ProSPeReS

SCENARIOS COLLECTION WITH REACTIONS' MODELS

This project is funded by the European Union's Internal Security Fund – Police under Grant Agreement No. 101034230 – ProSPeReS
prosperes.eu

Ministerstwo Edukacji i Nauki

Minister of Education and Science of the Republic of Poland in frames the Program for co-financing international projects "PMW" for 2021-2023 under the contract no. 5184/ISFPolice/2021/2

D4.2 Scenarios collection with reactions' models

prosperes.eu

This project is funded by the European Union's Internal Security Fund – Police under Grant Agreement No. 101034230 – ProSPeReS

Document description

WP number and title	**WP4 - Preparedness for CBRN protection**
Lead Beneficiary	SGSP
Contributor(s)	HI, WSB, UL, ISEMI
Document type	Deliverable D4.2
Last Update	19/11/2023
Dissemination level	**Public** / Confidential *

** Confidential – only for members of the consortium & EC Services*

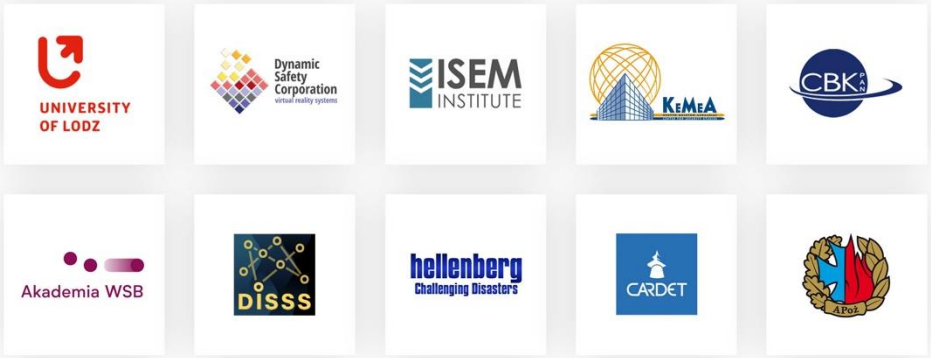
Acknowledgement:
This project is funded by the European Union's Internal Security Fund — Police. Grant Agreement No. 101034230 — ProSPeReS and the Polish Minister of Education and Science in frames the Program for co-financing international projects "PMW" for 2021-2023 under the contract no. 5184/ISFPolice/2021/2.

Table of Contents

Table of Figures

The ProSPeReS Consortium

Security experts, security research and academic institutions, providers of technical solutions and services



Law enforcement agencies (LEAs)

Faith-based organizations

1. Executive Summary

The **PRoSPeReS** project aims to support the implementation of the EU Action Plan to improve the protection of public spaces, in particular places of worship (PW). The project is also part of the "*Action Plan on the Protection of Places of Worship: united and in solidarity for safe and peaceful worship*" published in September 2019.

The **PRoSPeReS** project serves to raise the level of protection of religious places by synergising the scientific knowledge of academia and the empirical knowledge and experience of security specialists (practitioners), public service officers and representatives of religious institutions (representing the Catholic Church, the Orthodox Church and the Jewish community) in preparing a comprehensive protection system. This system includes measures to improve prevention, protection, minimisation and response to various types of terrorist threats and incidents that may occur at places of religious worship, including attacks using CBRN (chemical, biological, radiation and nuclear) agents. "Measures" should be understood here as sets of tools, procedures, equipment, guidelines for infrastructure improvement and protocols for cooperation with public services adapted to a specific type of threat (scenario).

The main objective of the **PRoSPeReS** project is to create an integrated security system that will improve the security of places of worship in EU member states. The project itself focuses on both prevention and response to terrorist threats that may occur at such sites.

This report "*D4.2 Scenarios of potential CBRN attacks with recommendations of responses*" is a collection of examples of potential scenarios which are dangerous and likely to happen at religious sites. For each scenario a model of reaction scheme has been prepared to be used as a guide for religious sites' staff.

2. Introduction

According to the European Commission Glossary, the term “CBRN" is an abbreviation from “chemical, biological, radiological, nuclear”. It represents four main threats that could harm the society through their deliberate release, dissemination or impact.

CBRN incidents could be conducted by state actors, non-state actors, organised crime groups or even by so-called “lone-wolfs”. CBRN incident against a place of worship (PW) in European region is considered as low probability but in today’s turbulent times we must prepare also in these.

Ongoing COVID-19 pandemic clearly shows that European society is not fully prepared for an all-hazards scenario with the need to strengthen its resilience. Naturally occurring pandemic also shows us how hard it would be to respond and contain deliberated release of biological agents.

CBRNE incidents are “low probability – high impact” incidents. Common features for these incidents have been that they have been unexpected and non-foreseeable, and thus the level of preparation preparedness and readiness for the response to meet the challenges of these incidents has been insufficient. However, communality of such incidents has also shown to be that many implications are unpredictable.

CBRN incidents have many specific features. One feature is the imperfect information; thus, for instance, first responders may need to make major decisions, commonly under the pressure of time and with imperfect information (Alexander – Klein 2009). Another feature is many CBRN incidents is the fear of something that is invisible, undetectable, ambiguous, and can pose long-term health risks – this can be very difficult for people to handle (see e.g. Carter et alia 2013, Liland 2015). Furthermore, also measures taken by the rescuers and health care personal – such as decontamination and quarantine - can be more stressful than the incident itself, if they are not managed appropriately (Carter et alia 2013).

During scenario building the range of plausible developments, their predicted impact on the people affected, and the related needs was identified. In order to be able to create plausible CBRN scenarios that will help the beneficiaries we have to take a broad look at the complex subject of CBRN threats and characteristics of soft targets.

Quite often in various (CBRN) scenarios the emphasize is in the technical details of dispersion etc. and the human factors are omitted. We tried to look at the whole cycle of the emergency starting from preparedness, weak signals etc. and further covering response and consequence management issues, concentrating in the human factors including the perpetrators and their motives.

An additional issue is the fact that the PWs (Places of worship) and the organisations and people involved are very multitude with different capabilities, various cultural and historical backgrounds. This means that the reaction models will be different as well

According to recent research[1], when considering potential threat of religious terrorism it is important to bear in mind the escalation of conflict in the Middle East and the migration crisis in Europe, it became clear that a central problem for the relevant government agencies was difficulty in understanding the behaviour, appearance, and inner-workings of religious groups in many countries. Security policy should preserve the balance between scrutiny of religious groups and adjustment of religious rules to accommodate interests of society, labour rights, and the economy. There are true extremists: the military involved in conflict, others prepared for action, and others demanding action. But there are also false extremists, such as religious fundamentalists who oppose secular rules, those who claim superiority of their identity, and missionaries who claim the superiority of their religious views in both sermons and politics.

[1] The National Academy of Sciences. The Convergence of Violent Extremism and Radiological Security, Proceedings of a Workshop—in Brief, March 2019, 2.

3. Historical Background in CBRN Incidents on Soft Targets

Hazardous substances have a long history of being used to poison individuals or groups. Already since the Middle Ages and Renaissance plant extracts were mostly used as chemical agents.

There have also been cases of biological warfare and one of the first recorded cases occurred in 1347, when Mongol forces are reported to have catapulted plague-infested bodies over the walls into the Black Sea port of Caffa (now Feodosiya, in the disputed Crimea), at that time a Genoese trade centre in the Crimean Peninsula. Similar methods were applied by advancing Russian forces under the command of the Ivan the IV "Terrible" in the Livonian war. Livonian War (1558–1583) was the Russian invasion of Old Livonia, and the prolonged series of military conflicts that followed, in which Tsar Ivan the Terrible of Russia (Muscovy). During the Great Northern War (1700–1721), many towns and areas around the Baltic Sea and East-Central Europe had a severe outbreak of the plague. The plague then followed trade, travel and army routes, reached the Baltic coast at Prussia in 1709, affected areas all around the Baltic Sea by 1711 and reached Hamburg by 1712. Therefore, the course of the war and the course of the plague mutually affected each other and was used even to advance the frontlines: while soldiers and refugees were often agents of the plague, the death toll in the military as well as the depopulation of towns and rural areas sometimes severely impacted the ability to resist enemy forces or to supply troops.[2]

The expansion of the chemical industry and breaking World War I to develop current understanding of dangerous chemical agents. It is said that chemical agents are the most brutal among the Weapons of Mass Destruction. Among thousands of different substances only few could be defined as a chemical weapon. Thus, substances should have high toxicity, be imperceptible to senses, rapid to action and persistent after dissemination. Chemicals that have such characteristics are listed as scheduled chemicals in the Chemical Weapons Convention. In present time, globalisation, easy access to raw materials and widely available technical information in the Internet causes that chemical related extremism and even terrorism is serious threat to security of societies.

Referring to Dr Audrey Kurth Cronin, American University, commercial processes of today´s World drive clusters of technologies such as small unmanned aerial vehicles (UAVs), additive manufacturing, smartphones, CRISPR technology, facial recognition technology, and simple robotics, available to everyone. To predict future scenarios, we must move beyond "dual use" to consider a more complex range of individual actors, including highly trained "insiders," professional consumers (prosumers), hobbyists, tinkerers, and amateurs— some of whom may have access to radiological material and nefarious purposes in mind.[3] Moreover, the terrorist threat posed by drones, including those carrying weapons of mass destruction, is not new. But in recent years, the community of drone hobby enthusiasts has become booming with online forums that openly discuss technology aspects. This unprecedented development enables potential terrorists to improve their technical skills, recruit appropriate engineering talent, find suitable equipment suppliers, and order the manufacture of airframes or hulls for drones and guidance components. The counter-terrorism response is complicated with unequal trade-offs of (a) personal freedom and technology progress for (b) security and predictability.[4] Following are a few examples of CBRN incidents affecting soft targets. We have selected different cases demonstrating the different harmful substances as well as the different types of perpetrators and targets.

