, further cooperation among authorities and RN professionals could grant a quicker and more efficient response to a RN attack.

The main concern among interested parties seems to be a possible significant improvement in the technological competencies of terrorists or criminals interested in conducting a RN attack. For this reason, stakeholders wish for meaningful advancements in the counter-action to technological and cyber-attacks. There is also a widespread hope that systematic and structured trainings for the prevention, preparation, response and recovery, including detection, of RN emergencies will continue and, possibly, will be enhanced by the introduction and efficient use of new equipment, and more realistic simulation scenarios will be employed.

4.2 CBRNe civil-military cooperation

Cooperation between the civil and military sector is very significant when it comes to operating in an environment affected by any kind of CBRN event. To this end, common training standards should be implemented.

NATO's role in the implementation of CBRNe civil-military cooperation is particularly relevant. In 2009, NATO adopted CBRN defence comprehensive approach which takes into consideration the political, military and civilian sectors encouraging through information exchange, planning, joint training and exercises.[150] At the basis of such concept lies the belief that the allies' civil preparedness to potential CBRN events might decrease the level of attractiveness of such agents, therefore reducing probability of malicious use on behalf of a violent non-state actor.

NATO Civil Emergency Planning Committee (CEPC) is appointed at supporting civilian authorities in the event of a CBRN emergency for which they might require assistance. Its role is precisely ensuring cooperation between the Alliance's military operations and national authorities.[151] Last year, NATO also published a series of non-binding guidelines for the enhanced civil-military cooperation in the management of potential large-scale CBRN incidents associated with terrorist attacks, which concentrate on six areas: planning, logistics, medical, public awareness and warning information systems, notifications and emergency communications, and training and exercises.[152]

[150] NATO, "NATO's Comprehensive, Strategic-Level Policy for Preventing the Proliferation of Weapons of Mass Destruction (WMD) and Defending against Chemical, Biological, Radiological and Nuclear (CBRN) Threats," 1st September 2009, https://www.nato.int/cps/en/natolive/official_texts_57218.htm.
[151] NATO," Civil Emergency Planning Committee (CEPC)," 15th November 2011, https://www.nato.int/cps/en/natohq/topics_50093.htm.
[152] NATO, "Non-binding guidelines for enhanced civil-military cooperation to deal with the consequences of large-scale CBRN events associated with terrorist attacks," 1st February 2019, https://www.securityresearch-cou.eu/sites/default/files/PO%282019%290054%20-

Several European countries have worked to establish measures and procedures for CBRNe civil-military cooperation. However, armed forces are usually involved for specific support only at a tactical level, and not in their full capabilities, creating additional obstacles due to the different tactical procedures followed by the military and the civil actors. To overcome such obstacles, a more active role of armed forces when dealing with a CBRN incident on civilian population should be part of a comprehensive approach in civil – military cooperation.[153]

Conclusions

While the likelihood of possible malicious use of RN substances seems to remain unvaried, some of the ways in which a potential RN attack might occur in the future are changing. For this reason, training should be tailored to current and future scenarios.

While the likelihood of possible malicious use of RN substances seems to remain unvaried, some of the ways in which a potential RN attack might occur in the future are changing to include new emerging scenarios, that should be included when conducting a risk assessment to identify the security functions, needed competences and the content of training needed to achieve them.

The illicit trafficking and smuggling of RN material continue to be serious sources of concern. Particularly worrying is the threat of contraband of RN agents through maritime shipping. With regard to the geographical distribution of smuggling activities, special attention should be placed on the Eastern European region. To counter the continued threat of illicit trafficking of RN material, the international community should consider adopting a set of common security standards, as well as enhancing the detection technologies that are currently in place.

Due to the widespread availability of new technologies and know-how, cyber-attacks represent a particularly threatening type of operation through which malicious actors might target a nuclear installation. Special attention shall be given to cyber-attacks and cybersecurity measures must be continuously enhanced. Such measures need to encompass both minor negligence such as the admission of guests' computers and USB flash drives inside nuclear facilities, and more substantial threats like the risk of malwares infecting a facility's informatic system.

An element posing a new threat consists in the possible employment of UASs to conduct RN attacks. More specifically, experts are showing concern about the risk of drones flying over nuclear facilities gathering sensitive information that might prove useful in the planning of a future attack, as well as drones being used as dirty bombs-carriers.