[2] https://en.wikipedia.org/wiki/Great_Northern_War_plague_outbreak
[3] The National Academy of Sciences. The Convergence of Violent Extremism and Radiological Security, Proceedings of a Workshop—in Brief, March 2019, 4
[4] The National Academy of Sciences. The Convergence of Violent Extremism and Radiological Security, Proceedings of a Workshop—in Brief, March 2019, 4

3.1 Chemical

Tokyo subway attack of 1995

The incident was a coordinated multiple-point terrorist attack in Tokyo on March 20, 1995, in which the odourless, colourless, and highly toxic nerve gas sarin was released in the city's subway system. The attack resulted in the deaths of 12 (later increased to 13) people, and some 5,500 others were injured to varying degrees. Members of the Japan-based new religious movement AUM Shinrikyo (since 2000 called Aleph) were soon identified as the perpetrators of the attack.

The group, led by Shoko Asahara, had already carried out several assassinations and terrorist attacks using sarin, including the Matsumoto sarin attack nine months earlier. They had also produced several other nerve agents, including VX, and attempted to produce botulinum toxin and had perpetrated several failed acts of bioterrorism. Asahara had been made aware of a police raid scheduled for March 22 and had planned the Tokyo subway attack in order to hinder police investigations into the cult and perhaps spark the apocalypse they believed in.

On the morning of March 20, five men entered the Tokyo subway system, each with bags of sarin. Each boarded a separate subway line, their trains all headed toward the central Tokyo. At virtually the same time, each attacker dropped his bags of sarin on the floor of the train and punctured them before exiting the train and station and leaving the scene in a waiting getaway car. As the liquid in the bags started to vaporize, the fumes began affecting the passengers. The trains continued on toward the centre of the city, with sickened passengers leaving the cars at each station. The fumes were spread at each stop, either by emanating from the tainted cars themselves or through contact with liquid contaminating peoples' clothing and shoes. Many of the individuals who were overcome by exposure to sarin during the attack were those who came into contact with the agent while trying to assist those who already had been stricken. Among the victims were two subway employees who died attempting to dispose of punctured sarin bags at the Kasumigaseki Station.

Two days after the incident, police mounted a massive raid on the AUM offices in Tokyo and its laboratory headquarters at Kamikuishiki in Yamanashi prefecture, in the process seizing numerous canisters of toxic chemicals used to manufacture sarin. In May AUM leader Shoko Asahara and more than a dozen other cult leaders were arrested in nationwide raids.

Figure 1 - The toxin struck victims down in a matter of seconds, leaving them choking and vomiting, some blinded and paralysed

Source: Shutterstock: Aum Shinrikyo: Images from the 1995 Tokyo Sarin attack. 6.6.2018 Available from: https://www.bbc.com/news/in-pictures-43629706

Poisoning of Sergei and Yulia Skripal

There is no better way to understand Russian propaganda and disinformation than to 'peek behind the curtain' and see what goes on inside the apparatus conducting the operation “controllable information society” launched at the pro-Putin seminar nearby Moscow in October 2000. It is worth to look also the propaganda and disinformation themes following the murder of former Russian First Deputy Prime Minister Boris Nemtsov on February 27, 2015. Similar tactics were redeployed after the attempted assassinations of Sergei Skripal in 2018 and opposition leader Alexei Navalny in 2020. An internal document reveals the themes and information that trolls at the Internet Research Agency (IRA) were instructed to spread following the Nemtsov murder. It is titled 'Assignments for Savushkina 55. February 28-March 7, 2015,' a reference to the IRA's address in St. Petersburg. It was leaked to the St. Petersburg-based website MR7.ru reportedly by Ludmila Savchuk, an internet activist who had infiltrated the IRA, working there for two months. The IRA, financed by the Kremlin-linked oligarch Yevgeniy Prigozhin, specializes in usage of disinformation and propaganda against political systems and elections worldwide[5].

On 4 March 2018, Sergei Skripal, a former Russian military officer and double agent for the British intelligence agencies, and his daughter, Yulia Skripal, were poisoned in the city of Salisbury, England. According to UK sources and the Organisation for the Prohibition of Chemical Weapons (OPCW), they were poisoned by means of a Novichok nerve agent. Both Sergei and Yulia Skripal spent several weeks in hospital in critical condition, before being discharged. The British government accused Russia of attempted murder and announced a series of punitive measures against Russia, including the expulsion of diplomats. The UK's official assessment of the incident was supported by 28 other countries which responded similarly. Russia denied the accusations, expelled foreign diplomats in retaliation for the expulsion of its own diplomats, and accused Britain of the poisoning. In June 2018, a similar poisoning of two British nationals in Amesbury, involved the same nerve agent. British police believe this incident was not a targeted attack, but a result of the way the nerve agent was disposed of after the poisoning in Salisbury. In September 2018, British authorities identified two Russian nationals, as suspected of the Skripals' poisoning, and alleged that they were active officers in Russian military intelligence. Police are also investigated the death of 44-year old Dawn Sturgess, who came in contact with Novichok in the town of Amesbury, only 10 miles from Salisbury, earlier this month. Her partner, was also contaminated. Sturgess was exposed to at least 10 times the amount of Novichok the Skripals were exposed to. Authorities believe Sturgess and her partner were contaminated via a discarded perfume bottle the couple found in a park or in Salisbury’s city centre.[6]

[5] Spinning Nemtsov's Murder and Attempted Murders of Navalny and Skripal. United States Department of State. Global Engagement Center. 4 Oct, 2021. Available from: https://www.hsdl.org/c/abstract/?docid=870732

[6] Galindo, Gabriella. UK police identify suspects behind Skripal poisoning: report. Politico. 19.7.2018. Available from: https://www.politico.eu/article/sergei-skripal-russia-spy-poisoning-uk-police-identify-suspects-report/

Figure 2 - Members of the military, following the poisoning of Sergei Skripal and his daughter in April 2018

Source: Matt Cardy, Getty Images

3.2 Biological

Salmonella poisoning in Oregon, USA 1984

In the fall of 1984, hundreds of people in The Dalles In Oregon of followers of Rajneesh a Mystic in India. A group of prominent followers of Rajneesh led by Ma Anand Sheela had hoped to incapacitate the voting population of the city so that their own candidates would win the 1984 Wasco County elections. Fearing they would not gain enough votes, some Rajneeshpuram officials decided to incapacitate voters in The Dalles, the largest population centre in Wasco County. They deliberately contaminated salad bars at ten local restaurants with Salmonella across Wasco County.

The chosen biological agent was Salmonella enterica Typhimurium, which was first delivered through glasses of water to two County Commissioners and then, on a larger scale, at salad bars and in salad dressing. First came the stomachache problems and chills following vomiting spells and diarrhoea. Finally, for 45 of them, hospitalization. Though no one died, 751 people fell victim to what remains today the largest bioterror attack in American history, more severe than the anthrax attacks of the early aught. A CDC probe initially blamed the outbreak on improperly-trained food handlers, but a more exhaustive investigation soon revealed it was the work of the followers of cult leader Baghwan Shree Rajneesh (who called himself Osho). His charisma was so all-encompassing that he managed to amass tens of thousands followers across the world who swore by his freewheeling attitudes towards sex. Many of these acolytes were concentrated in the Oregon city of Antelope, renamed Rajneeshpuram after his followers had migrated there.[7]

[7] Sen, Mayukh. How a Cult Used Salad Bars to Orchestrate the Worst Bioterror Attack in US History. Vice. March 15, 2018. Available from: https://www.vice.com/en/article/kzp4n9/wild-wild-country-netflix-salad-bar-bioterror-attack

Figure 3 - Salmonella poisoning in Oregon, USA 1984

Source: Composite image; photos via Netflix and Flickr user Larry Hoffman

Ricin Plot Cologne Germany in 2018

Ricin is a by-product of castor beans (the seeds of the Ricinus plant) from which castor oil can be produced with uses in various industries and products Produced by processing castor beans, ricin is lethal in minute doses if swallowed, inhaled or injected and 6,000 times more potent than cyanide, with no known antidote. In 1978, ricin was used in the assassination of the Bulgarian dissident and journalist Georgi Markov in London, an agent for the Bulgarian secret police shot a ricin pellet into Markov's leg from a modified umbrella. Markov died several days later.

The main suspect, Sief Allah H., was born in Tunisia. Little is known about his path to alleged radicalization. While still living in Tunisia, he met a German woman on the internet. In October 2015, the pair married in Tunisia. Sief Allah H. legally entered Germany for the first time on November 2016, and moved into an apartment in Cologne-Chorweiler with his wife. At the time of their arrest, the couple had two children.
The first time Sief Allah H. was notified by German counterterrorism forces was in December 2017. Authorities suspected that Sief Allah H. had travelled to conflict zones and tried to replace passports that might contain stamps or entry visas which might indicate terrorist activities. German authorities also asked their Tunisian counterparts for information on him and were told that he was suspected of being a follower of Islamic ultra-conservative Salafi ideology.

The couple were caught after a tip-off from the US Central Intelligence Agency, which had noticed the large online purchase of castor seeds, according to German media reports. The couple had for a long time identified with the aims and values of the terrorist organisation Islamic State. They decided in 2017 to detonate an explosive in a large crowd. The pair had allegedly studied various forms of explosives before deciding on the deadly poison. They ordered 3,300 castor beans over the internet and successfully made a small amount of ricin. They also bought a hamster to test the potency of the poison.

Figure 4 - Ricin Plot Cologne Germany in 2018 (AP)

Source:

On June 12, 2018, heavily armed German special forces police with gas masks raided their apartment and Sief Allah H., was arrested. His wife, a German convert to Islam named Yasmin H., was also taken into police custody and was later accused of helping her husband in a terrorist plot. Sief Allah H. admitted to building the bomb, but denied that he had planned an attack on German soil.

Prosecutors accuse Sief Allah Hammami of planning an attack using the poison ricin, which he had manufactured at his home.

Hammami was arrested at his home, a nondescript high-rise building on Osloer Street in Köln-Chorweiler, on June 13. The subsequent search of the premises was conducted by police dressed in full protective gear and assisted by a specialist unit from the fire services and toxicological experts from the Robert Koch Institute, a German federal government agency responsible for disease control and prevention. Hammami had, it appeared, turned his home into a laboratory where he had manufactured ricin from around 1,000 castor oil beans. During the subsequent search of the flat, authorities found 84.3 milligrams of the highly poisonous substance, as well as 2,000 unused castor oil beans. Altogether, Hammami had successfully acquired 3,150 castor oil beans. The authorities also secured 250 metallic balls, fishing hooks, two bottles of acetone nail polish remover and 950 grams of what was described as a mix of aluminium powder and pyrotechnic material. While such an attack would constitute a new escalation in terms of the terrorism threat in Germany, there are echoes of similar plots elsewhere in Europe. With international operations becoming increasingly important for Islamic State (IS) as it contemplates its own decline, some fear that the group is planning a major headline-grabbing attack in the West, possibly one involving a biological or chemical agent.

While a ricin attack would constitute a new escalation in terms of the terrorism threat in Germany, similar plots have been detected in Europe. In mid-May, French authorities arrested an Egyptian–born student in Paris after intercepting messages on the secure messaging platform Telegram. According to French authorities, the student possessed “instructions on how to build ricin-based poisons”.

In January 2003, British authorities disrupted an alleged ricin plot led by the suspected al-Qaeda operative Kamel Bourgass. His plan, prosecutors said, was to produce a ricin-based paste that the plotters would smear in small quantities on surfaces in public places in the British capital—such as the doors of taxis, handrails on the London Underground system, and in buses. Bourgass was convicted of conspiracy to cause a public nuisance at a trial in 2005, and two others were convicted of possessing false passports, while the others accused in the plot were acquitted (BBC, April 13, 2005). In comparison to the suspected Cologne plot, the authorities confiscated "only" 22 castor oil beans, and while equipment and recipes needed to produce ricin were found, the alleged plotters had yet to weaponize the poison.

Compared to these, the suspected plot in Cologne appears to have reached a dangerously advanced stage. German State Prosecutor Frank warned that jihadists have for some time contemplated the use of biological weapons and have "in the last years distributed time and again different manuals for the manufacturing of these, including for the production of ricin from castor oil beans".

The arrests in France and Germany show the continued interest jihadists have to acquire and use biological and chemical weapons, but the BfV believes that IS has already manufactured ricin with traces of it secured in Iraq and the Iraqi-Syrian border. In Iraq, IS had access to laboratories at Mosul University and some of Saddam's chemical weapons engineers among its membership. There the group reportedly conducted deadly tests using thallium sulphate and a nicotine agent on human subjects.

Al-Qaeda has already experimented with producing poison from nicotine, largely because of its easy availability. The Egyptian-born bomb-maker and chemist Abu Khabab al-Masri developed a procedure for extracting nicotine poison from cigarettes in the late 1990s, as witnessed by former al-Qaeda member and later MI6 spy Aimen Dean. In 2004, a jihadist cell in the UK contemplated applying nicotine poison to the door handles of expensive cars. In addition, IS appears to have experimented with chlorine and sulphur mustard attacks in Syria and Iraq, becoming the first non-state actor to have developed a banned chemical warfare agent and combining it with a projectile delivery system, according to the London-based IHS Conflict Monitor. IS has encouraged the use of these unconventional weapons abroad. In a plot uncovered in 2017 in Australia, two Lebanese Australian brothers, Khaled and Mahmoud Khayat, were allegedly planning to build an "improvised chemical dispersion device" that would release highly toxic hydrogen sulphide. The plotters had allegedly received instruction from an IS controller in Syria, who had been put in touch with them by a third brother, Tarek, who was with the group. The Cologne plot shows some similarities with the one prevented in Australia. The German authorities allege that Hammami received instructions on how to prepare the ricin and construct the explosive device from two different individuals via social media.

Although happily prevented, the alleged Cologne ricin plot appears to alter and expand the spectrum of IS tactics in Europe. IS-directed attacks, such as those in Paris in 2015 and Brussels in 2016, have been conducted using firearms and explosives, while the spate of low-tech, IS-inspired attacks seen in Europe have involved knives and vehicles used as weapons. Often these have been carried out by lone actors, have required limited preparation and often resulted in only a small number of casualties. The suspected Cologne plotter seems to fall into a category of being initially IS-inspired, but then becoming a remotely guided attacker. Hammami's plot demonstrates a new level of ambition and complexity. It highlights the creativity of IS jihadists, their willingness to test a wide range of asymmetric possibilities, and the desire to achieve a much higher number of casualties with such attacks. Describing the alleged Cologne plot, BfV director Hans-Georg Maaßen warned Hammami could have "wounded, if not even killed, hundreds of people". At the same time, the Sydney, Cologne and Paris cases also underline the risk of biological and chemical weapons knowhow spreading in the jihadist milieu.[8]

[8] Jokinen, Christian. Foiled Ricin Plot Raises Specter of 'More Sophisticated' IS-inspired Attacks. Publication: Terrorism Monitor Volume: 16 Issue: 16. August 10, 2018. Available from. https://jamestown.org/program/foiled-ricin-plot-raises-specter-of-more-sophisticated-is-inspired-attacks/

Anthrax letters USA 2001

In 2001, soon after the terrorist attacks of 9/11 in September 2001, the intentional release of anthrax spores in the eastern United States increased concern about exposure to anthrax nationwide, and residents of Idaho sought assistance. Response from state and local agencies was required, increasing the strain on epidemiologists, laboratorians, and communications personnel. In late 2001, Idaho's public health communications system handled 133 calls about suspicious powders. For each call, a multiagency bridge call was established, and participants (public health officials, epidemiologists, police, Federal Bureau of Investigation personnel, hazardous materials officials, and others) determined which samples would be tested by the state public health laboratory. A triage system for calls helped relieve the burden on public safety and health systems.[9]

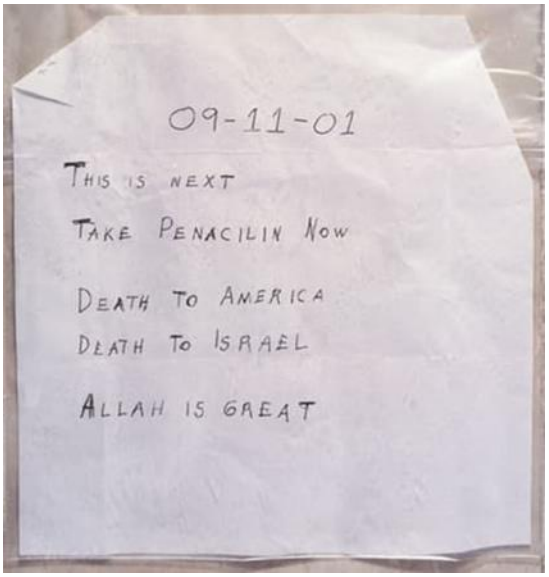
Figure 5 - Members of a hazardous materials response team help to remove a hazardous materials suit from an investigator who had emerged from the U.S. Post Office in West Trenton, N.J., on Oct. 25, 2001. The post office was closed after two letters containing anthrax were traced back to this facility.

Source: Tom Mihalek/AFP/Getty Images

These letters laced with anthrax began appearing in the U.S. mail. Five Americans were killed and 17 were sickened in the worst biological attacks in U.S. history. The first patient arrived at a Florida hospital in the early morning hours of October 2, 2001. The doctors thought the 62-year-old patient might be suffering from meningitis. But specialists suspected and Lab tests confirmed that the patient was suffering from inhalation anthrax, a bacterial disease primarily found in livestock and was considered as a potential agent of bioterrorism. Over the next two months, the first patient and four other people would die after inhaling anthrax, and 17 others would be infected, either by inhaling anthrax or getting it on their skin.

[9] Tengelsen, Leslie. Coordinated Response to Reports of Possible Anthrax Contamination, Idaho, 2001 Centers for Disease Control and Prevention (U.S.). October 2002. Available from: https://www.hsdl.org/c/abstract/?docid=3185

Figure 6 - The letter sent to NBC News anchor Tom Brokaw, which contained anthrax



Source: FBI/Getty Images

The lethal spores arrived via a series of letters mailed to locations in four states (Florida, New York, New Jersey and Connecticut) and Washington, D.C., spreading a new wave of panic after the terrorist attacks of 9/11 just a few weeks earlier. After anthrax was discovered at the first patient's workplace, American Media, and two more of his colleagues were found to have been exposed, state authorities in Florida initially tried to calm the public down by insisting there was no terror link. But as more information came out.it became clear that there had been some conscious, deliberate release of anthrax. The FBI launched an investigation, and by early November had found three of the letters containing anthrax spores, including ones sent to the offices of Senate Majority Leader Tom Daschle in Washington, D.C., and The New York Post and NBC in New York City. The authorities determined that the first group of anthrax-laced letters had been posted from a mailbox in New Jersey on September 18, 2011. A second bunch of letters had been mailed on October 9. In addition to anthrax powder, some of the letters also contained threatening notes using radical Islamic rhetoric, including such phrases as “Death to America. Death to Israel. Allah is Great.”

The perpetrator and his motives remain unclear although the Law enforcement authorities pointed at a scientist who had once worked in the U.S. Army’s Medical Research Institute of Infectious Diseases (USAMRIID) at Fort Detrick, Maryland, which kept stocks of anthrax. The suspected person, however, committed suicide in 2008.