Looking forward, it is important to take the risk of insider threats into serious consideration. Facility operators should continuously address the insider threat by enhancing their physical protection measures with special emphasis on preventive and protective measures.

%20Non%20Binding%20Guidelines%20on%20Civil-Military%20Cooperation%20in%20CBRN%20Defence.pdf.

[153] INCLUDING, Hellenic Ministry of National Defence (HMOD), "RN threat situation / assessment in Europe from NATO point of view."

The perception of the RN community about the evolution of the RN threat and its likely future developments seems to mirror the available literature. A particularly valuable contribution offered by the interviewed parties consists in their take on the need for improvement of RN training. Advancements in technology could be exploited to this end, with the ultimate aim of ensuring all those involved in the response to a RN event have a comprehensive understanding of the risk posed by radioactive material, and are able to protect themselves and the wider public from its dangers in case of an accident.

To complement the findings of this Intermediate Note, further inputs specifically tailored to the content of the future Joint Actions will be elaborated over the Project's duration, and feed into the final Deliverable 3.*1 Report on Evolution of RN unconventional threat* (M56).

REFERENCES

- Ackerman, G. and Jacome, M., "WMD Terrorism - The Once and Future Threat," *PRISM: A Journal of the Center for Complex Operations* Vol. 7 No. 3, May 2018.
- Albright, D., Brannan, P. and Walrond, C., "Stuxnet Malware and Natanz: Update of ISIS December 22, 2010 Report," ISIS Report, 15th February 2011, p. 2 in Kesler B., "The Vulnerability of Nuclear Facilities to Cyber Attack," Strategic Insights. Volume 10, Issue 1, Spring 2011, http://large.stanford.edu/courses/2015/ph241/holloway1/docs/SI-v10-I1_Kesler.pdf.
- Amiard, J-C., "Nuclear Accidents: Prevention and Management of an Accidental Crisis," February 2020.
- Baylon, C., "Drones are an Increasing Security Issue for the Nuclear Industry", 18th December 2014, https://www.chathamhouse.org/expert/comment/drones-are-increasing-security-issue-nuclear-industry.
- Baylon, C., Brunt, R. and Livingstone, D., "Cyber Security at Civil Nuclear Facilities - Understanding the Risks," Chatham House Report, Chatham House, London, United Kingdom, September 2015.
- BBC News, "Alexander Litvinenko: Profile of murdered Russian spy," 21st January 2016, https://www.bbc.com/news/uk-19647226.
- Berghofer, J., "Apocalypse now? Cyber threats and nuclear weapons systems," European Leadership Network, May 2019, https://www.europeanleadershipnetwork.org/commentary/understanding-and-addressing-cyber-threats-to-nuclear-weapons-systems/.
- Bieniawski, A., "The Radiological Risk and Comparison with an Improvised Nuclear Device (IND)," Nuclear Threat Initiative (NTI)/Pool Re Conference, 6 April 2017.
- Bieniawski, A., Iliopulos, I. and Nalabandian, M., "Radiological Security Progress Report: Preventing Dirty Bombs – Fighting Weapons of Mass Destruction," Nuclear Threat Initiative (NTI), March 2016, https://media.nti.org/pdfs/NTI_Rad_Security_Report_final.pdf.
- Bland, J., Potter, S., and Homann, S., "Radiological Exposure Devices (RED) - Technical Basis for Threat Profile," Sandia National Laboratories, June 2018, https://prod-ng.sandia.gov/techlib-noauth/access-control.cgi/2018/186003.pdf.
- Bunn, M. and Sagan, S., *Insider Threats*, Cornell University Press, 2017.
- Bunn, M. *et al.*, "Preventing Nuclear Terrorism – Continuous Improvement or Dangerous Decline?," Harvard Kennedy School, Belfer Center for Science and International Affairs, Cambridge, Massachusetts, March 2016.
- Bunn, M., "Securing the Bomb 2010 – Securing All Nuclear Materials in Four Years," Nuclear Threat Initiative (NTI) , April 2010, https://media.nti.org/pdfs/Securing_The_Bomb_2010.pdf.
- Cathcart, W. and Epstein, J. A., "White Supremacists Want a Dirty Bomb," Foreign Policy, 16th August 2019, https://foreignpolicy.com/2019/08/16/white-supremacists-want-a-nuclear-weapon/.
- Colella, M. *et al.*, "An introduction to radiological terrorism," *The Australian Journal of Emergency Management*, Vol. 20 No. 2, May 2005, http://www.austlii.edu.au/au/journals/AUJlEmMgmt/2005/16.pdf.
- De Clercq, G. and Steitz, C., "Militant interest in attacking nuclear sites stirs concern in Europe," Reuters, 10th October 2016, https://www.reuters.com/article/us-belgium-