Hoax letters

Anthrax hoaxes involving the use of white powder or labels to falsely suggest the use of anthrax had been reported also earlier but in the months following the 2001 anthrax attacks, hundreds of hoaxes were reported worldwide. It resulted in changes of legislation e.g. in the UK in October 2001 which stipulated that anyone convicted of a hoax involving threats of biological, chemical, nuclear or radioactive contamination would face a seven-year prison sentence.

Public safety is threatened when resources are diverted to investigating legitimate threats. The Anti-Hoax Terrorism Act of 2001 made it a felony to perpetrate a hoax related to biological, chemical and nuclear attacks. The Act stated the felony caused “If a hoax causes a hospital to be evacuated, people could die.

If a hoax causes a business to close, people could lose their jobs. And if a hoax occupies law enforcement officials, the public is denied protection from other crimes."[10]

Also in the US legislation making terrorism hoaxes a federal offence was passed as part of the Intelligence Reform and Terrorism Prevention Act of 2004.

An example of this type of hoax in a PW happened in November 2008, when white powder was mailed to temples of The Church of Jesus Christ of Latter-day Saints (Mormons) in Los Angeles and Salt Lake City, causing both to be closed temporarily while the mailings were investigated. Protests in previous days had targeted the Mormon church, which encouraged its members to fight the earlier passed amendment banning gay marriage in California.

A temple that was the site of a gay rights protest in Los Angeles was closed after receiving the envelope. The package was being inspected and powder spilled from an envelope onto a clerk's hand Tat the temple in downtown Salt Lake City. The room was decontaminated and the envelope taken by the FBI for testing. The clerk showed no signs of illness, but the scare shut down a building at Temple Square for more than an hour.

3.3 Radioactive

In addition to the infamous case of polonium poisoning of Alexander Litvinenko there are not many radioactive cases against soft targets. Therefore, we have selected an accidental release of radioactive material to a community because it clearly describes the characteristics of this type of incident also with malevolent endeavour.

Orphan Source, Goiana Brasil in 1987.

The cesium-137 radiation-dispersal disaster in 1987 occurred in Goiania, a city of one million residents in the centre of Brazil known for its cereal farms and cattle ranches. Relatively unknown to most people, this disaster has been carefully assessed and documented by the IAEA in a 150-page case study available online.[11] In 1985 a 50.9 TBq Cs-137 teletherapy source was left behind when a radiotherapy institute moved to new premises. In September 1987, two scavengers went into the unoccupied old clinic and found and removed the still encapsulated source. They later disassembled the source, compromising the encapsulation of the powdered radioactive material, and sold some of the pieces on to a scrap dealer. Over the next days the scrap dealers and several of their family members developed An Orphan Source left behind in Hospital at Goiania Brasil causing accidental release to local community symptoms of radiation poisoning, but did not connect this to the source. Only about two weeks after the source had first been compromised, one of the affected people suspected that the material from the hospital equipment was connected to the illness, and brought the source to a local doctor. The doctor suspected the material might be radioactive and managed to get in contact with radiological expertise.

[10] Anti-Hoax Terrorism Act of 2001, Hearing Before the Subcommittee on Crime of The Committee on the Judiciary, House of Representatives, One Hundred Seventh Congress, First Session on H.R. 3209, November 7, 2001; United States. Government Printing Office. Homeland Security Digital Library. Available from: https://www.hsdl.org/c/abstract/?docid=27546

[11] Cesium Radiation Goiania, Brazil Sept 13th 1987. HotNews. 20.2.2012. Available from: https://panji1102.wordpress.com/2012/02/20/cesium-radiation-goiania-brazil/

Figure 7 - Cesium Radiation Goiania, Brazil Sept 13th 1987

Source: HotNews. 20.2.2012

By the time the radioactivity had been identified and the government informed, radioactive powder from the source had already been spread over a large area including 85 buildings and 50 vehicles. Four people died as a result of radiation poisoning and 28 more received local radiation damage. 112 000 people sought medical attention, 600 were measured for contamination and 248 were actually contaminated.

Radioactive letters Slovakia 2016

Five letters containing radioactive material were sent to the courts, police and the Ministry of Justice of the Slovak Republic by a man from eastern Slovakia who is seeking revenge for a lost court.

Figure 8 - An investigator from the National Criminal Agency (NAKA) pressed charges on December 16 against a 53-year-old man from Poprad identified by the police only as Štefan K. regarding terrorism, certain forms of participation in terrorism and the illegal manufacturing and possession of nuclear and radioactive materials

Source: Man accused of sending radioactive packages faces life sentence, the Slovak Spectator. 22. Dec 2016. Available from: https://spectator.sme.sk/c/20416802/man-accused-of-sending-radioactive-packages-faces-life-sentence.

The letter delivered to the Justice Ministry contained trace contamination with Americium-241, with amounts of external radiation reaching three to four times the normal level, but still far below any dangerous intensity. The substance can be dangerous if inhaled or consumed, however. All the letters were sent from eastern Slovakia and they contained messages regarding the sender's general dissatisfaction, which was not directed against anyone in particular.[12]

[12] Spectator. Police investigate series of radioactive letters as terrorism. 28. Nov 2016. Available from: https://spectator.sme.sk/c/20395478/police-investigate-series-of-radioactive-letters-as-terrorism.html

4. Needs & GAP Analysis

The primary objectives of the **ProSPeReS**'s work package WP2 is to exchange good practice examples in current security systems and identify a common set of needs and gaps evident at various religious sites of worship that need to be addressed for enhancing the offered level of security EU-wide. In this regard, a vulnerability assessment based on exploiting the Vulnerability Assessment Tool (VAT) developed and maintained by DG HOME on selected religious sites was conducted. The results of the vulnerability assessment and needs analysis of religious sites are presented in:

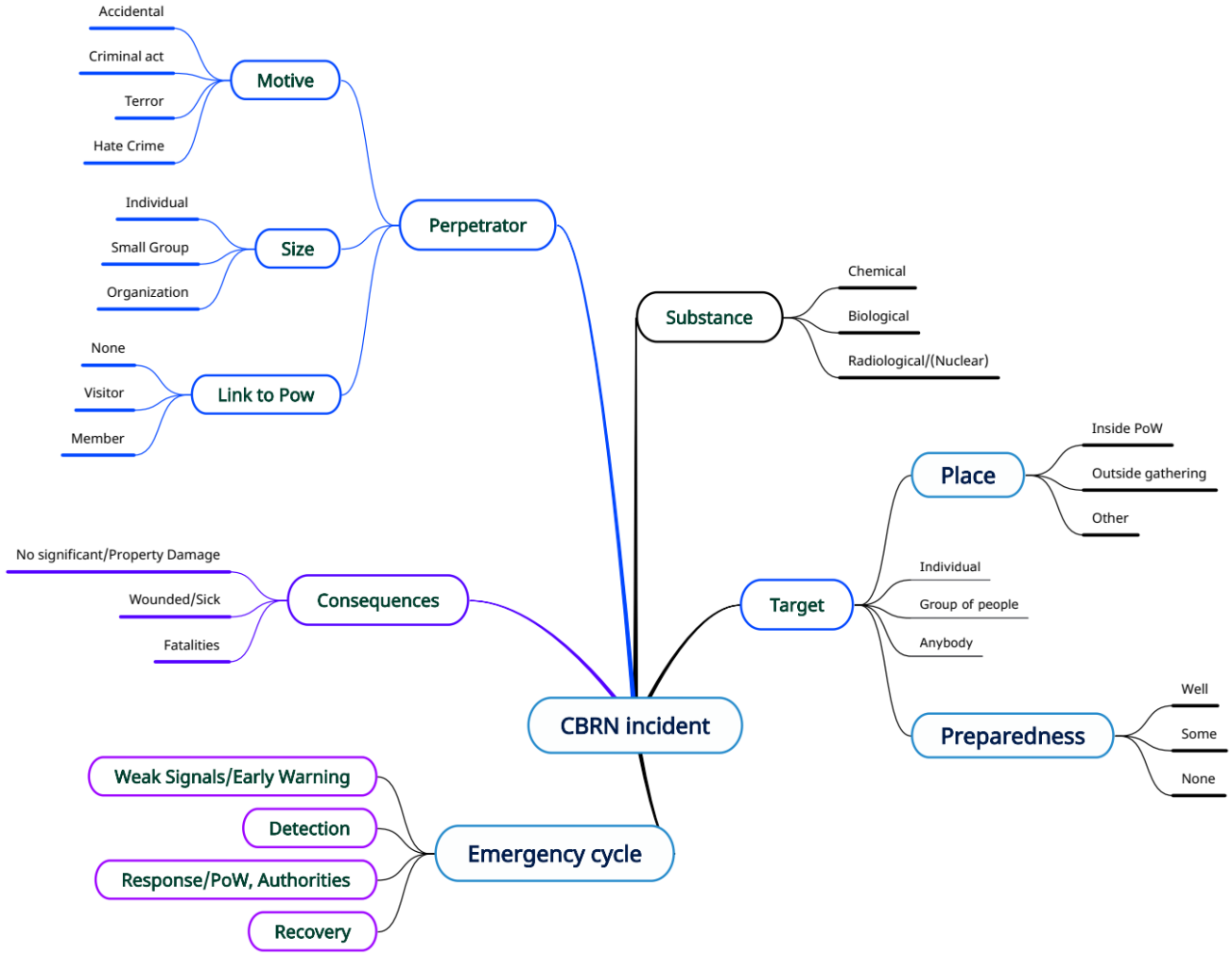
- "D2.1 Manual for vulnerability assessment",
- "D2.6 Report on Past Events / Best Practices / Gap Analysis / Needs assessment of Religious sites".

5. ProSPeReS Scenarios Description

Scenarios are an appropriate method for preparing for CBRNE incidents. Realistic scenarios play an instrumental role in identifying the needs for improvements, in particular, to understand the most cost-efficient ways to introduce these enhancements into the existing policy framework, structures and operations. Also, the necessity to develop and integrate new elements become more evident and their introductions more clearly justified.

The Figure 2 describes the different elements that may have some significance in building a CBRN scenario.

Figure 9 - Elements of CBRN scenario



5.1 Selecting the threats and building the scenarios

When looking at the full emergency cycle the scenarios should emphasize how the actions taken in different stages will affect the end result.

Therefore we need to look at:

- **Mitigation/Preparedness** of the target PW, as well as the local emergency authorities.
- **Weak Signals/Early warning**, depending on the perpetrator(s) and the motives there might be some advance information.
- The harmful **substance**, the behaviour and consequences are different.
- **Impact**, is it a static or dynamic incident.
- **Detection** is it obvious or are people getting symptoms by time.
- **Response** of the PW staff and contacts with the emergency authorities.

Identifying threats:

- On-the-ground assessments of capabilities and interests of extremists and disenfranchised scientists, engineers, and medical professionals to obtain access to radiation sources.
- Expansion and effective use of specialized databases that link location of inadequately controlled radiation sources with the presence of terrorist organizations.
- Examples of calls for closures of urban areas where radiation measurements have inexplicably risen to new levels, and resolution of real or perceived problems.
- Importance and cost of radiation monitoring of surface and subsurface water resources near waste sites for radiation-contaminated material and uncontrolled junk sites for scrap metal.

Improving responses to threats:

- Identifying successes and missed opportunities in providing local law enforcement personnel with radiation detectors, related equipment, and expert support for identifying inadequately controlled sources.
- Increasing technology-related expertise of journalists who cover radiation incidents.
- Increasing operational-tactical CBRN exercises (live and table-top) using external experts in designing the threat scenarios, evaluating the outcomes, and suggesting improvements.
- Improving understanding and capabilities of first responders who determine threat levels associated with radiological incidents, since they are key in reducing politicization before, during, and after incidents.

5.2 Describing the representative scenarios

Taking into account the approach described in section 5.1 a set of 7 representative scenarios – chemical (chem), biological (bio) and radiological (rad) – are presented. The low detail level of description is used regarding the fact, that more precise and complex one could be an unwanted guide for eventual attack.

Scenario 1 - Discharge of a hazardous chemical/biological substance from a drone (chem/bio)

Perpetrator
local gang with extreme opinions
Target

congregation members crowding outside building

Time

holiday day, during prayers

Motive

express frustration of the congregation

Weak signal

no week signals

Early warning

drone flying nearby crowd

Impact

drone fly above most dense crowd spreading hazardous material i.ex. concentrated hydrochloric acid

Detection

people below drone flight route feel falling droplets and burning sensation

Response

quick evacuation or invacuation, decontamination

First action

alert needed emergency services, conduct decontamination, ground the drone

Lesson learned

need of quick decontamination, anti-drone system.

Scenario 2 - Dirty bomb (rad)

Perpetrator

terrorist group

Target

main religion fraction during its important date

Time

main holidays

Motive

destabilization of society in particular region

Week signal

difficult situation between countries

Early warning

only known to intelligence agencies

Impact

detonation of bomb with radioactive material near main event

Detection

gathered people see and feel the blast, first responders detect increased level of radiation

Response

evacuation, decontamination, detection, first aid

First action

alter emergency services, conduct first aid,

Lesson learned

evacuation plans, decontamination site, crisis communication

Scenario 3 - Exposure (dousing/spraying/gas release) to a hazardous chemical substance (chem)

Perpetrator

individual conflicted with local religious leader

Target

local religious leader and people close to him

Time

in the vicinity of public appearance

Motive
revenge
Week signal
conflict with someone
Early warning
Person buying chemicals not needed before or in excessive amount
Impact
attacker spread substance on victim, corrosive and toxic effects are quickly seen
Detection
victims damage
Response
quick decontamination, sampling and detection
First action
detention of attacker, first aid
Lesson learned
protection of vip, safe room

Scenario 4 - Contaminated host / sprinkled/bottled/holy water (chem/rad/bio)

Perpetrator
domestic terrorist group
Target
religious VIP and followers
Time
mass event
Motive
destabilization of society
Week signal
unknown, unchecked people in organization of event
Early warning
no early warning
Impact
many people has direct contact with dangerous substance
Detection
lot of people has similar symptoms after contact with particular object
Response
triage, first aid, decontamination, sampling and detection
First action
triage
Lesson learned
check perpetrators and outsourced companies during mass event

Scenario 5 - Improvise explosive device in an abandoned car/package/basket/under a sidewalk slab

Perpetrator
mafia/organized crime group
Target
religious leader
Time
before or after public presence
Motive
to intimidate or eliminate chosen person

Week signal
conflict with some influential person or group
Early warning
suspicious package or vehicle, unauthorized construction sites
Impact
people see and feel the blast, heavily injured victims
Detection
no detection
Response
evacuation, triage, first aid
First action
evacuation
Lesson learned
need to check site for suspicious objects

Scenario 6 - Suspicious package of unknown origin (bio)

Perpetrator
frustrated individual
Target
religious leader
Time
not specified
Motive
to intimidate or injure chosen person
Weak signal
no weak signal
Early warning
suspicious, unexpected mails and packages
Impact
person who open mail/package is contaminated by dangerous material inside
Detection
material falling or spilling from inside package
Response
isolation of contaminated person, decontamination
First action
isolation, turn off ventilation
Lesson learned
protocol for suspicious package

Scenario 7 - Exposure to a high activity radioactive source (rad)

Perpetrator
terrorist group
Target
people gathered
Time
during mass event
Motive
injuring as much people as possible without warning
Week signal
no week signal
Early warning

suspicious packages

Impact

many people come in contact with high activity source

Detection

similar radiation sickness symptoms

Response

triage, evacuation, detection

First action

inform emergency services

Lesson learned

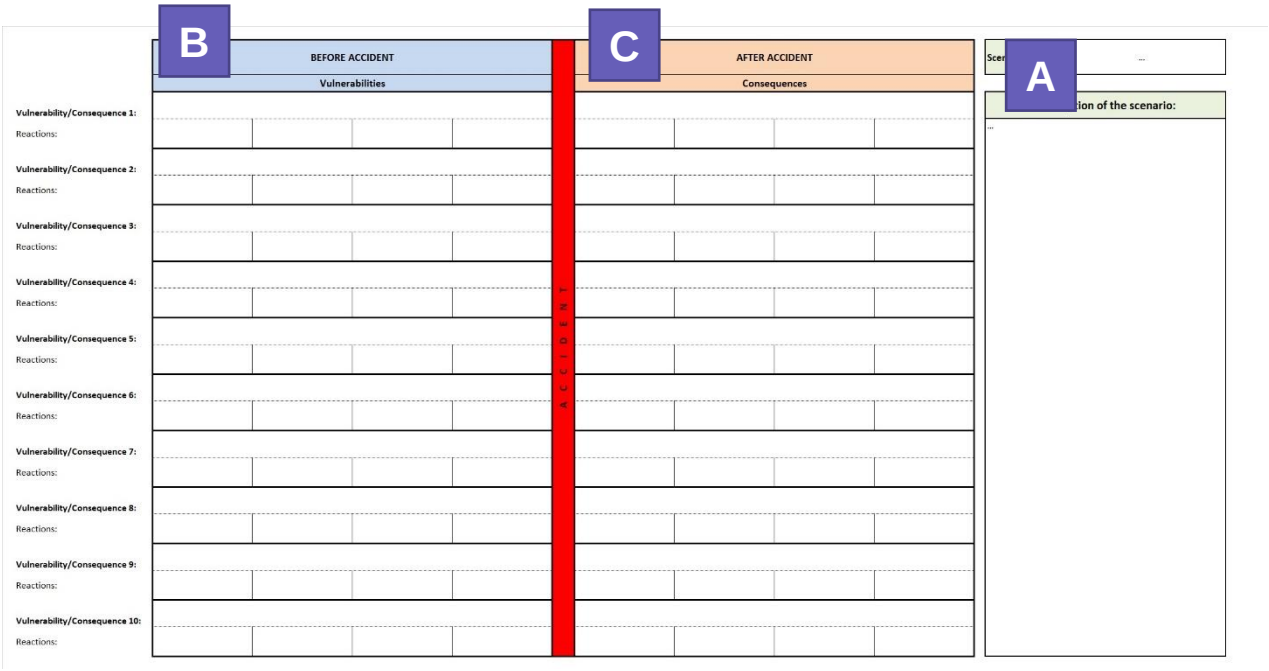
search for suspicious packages

6. Reaction Models

Increasing the awareness of religious sites' staff on CBRN accident could be implemented through the prepared certain reaction model. This kind of model may play a role of a specific guide for the response in an actual CBRN crisis situation. However, development of the holistic model for all stockholders of the accident is really difficult and is not an aim of the Prospers projects. That's why the model described in this section is focused on the possible reactions, which significantly may lower the impact of the accident, only staying within the competence of persons and/or institutions responsible for the security and safety of PW – owner/organizers of the gathering/event.

In order to unify the approach the Reaction Model Template (RMT) was developed using the MS Excel application (Figure 3) (Smolarkiewicz & Zwęgliński, 2023).

Figure 10 - The Reaction Model Template (RMT) – view of the empty template



As is showed on Figure 3, the RMT contains three sections:

- description of the CBRN scenario (A),
- a list of vulnerabilities which characterised a certain PW, which make the accident more probable and cause the PW more vulnerable for that type of the scenario (B),
- a list of consequences (impact) of the accident correspond to the scenario (C).

For each PW's vulnerabilities identified and listed in section B, as well as for each consequence listed in section C, up to 4 different "reaction activities" can be chosen respectively. It has to be emphasized that the entity implementing these activities is the owner of the PW or the entity responsible for its security. All these activities remain solely within the competence of this entity. The list excludes activities that are within the competence of, services, inspections or public administration.