blast-nuclear/militant-interest-in-attacking-nuclear-sites-stirs-concern-in-europe-idUSKCN12A1PF.

- De la Baume, M., "Unidentified Drones Are Seen Above French Nuclear Plants," *The New York Times*, 3rd November 2014, https://www.nytimes.com/2014/11/04/world/europe/unidentified-drones-are-spotted-above-french-nuclear-plants.html.
- De Riccardis, S., "Imane: nessuna traccia di radioattività", La Repubblica, 21st March 2019, https://milano.repubblica.it/cronaca/2019/03/21/news/imane_fadil_ruby_ter_berlusconi_esami_radioattivita_-222159336/.
- Downes, R., Hobbs, C. and Salisbury, D., "Combating nuclear smuggling? Exploring drivers and challenges to detecting nuclear and radiological materials at maritime facilities," *The Nonproliferation Review* Vol. 26 No. 1-2, 2019.
- DutchNews.nl, "Scrap metal dealers arrested for passing on radioactive metal waste," 20th June 2018, https://www.dutchnews.nl/news/2018/06/scrap-metal-dealers-arrested-for-passing-on-radioactive-metal-waste/.
- Eisenstadt, M. and Mukhlis, O., "The Potential for Radiological Terrorism by al-Qaeda and the Islamic State," The Washington Institute, August 2016, https://www.washingtoninstitute.org/policy-analysis/view/the-potential-for-radiological-terrorism-by-al-qaeda-and-the-islamic-state.
- European Commission and European Union External Action, " EU efforts to strengthen nuclear security," Joint Staff Working Document - SWD(2016)98 final, 16th March 2016, https://ec.europa.eu/jrc/sites/jrcsh/files/eu-efforts-to-strengthen-nuclear-security_en.pdf.
- Europol, "Crime group suspected of smuggling nuclear materials arrested in Vienna," 6th December 2019, https://www.europol.europa.eu/newsroom/news/crime-group-suspected-of-smuggling-nuclear-materials-arrested-in-vienna.
- Friedrich Grommes in Johnson, T., "ISIS may mount dirty bombs on drones," *Greenfield Recorder*, 8th September 2017, https://www.recorder.com/Something-else-to-fret-about-ISIS-mounting-dirty-bombs-on-drones-12382135.
- Fruhlinger, J., "What is WannaCry ransomware, how does it infect, and who was responsible?," CSO online, 30th August 2018, https://www.csoonline.com/article/3227906/what-is-wannacry-ransomware-how-does-it-infect-and-who-was-responsible.html.
- Gadher, D., "Isis plots drone chemical strike on UK," *The Sunday Times*, 4th December 2016, https://www.thetimes.co.uk/article/isis-plots-drone-chemical-strike-on-uk-9vwzm38s7.
- Gale, R. and Armitage, J., "Are We Prepared for Nuclear Terrorism?," *The New England Journal of Medicine*, Vol. 378, 29 March 2018, https://www.nejm.org/doi/full/10.1056/NEJMsr1714289.
- GICNT's official website: https://gicnt.org.
- Hersh, M., "Commentary: Drone Threat to Nuclear Plants," Defense News, 30 January 2015, https://www.defensenews.com/opinion/commentary/2015/01/30/commentary-drone-threat-to-nuclear-plants/.
- IAEA, "Code of Conduct on the Safety and Security of Radioactive Sources," Vienna, Austria, 2004.
- IAEA, "Combating Illicit Trafficking in Nuclear and other Radioactive Material," IAEA Nuclear Security Series No. 6, Vienna, Austria, 2007.