A list of PW's vulnerabilities was created based on the results of analyses described in ProSPeReS's deliverables ("D2.1 Manual for vulnerability assessment", "D2.6 Report on Past Events / Best Practices / Gap Analysis / Needs assessment of Religious sites") and includes:

- Ventilation system inlet available for outsiders.
- Pedestrian routes available for car traffic.
- Litter bins unattended near escape routes.
- Lack of CBR agents detection devices.
- Lack of anti-drone procedures.
- No designated safe room.
- No place for carrying decontamination.
- Lack of crowd control devices.
- No CBR PPE equipment.
- No CBR materials management procedures.
- Difficult access to fire alert/extinguishing equipment.
- Lack of crisis communication.
- Electrical infrastructure has no back-up system.
- No trial evacuations conducted.
- Assembly points are unknown for personal.
- Existing vehicle barriers are not certified.
- No CCTV permanent supervision.
- Not sufficient light for CCTV.
- No CCTV coverage at the critical areas.
- Lack of knowledge in context of dangerous goods transport in near roads/railroads.
- Lack of knowledge in using extinguishing equipment.
- Limited security personnel.
- Low awareness of security personnel.
- Security personnel not familiar with existing procedures.
- No access for emergency services during mass event.
- No support from emergency agencies during mass event.
- No emergency response plans.
- No means of communication with emergency services.
- Not suitable evacuation routes.
- Lack of anti-panic measures.
- No active team making research for possible threats.
- any other (identified by the PW owner).

A list of accident's consequences (impact of the accident) PW's vulnerabilities was created based on the results of the PRACTICE project[13]. The overall aim of the project PRACTICE was to improve the ability to respond to and recover from a chemical, biological, radiological or nuclear incident. The objective of the project was to create an integrated European approach to a CBRN crisis – i.e. a European Integrated CBRN Response System. This was achieved through the development of an improved system of tools, methods and procedures that is going to provide EU with a capability to carry out a truly integrated and coordinated operational reaction following the occurrence of a CBRN crisis, whether it is caused by a terrorist act or an accident. Among other results, in frame of the PRACTICE project the CBRN scenario template was introduced (Endregard at al., 2011). In this template the impact of the accident (consequences of a certain scenario) was described by using the 3-tier impact model from the ASSRBCVUL project – "Assessment of the vulnerabilities of modern societies to terrorist acts employing radiological, biological or chemical agents with the view to assist in developing preventive and suppressive crisis management strategies" (Leeuw, 2007). This impact model was adopted to create a list of accident's consequences to describe certain PW CBRN scenario, which includes:

- 1st order challenges related to the direct effects of the accident, i.e. effects on the population, first responders, authorities, infrastructure and the environment that are directly caused by the attack, accident, or disease:
  - Directly affected population.
  - First responders.
  - Health services.
  - Command and control centres.
  - Site/building/infrastructure stakeholder(s).
  - Other authorities.
  - Media.
  - Infrastructure.
  - Environment.
  - Authorities in other countries.
  - International organisations.
- 2nd order challenges that indirectly cause problems or disruption for the population, the authorities and infrastructure:
  - Indirectly affected population.
  - Government.
  - Health services.
  - Police and law.
  - Food and water production and distribution.
  - Communication.
  - Transportation.
  - Energy supply.
  - Industry and commerce.

[13] European Union 7th Framework Programme, "Preparedness and Resilience Against CBRN Terrorism using Integrated Concepts and Equipment" (PRACTICE), https://practice-fp7-security.eu/

  - Leisure.
- 3rd order challenges, overarching societal, political and economic challenges indirectly caused by the accident:
  - Societal trust.
  - Shock resistance.
  - Political will endurance.
  - Economic health.
  - Rule stability.
- and any other (identified by the PW owner).

A list of reaction activities was created based on the results of analyses described in ProSPeReS's deliverables ("D3.2 Security by design guidebook for religious sites", "D3.3 A guidebook including recommendations of procedures, equipment and templates to prevent, protect, detect, respond and mitigate the result of the terrorist attack") and includes:

- Familiarize with incident managers guide. [→ WP3.3 – Set of procedures to prevent, protect, detect, respond and mitigate the result of terrorist attacks, p. 10-14]
- Familiarize with interoperability with emergency service guide. [→ WP3.3 – Set of procedures to prevent, protect, detect, respond and mitigate the result of terrorist attacks, p. 15]
- Develop a welcome team. [→ WP3.3 – Set of procedures to prevent, protect, detect, respond and mitigate the result of terrorist attacks, p. 16-17]
- Develop and implement Run/Hide/Tell protocol. [→ WP3.3 – Set of procedures to prevent, protect, detect, respond and mitigate the result of terrorist attacks, p.18]
- Develop and implement Recognize/Assess/React protocol for CBRN incident. [→ WP3.3 – Set of procedures to prevent, protect, detect, respond and mitigate the result of terrorist attacks, p.24]
- Full evacuation. [→ WP3.3 – Set of procedures to prevent, protect, detect, respond and mitigate the result of terrorist attacks, p. 24]
- Partial/phased/zonal evacuation. [→ WP3.3 – Set of procedures to prevent, protect, detect, respond and mitigate the result of terrorist attacks, p. 24]
- Directional evacuation. [→ WP3.3 – Set of procedures to prevent, protect, detect, respond and mitigate the result of terrorist attacks, p. 24]
- Invacuation. [→ WP3.3 – Set of procedures to prevent, protect, detect, respond and mitigate the result of terrorist attacks, p. 24]
- Full lockdown. [→ WP3.3 – Set of procedures to prevent, protect, detect, respond and mitigate the result of terrorist attacks, p. 24]
- Develop and implement Suspicious package/substance protocol. [→ WP3.3 – Set of procedures to prevent, protect, detect, respond and mitigate the result of terrorist attacks, p. 33]
- Develop and implement Bomb threat-hoax protocol. [→ WP3.3 – Set of procedures to prevent, protect, detect, respond and mitigate the result of terrorist attacks, p. 35]
- Develop and implement Suspicious item protocol. [→ WP3.3 – Set of procedures to prevent, protect, detect, respond and mitigate the result of terrorist attacks, p. 39]

- Develop and implement Venue search protocol. [→ WP3.3 – Set of procedures to prevent, protect, detect, respond and mitigate the result of terrorist attacks, p. 40]
- Familiarize with security by design guide. [→ WP3.2 - security by design guidebook for religious sites]
- Familiarize with equipment recommendation guide. [→ WP3.4. recommendations for equipment – monitoring, detection, and protection.]
- Evacuation guide. [→ WP3.3 – Set of procedures to prevent, protect, detect, respond and mitigate the result of terrorist attacks, p. 26 - 27]
- Invacuation guide. [→ WP3.3 – Set of procedures to prevent, protect, detect, respond and mitigate the result of terrorist attacks, p. 28 - 30]
- Lockdown guide. [→ WP3.3 – Set of procedures to prevent, protect, detect, respond and mitigate the result of terrorist attacks, p. 31 - 32]
- Mixed evacuation/invacuation procedure. [→ WP3.3 – Set of procedures to prevent, protect, detect, respond and mitigate the result of terrorist attacks]
- Buy needed detection tools. [→ A.3.2 Preparing the security by design guidebook for religious sites]
- Install required equipment/system. [→ A.3.2 Preparing the security by design guidebook for religious sites]
- Outsource security specialist. [→ A.3.2 Preparing the security by design guidebook for religious sites]
- Develop crisis communication channels. [→ WP3.3 – Set of procedures to prevent, protect, detect, respond and mitigate the result of terrorist attacks, p. 10-14, → https://www.bernsteincrisismanagement.com/the-10-steps-of-crisis-communications/]
- Prepare building and surroundings for large crowd. [→ A.3.2 Preparing the security by design guidebook for religious sites]
- Hire additional staff. [→ A.3.2 Preparing the security by design guidebook for religious sites]
- No action required. [→ WP3.3 – Set of procedures to prevent, protect, detect, respond and mitigate the result of terrorist attacks, p. 24]
- any other action (planned by the PW owner).

In sections 6.1 – 6.7 reaction models, created with use of the Reaction Model Template, for scenarios described in section 5 are presented. It is important to mention that Reaction Model Template can be used as a tool, however with some restrictions:

- The RMT is dedicated mainly to the administrators of PW with basic knowledge of CBRN (e.g. after reading the deliverable “D4.1 Introduction to CBRN”).
- The RMT takes into consideration the perspective of PW administrators (not the specialized agencies since they have their own procedures).
- RMT is recommended to be used for preparation purposes before religious gathering in his PW (or organized by his PW) for identifying vulnerabilities, bounding them through potential scenarios with required reactions (for preparation purposes e.g. running a training, reading or preparing a guideline; etc.).

- If not enough knowledge an external expert might use the RMT with PW staff support especially as it comes to the PW characteristics.
- The RMT is universal and might be used for different scenarios and reaction compilations (a set of 7 reference scenarios built up out of several blocks are proposed; a set of several vulnerabilities – results of WP2 and a set of reactions – results of WP3 are implemented in the tool and have been used for building the reference scenarios and reaction models).
- Reference scenarios with reactions are set up on relatively general level (due to the risk of potential classification), however on individual bases the user might define detailed scenarios referenced only to his PW specifics.

6.1 Reaction model for the scenario 1 : “Discharge of a hazardous chemical/biological substance from a drone (chem/bio)”

Figure 11 - Reaction model for the scenario “Discharge of a hazardous chemical/biological substance from a drone”

	BEFORE ACCIDENT					DURING and AFTER ACCIDENT			
	Vulnerabilities					Consequences			
Vulnerability/Consequence 1:	Lack of anti-drone procedures.					Tier 1: Directly affected population.			
Reactions:	Invacuation .	Prepare building and surroundings for large crowd.	Develop and implement Suspicious package/substance protocol.	Install required equipment/system.		Mixed evacuation/invacuation procedure.	Develop and implement Recognize/Assess/React protocol for CBRN incident.	Familiarize with incident managers guide.	Familiarize with interoperability with emergency service guide.
Vulnerability/Consequence 2:	Lack of crisis communication.					Tier 2: Indirectly affected population.			
Reactions:	Develop and implement Recognize/Assess/React protocol for CBRN incident.	Familiarize with incident managers guide.	Familiarize with interoperability with emergency service guide.	Develop crisis communication channels.		Develop crisis communication channels.			
Vulnerability/Consequence 3:	Lack of CBR agents detection devices.					Tier 2: Health services.			
Reactions:	Buy needed detection tools.					Develop crisis communication channels.			
Vulnerability/Consequence 4:	Lack of anti-panic measures.					Tier 3: Societal trust.			
Reactions:	Prepare building and surroundings for large crowd.	Evacuation guide.	Hire additional staff.	Develop a welcome team.		Develop crisis communication channels.			
Vulnerability/Consequence 5:	Low awareness of security personnel.								
Reactions:	Familiarize with incident managers guide.	Familiarize with interoperability with emergency service guide.	Outsource security specialist.						
Vulnerability/Consequence 6:	No support from emergency agencies during mass event.								
Reactions:	Familiarize with interoperability with emergency service guide.	Outsource security specialist.							
Vulnerability/Consequence 7:									
Reactions:									
Vulnerability/Consequence 8:									
Reactions:									
Vulnerability/Consequence 9:									
Reactions:									
Vulnerability/Consequence 10:									
Reactions:									

A C C I D E N T

Scenario name:	**Discharge of a hazardous chemical/biological substance from a drone**

Description of the scenario:

Preparator
Local gang with extreme opinions
Target
Congregation members crowding outside building
Time
Holiday day, during prayers
Motive
Express frustration of the congregation
Weak signal
No week signals
Early warning
Drone flying nearby crowd
Impact
Drone fly above most dense crowd spreading hazardous material i.ex. concentrated hydrochloric acid
Detection
People below drone flight route feel falling droplets and burning sensation
Response
quick evacuation or invacuation
decontamination
First action
Alert needed emergency services, conduct decontamination, ground the drone
Lesson learned
need of quick decontamination, antidrone system

6.2 Reaction model for the scenario 2 : “Dirty bomb (rad)”

Figure 12 - Reaction model for the scenario “Dirty bomb”

	BEFORE ACCIDENT					DURING and AFTER ACCIDENT			
	Vulnerabilities					Consequences			
Vulnerability/Consequence 1:	Litter bins unattended near escape routes.					Tier 1: Directly affected population.			
Reactions:	Familiarize with security by design guide.	Develop and implement Bomb threat-hoax protocol.	Develop and implement Suspicious item protocol.			Familiarize with incident managers guide.	Develop and implement Recognize/Assess/React protocol for CBRN incident.	Familiarize with interoperability with emergency service guide.	
Vulnerability/Consequence 2:	Lack of CBR agents detection devices.					Tier 1: Site/building/infrastructure stakeholder(s).			
Reactions:	Buy needed detection tools.					Full evacuation.	Develop and implement Bomb threat-hoax protocol.	Prepare building and surroundings for large crowd.	
Vulnerability/Consequence 3:	No CCTV permanent supervision.					Tier 2: Transportation.			
Reactions:	Develop and implement Venue search protocol.	Hire additional staff.				Develop crisis communication channels.			
Vulnerability/Consequence 4:	Limited security personnel.					Tier 2: Health services.			
Reactions:	Outsource security specialist.	Hire additional staff.	Develop a welcome team.			Develop crisis communication channels.			
Vulnerability/Consequence 5:	Low awareness of security personnel.					Tier 2: Police and law.			
Reactions:	Familiarize with incident managers guide.	Familiarize with interoperability with emergency service guide.	Outsource security specialist.			Develop crisis communication channels.			
Vulnerability/Consequence 6:	No place for carrying decontamination.					Tier 3: Societal trust.			
Reactions:	Prepare building and surroundings for large crowd.					Develop crisis communication channels.			
Vulnerability/Consequence 7:						Tier 3: Political will endurance.			
Reactions:									
Vulnerability/Consequence 8:									
Reactions:									
Vulnerability/Consequence 9:									
Reactions:									
Vulnerability/Consequence 10:									
Reactions:									

ACCIDENT

Scenario name:	**Dirty bomb**

Description of the scenario:

Preparator
Terrorist group
Target
Main religion fraction during its important date
Time
Main holidays
Motive
Destabilization of society in particular region
Week signal
Difficult situation between countries
Early warning
Only known to intelligence agencies
Impact
Detonation of bomb with radioactive material near main event
Detection
Gathered people see and feel the blast, first responders detect increased level of radiation
Response
Evacuation, decontamination, detection, first aid
First action
alter emergency services, conduct first aid,
Lesson learned
evacuation plans, decontamination site, crisis communication

6.3 Reaction model for the scenario 3 : “Exposure (dousing/spraying/gas release) to a hazard. chemical substance (chem)”

Figure 13 - Reaction model for the scenario “Exposure (dousing/spraying/gas release) to a hazardous chemical substance”

	BEFORE ACCIDENT					DURING and AFTER ACCIDENT			
	Vulnerabilities					Consequences			
Vulnerability/Consequence 1:	No place for carrying decontamination.					Tier 1: Directly affected population.			
Reactions:	Prepare building and surroundings for large crowd.					Familiarize with incident managers guide.	Develop and implement Recognize/Assess/React protocol for CBRN incident.	Familiarize with interoperability with emergency service guide.	
Vulnerability/Consequence 2:	No CBR PPE equipment.					Tier 1: Site/building/infrastructure stakeholder(s).			
Reactions:	Buy needed detection tools.					Partial/phased/zonal evacuation.	Prepare building and surroundings for large crowd.		
Vulnerability/Consequence 3:	No CCTV permanent supervision.								
Reactions:	Develop and implement Venue search protocol.	Hire additional staff.							
Vulnerability/Consequence 4:	Limited security personnel.								
Reactions:	Outsource security specialist.	Hire additional staff.	Develop a welcome team.						
Vulnerability/Consequence 5:	Low awareness of security personnel.								
Reactions:	Familiarize with incident managers guide.	Familiarize with interoperability with emergency service guide.	Outsource security specialist.	Develop and implement Suspicious package/substance protocol.					
Vulnerability/Consequence 6:									
Reactions:									
Vulnerability/Consequence 7:									
Reactions:									
Vulnerability/Consequence 8:									
Reactions:									
Vulnerability/Consequence 9:									
Reactions:									
Vulnerability/Consequence 10:									
Reactions:									

A C C I D E N T

Scenario name:	**Exposure (dousing/spraying/gas release) to a hazardous chemical substance**

Description of the scenario:

Preparator
Individual conflicted with local religious leader
Target
local religious leader and people close to him
Time
In the vicinity of public appearance
Motive
revenge
Week signal
conflict with someone
Early warning
Person buying chemicals not needed before or in excessive amount
Impact
attacker spread substance on victim, corrosive and toxic effects are quickly seen
Detection
victims damage
Response
quick decontamination, sampling and detection
First action
detention of attacker, first aid
Lesson learned
protection of vip, safe room

6.4 Reaction model for the scenario 4 : “Contaminated host/sprinkled/bottled/holy water (chem/rad/bio)”

Figure 14 - Reaction model for the scenario “Contaminated host/sprinkled/bottled/holy water”

	BEFORE ACCIDENT					DURING and AFTER ACCIDENT			
	Vulnerabilities					Consequences			
Vulnerability/Consequence 1:	Lack of CBR agents detection devices.					Tier 1: Directly affected population.			
Reactions:	Buy needed detection tools.					Familiarize with incident managers guide.	Familiarize with interoperability with emergency service guide.	Develop and implement Recognize/Assess/React protocol for CBRN incident.	Partial/phased/zonal evacuation.
Vulnerability/Consequence 2:	No CCTV permanent supervision.					Tier 2: Indirectly affected population.			
Reactions:	Hire additional staff.	Develop and implement Suspicious package/substance protocol.	Install required equipment/system.	Develop a welcome team.		Develop crisis communication channels.			
Vulnerability/Consequence 3:	Low awareness of security personnel.					Tier 2: Health services.			
Reactions:	Familiarize with incident managers guide.	Familiarize with interoperability with emergency service guide.	Outsource security specialist.			Develop crisis communication channels.			
Vulnerability/Consequence 4:	Security personnel not familiar with existing procedures.								
Reactions:	Familiarize with incident managers guide.	Familiarize with interoperability with emergency service guide.							
Vulnerability/Consequence 5:	Limited security personnel.								
Reactions:	Hire additional staff.	Install required equipment/system.							
Vulnerability/Consequence 6:									
Reactions:									
Vulnerability/Consequence 7:									
Reactions:									
Vulnerability/Consequence 8:									
Reactions:									
Vulnerability/Consequence 9:									
Reactions:									
Vulnerability/Consequence 10:									
Reactions:									

A C C I D E N T

Scenario name:	**Contaminated host / sprinkled/bottled/holy water**

Description of the scenario:

Preparator
Domestic terrorist group
Target
Religious vip and followers
Time
Mass event
Motive
Destabilization of society
Week signal
Unknown, unchecked people in organization of event
Early warning
No early warning
Impact
Many people has direct contact with dangerous substance
Detection
Lot of people has similar symptoms after contact with particular object
Response
triage, first aid, decontamination, sampling and detection
First action
triage
Lesson learned
check preparators and outsourced companies during mass event

6.5 Reaction model for the scenario 5 : “Improvise explosive device in an abandoned car/package/basket/under a slab”

Figure 15 - Reaction model for the scenario “Improvise explosive device in an abandoned car/package/basket/under a slab”