- IAEA, “Convention on the Physical Protection of Nuclear Material,” Legal Series No. 12, Vienna, Austria, 1982, https://www-pub.iaea.org/MTCD/Publications/PDF/Pub615web.pdf.
- IAEA, “IAEA Safety Glossary. Terminology Used in Nuclear Safety and Radiation Protection”, 2018, https://www-pub.iaea.org/MTCD/Publications/PDF/PUB1830_web.pdf.
- IAEA, “Incident and Trafficking Database (ITDB),” https://www.iaea.org/resources/databases/itdb.
- IAEA, “Nuclear Proliferation and the Potential Threat of Nuclear Terrorism”, November 2004, https://www.iaea.org/newscenter/statements/nuclear-proliferation-and-potential-threat-nuclear-terrorism.
- IAEA, “Nuclear Security Recommendations on Radioactive Material and Associated Facilities,” IAEA Nuclear Security Series No. 14, 2011, https://www.iaea.org/publications/8616/nuclear-security-recommendations-on-radioactive-material-and-associated-facilities.
- IAEA, “Nuclear Security Series Glossary Version 1.3,” November 2015, https://www-ns.iaea.org/downloads/security/nuclear-security-series-glossary-v1-3.pdf.
- IAEA, “Prevention of the inadvertent movement and illicit trafficking of radioactive materials,” September 2002, https://www-pub.iaea.org/MTCD/Publications/PDF/te_1311_web.pdf.
- INCLUDING Grant Agreement, Part B, p. 2.
- INCLUDING, Hellenic Ministry of National Defence (HMOD), “RN threat situation / assessment in Europe from NATO point of view.”
- INCLUDING, Lithuanian Nuclear Security Centre of Excellence (NSCOE), “Evolution of RN threats.”
- International Chamber of Shipping, “Shipping and World Trade,” https://www.ics-shipping.org/shipping-facts/shipping-and-world-trade.
- Jae, S. K., “A Study on the Possibility of Unmanned Aerial Vehicles (UAV)’ Threat in Nuclear Facilities,” Transactions of the Korean Nuclear Society Autumn Meeting, Goyang, Korea, 24-25 October 2019, https://www.kns.org/files/pre_paper/42/19A-202-%EA%B9%80%EC%9E%AC%EC%82%B0.pdf.
- James Martin Center for Nonproliferation Studies (CNS), “CNS Global Incidents and Trafficking Database,” July 2019, https://media.nti.org/documents/global_incidents_trafficking_2018.pdf.
- Jiménez García, E., “Radiological and nuclear terrorism: definition, nature, scenarios and deterrence,” Instituto Español de Estudios Estratégicos (IEEE), February 2019, http://www.ieee.es/Galerias/fichero/docs_opinion/2019/DIEEEO17_209EDGJIM-TerrorNuclear_ENG.pdf.
- Joyner, C., “Countering Nuclear Terrorism: A Conventional Response,” The European Journal of International Law Vol. 18, No. 2, 2007, p. 225-251.
- Laka - Documentation and research centre on nuclear energy, “Co60 source discovered in a scrap metal delivery,” https://www.laka.org/docu/ines/event/1148.
- Laka - Documentation and research centre on nuclear energy, “Dangerous Co60 sources discovered in scrap metal containers,” https://www.laka.org/docu/ines/event/1147.
- Moldovan representative, Presentation at the “International Conference on Illicit Trafficking Issues in the Black Sea Region,” Chișinău, Moldova, November 2013.

- Mortera-Martinez, C., "Game over? Europe's cyber problem," Centre for European Reform, July 2018, https://www.cer.eu/publications/archive/policy-brief/2018/game-over-europes-cyber-problem.
- NATO, "NATO's Comprehensive, Strategic-Level Policy for Preventing the Proliferation of Weapons of Mass Destruction (WMD) and Defending against Chemical, Biological, Radiological and Nuclear (CBRN) Threats," 1st September 2009, https://www.nato.int/cps/en/natolive/official_texts_57218.htm.
- NATO, "Non-binding guidelines for enhanced civil-military cooperation to deal with the consequences of large-scale CBRN events associated with terrorist attacks," 1st February 2019, https://www.securityresearch-cou.eu/sites/default/files/PO%282019%290054%20-%20Non%20Binding%20Guidelines%20on%20Civil-Military%20Cooperation%20in%20CBRN%20Defence.pdf.
- NATO," Civil Emergency Planning Committee (CEPC)," 15th November 2011, https://www.nato.int/cps/en/natohq/topics_50093.htm.
- NTI, "Addressing Cyber-Nuclear Security Threats, Nuclear Threat Initiative, https://www.nti.org/about/projects/addressing-cyber-nuclear-security-threats/.
- Pomper, M. and Tarini, G., "Nuclear terrorism – Threat or not?," AIP Conference Proceedings 1898, November 2017, https://aip.scitation.org/doi/abs/10.1063/1.5009230.
- Pradier P., "Greenpeace intentionally crashes drone into French nuclear power plant to reveal security vulnerability," ABC News, 3rd July 2018, https://abcnews.go.com/International/greenpeace-intentionally-crashes-drone-french-nuclear-power-plant/story?id=56343027.
- RaiNews, "Anche l'Enea esclude la presenza di radioattività nel corpo di Imane Fadil. Iniziata l'autopsia," 26th March 2019, http://www.rainews.it/dl/rainews/articoli/Morte-Imane-Fadil-radioattivita-anche-Enea-esclude-autopsia-da337c8e-446f-41cc-9ef1-49b249352fc3.html.
- Rosenbach, E. and Chorev, M., "Belgium Highlights the Nuclear Terrorism Threat and Security Measures to Stop it," HuffPost, 29th March 2016, https://www.huffpost.com/entry/belgium-nuclear-terrorism_b_9559006?guccounter=1.
- Rossetti, P. *et al.*, "Dirty Bomb Drones, Physical-Logical Urban Protection Systems and Explosive/Radiological Materials regulation's challenges in the Age of Globalization," *Biomedicine & Prevention*, Vol. 3, 2017, pp. 136-139.
- Rubin, A. and Schreuer, M., "Belgium Fears Nuclear Plants Are Vulnerable," *The New York Times*, 25th March 2016, https://www.nytimes.com/2016/03/26/world/europe/belgium-fears-nuclear-plants-are-vulnerable.html.
- Rühle, M., "Analysis - The nuclear dimensions of jihadist terrorism," NATO Review, October 2017, https://www.nato.int/docu/review/articles/2007/10/01/analysis-the-nuclear-dimensions-of-jihadist-terrorism/index.html.
- Stoutland, P. and Pitts-Kiefer, S., "Nuclear weapons in the new cyber age. Report of cyber-nuclear weapons study group," Nuclear Threat Initiative (NTI), September 2018, https://media.nti.org/documents/Cyber_report_finalsmall.pdf.
- The Conversation, "How to protect nuclear plants from terrorists," 13th April 2016, https://theconversation.com/how-to-protect-nuclear-plants-from-terrorists-57094.

- The Economist, “The Litvinenko affair: Murder most opaque,” 13th December 2006, https://www.economist.com/taxonomy/term/29/0?page=859.
- Turkish Ministry of Interior and Turkish National Police, Department of Anti-Smuggling and Organized Crime (KOM), “Turkish Report of anti-smuggling and organized crime 2011,” March 2012, http://www.tadoc.gov.tr/Dosyalar/Raporlar/2011eng/index.html.
- UNODC, University Module Series, https://www.unodc.org/e4j/en/organized-crime/module-1/key-issues/similarities-and-differences.html.
- UN, “International Convention for the Suppression of Acts of Nuclear Terrorism,” 2005, https://treaties.un.org/doc/db/Terrorism/english-18-15.pdf.
- Van Dine, A., Assante, M. and Stoutland, P., “Outpacing cyber threats. Priorities for cybersecurity at nuclear facilities,” Nuclear Threat Initiative (NTI), 2016, https://media.nti.org/documents/nti_cyberthreats__final.pdf.
- VERTIC, “Illicit Trafficking of Nuclear and other Radioactive Material - The Legislative Response,” London, United Kingdom, April 2012, http://www.vertic.org/media/assets/Publications/ITR_WEB.pdf.
- Zaitseva, L. and Steinhäusler, F., “Nuclear Trafficking Issues in the Black Sea Region,” *Non-Proliferation Papers* No. 39, April 2014.

ANNEX I

[THIS PAGE INTENTIONALLY LEFT BLANK]