	BEFORE ACCIDENT					DURING and AFTER ACCIDENT			
	Vulnerabilities					Consequences			
Vulnerability/Consequence 1:	Litter bins unattended near escape routes.					Tier 1: Directly affected population.			
Reactions:	Familiarize with security by design guide.	Develop and implement Bomb threat-hoax protocol.	Develop and implement Suspicious item protocol.			Familiarize with incident managers guide.	Develop and implement Recognize/Assess/React protocol for CBRN incident.	Familiarize with interoperability with emergency service guide.	
Vulnerability/Consequence 2:	Lack of knowledge in context of dangerous goods transport in near roads/railroads.					Tier 1: Site/building/infrastructure stakeholder(s).			
Reactions:	Develop and implement Bomb threat-hoax protocol.	Familiarize with incident managers guide.	Familiarize with security by design guide.			Full evacuation.	Develop and implement Bomb threat-hoax protocol.	Prepare building and surroundings for large crowd.	
Vulnerability/Consequence 3:	No CCTV permanent supervision.					Tier 2: Health services.			
Reactions:	Develop and implement Venue search protocol.	Hire additional staff.				Develop crisis communication channels.			
Vulnerability/Consequence 4:	Limited security personnel.					Tier 2: Police and law.			
Reactions:	Outsource security specialist.	Hire additional staff.	Develop a welcome team.			Develop crisis communication channels.			
Vulnerability/Consequence 5:	Low awareness of security personnel.					Tier 3: Societal trust.			
Reactions:	Familiarize with incident managers guide.	Familiarize with interoperability with emergency service guide.	Outsource security specialist.			Develop crisis communication channels.			
Vulnerability/Consequence 6:	Pedestrian routes available for car traffic.					Tier 3: Political will endurance.			
Reactions:	Familiarize with security by design guide.	Invacuation guide.				Develop crisis communication channels.			
Vulnerability/Consequence 7:	Existing vehicle barriers are not certified.								
Reactions:	Familiarize with security by design guide.								
Vulnerability/Consequence 8:									
Reactions:									
Vulnerability/Consequence 9:									
Reactions:									
Vulnerability/Consequence 10:									
Reactions:									

A C C I D E N T

Scenario name:	**Improvise explosive device (IED) in an abandoned car/package/basket/under a sidewalk slab**

Description of the scenario:

Preparator
Mafia/organized crime group
Target
Religious leader
Time
Before or after public presence
Motive
to intimidate or eliminate chosen person
Week signal
conflict with some influential person or group
Early warning
suspicious package or vehicle, unauthorized construction sites
Impact
People see and feel the blast, heavily injured victims
Detection
No detection
Response
Evacuation, triage, first aid
First action
Evacuation
Lesson learned
Need to check site for suspicious objects

6.6 Reaction model for the scenario 6 : “Suspicious package of unknown origin (bio)”

Figure 16 - Reaction model for the scenario “Suspicious package of unknown origin”

	BEFORE ACCIDENT					DURING and AFTER ACCIDENT			
	Vulnerabilities					Consequences			
Vulnerability/Consequence 1:	Lack of CBR agents detection devices.					Tier 1: Directly affected population.			
Reactions:	Buy needed detection tools.					Familiarize with incident managers guide.	Familiarize with interoperability with emergency service guide.	Develop and implement Recognize/Assess/React protocol for CBRN incident.	Partial/phased/zonal evacuation.
Vulnerability/Consequence 2:	No CCTV permanent supervision.					Tier 2: Indirectly affected population.			
Reactions:	Hire additional staff.	Develop and implement Suspicious package/substance protocol.	Install required equipment/system.	Develop a welcome team.		Develop crisis communication channels.			
Vulnerability/Consequence 3:	Low awareness of security personnel.					Tier 2: Health services.			
Reactions:	Familiarize with incident managers guide.	Familiarize with interoperability with emergency service guide.	Outsource security specialist.			Develop crisis communication channels.			
Vulnerability/Consequence 4:	Security personnel not familiar with existing procedures.					Tier 2: Police and law.			
Reactions:	Familiarize with incident managers guide.	Familiarize with interoperability with emergency service guide.				Develop crisis communication channels.			
Vulnerability/Consequence 5:	Limited security personnel.								
Reactions:	Hire additional staff.	Install required equipment/system.							
Vulnerability/Consequence 6:	No designated safe room.								
Reactions:	Familiarize with security by design guide.	Familiarize with equipment recommendation guide.	Develop and implement Suspicious package/substance protocol.						
Vulnerability/Consequence 7:									
Reactions:									
Vulnerability/Consequence 8:									
Reactions:									
Vulnerability/Consequence 9:									
Reactions:									
Vulnerability/Consequence 10:									
Reactions:									

A C C I D E N T

Scenario name:	**Suspicious package of unknown origin (bio)**

Description of the scenario:

Preparator
Frustrated individual
Target
Religious leader
Time
Not specified
Motive
to intimidate or injure chosen person
Weak signal
No weak signal
Early warning
suspicious, unexpected mails and packages
Impact
Person who open mail/package is contaminated by dangerous material inside
Detection
Material falling or spilling from inside package
Response
Isolation of contaminated person, decontamination
First action
Isolation, turn off ventilation
Lesson learned
Protocol for suspicious package

6.7 Reaction model for the scenario 7 : “Exposure to a high activity radioactive source (rad)”

Figure 17 - Reaction model for the scenario “Exposure to a high activity radioactive source”

	BEFORE ACCIDENT					DURING and AFTER ACCIDENT			
	Vulnerabilities					Consequences			
Vulnerability/Consequence 1:	Litter bins unattended near escape routes.					Tier 1: Directly affected population.			
Reactions:	Familiarize with security by design guide.	Develop and implement Bomb threat-hoax protocol.	Develop and implement Suspicious item protocol.			Familiarize with incident managers guide.	Develop and implement Recognize/Assess/React protocol for CBRN incident.	Familiarize with interoperability with emergency service guide.	
Vulnerability/Consequence 2:	Lack of CBR agents detection devices.					Tier 1: Site/building/infrastructure stakeholder(s).			
Reactions:	Buy needed detection tools.	Develop and implement Venue search protocol.				Full evacuation.			
Vulnerability/Consequence 3:	No CCTV permanent supervision.					Tier 2: Health services.			
Reactions:	Develop and implement Venue search protocol.	Hire additional staff.				Develop crisis communication channels.			
Vulnerability/Consequence 4:	Limited security personnel.					Tier 2: Police and law.			
Reactions:	Outsource security specialist.	Hire additional staff.	Develop a welcome team.			Develop crisis communication channels.			
Vulnerability/Consequence 5:	Low awareness of security personnel.								
Reactions:	Familiarize with incident managers guide.	Familiarize with interoperability with emergency service guide.	Outsource security specialist.						
Vulnerability/Consequence 6:	No designated safe room.								
Reactions:	Familiarize with security by design guide.	Familiarize with equipment recommendation guide.	Develop and implement Suspicious package/substance protocol.						
Vulnerability/Consequence 7:									
Reactions:									
Vulnerability/Consequence 8:									
Reactions:									
Vulnerability/Consequence 9:									
Reactions:									
Vulnerability/Consequence 10:									
Reactions:									

ACCIDENT

Scenario name:	**Exposure to a high activity radioactive source (rad)**

Description of the scenario:

Preparator
Terrorist group
Target
People gathered
Time
During mass event
Motive
Injuring as much people as possible without warning
Week signal
No week signal
Early warning
Suspicious packages
Impact
Many people come in contact with high activity source
Detection
Similar radiation sickness symptoms
Response
triage, evacuation, detection
First action
inform emergency services
Lesson learned
search for suspicious packages

7. References

1. Alexander, D. A., & Klein, S. (2009). First responders after disasters: a review of stress reactions, at-risk, vulnerability, and resilience factors. Prehospital and Disaster Medicine, 24(2), 87-94.
2. Alexandra RIMPLER-SCHMID, Ralf TRAPP, Sarah LEONARD, Christian KAUNERT, Yves DUBUCQ, Claude LEFEBVRE, Hanna MOHN “EU preparedness and responses to Chemical, Biological, Radiological and Nuclear (CBRN) threats”, Brussels 2021
3. Carter, H., Drury, J., Rubin, G. J., Williams, R., & Amlôt, R. (2013). The effect of communication during mass decontamination. Disaster Prevention and Management: An International Journal, 22(2), 132-147.
4. Centers for Disease Control and Prevention (U.S.). October 2002. Available from: https://www.hsdl.org/c/abstract/?docid=3185
5. Cesium Radiation Goiania, Brazil Sept 13th 1987. Hot News. 20.2.2012. Available from: https://panji1102.wordpress.com/2012/02/20/cesium-radiation-goiania-brazil/
6. Endregard M., Breivik H., Schultz Heireng H., Enger E., Sandrup T., Kelly D. (2011), “D2.1 Scenario template, existing CBRN scenarios and historical incidents”, PRACTICE WP2 deliverable, 978-82-464-1986-2, https://www.ffi.no/en/publications-archive/d2.1-scenario-template-existing-cbrn-scenarios-and-historical-incidents
7. Homeland Security Digital Library. Available from: https://www.hsdl.org/c/tl/waco-siege-ended/
8. Jokinen, Christian. Foiled Ricin Plot Raises Specter of ‘More Sophisticated’ IS-inspired Attacks. Publication: Terrorism Monitor Volume: 16 Issue: 16. August 10, 2018. Available from. https://jamestown.org/program/foiled-ricin-plot-raises-specter-of-more-sophisticated-is-inspired-attacks/
9. Leeuw, M.W. (Project Coordinator) (2007), “Deliverable #9. Final report”, Assessment of the vulnerabilities of modern societies to terrorist acts employing radiological, biological or chemical agents with the view to assist in developing preventive and suppressive crisis management strategies (ASSRBCVUL), 2007-05-04, EU Restricted.
10. Liland, A. (2015). Societal Consequences of Nuclear Accidents. In Nuclear Terrorism and National Preparedness (pp. 201-212). Springer, Dordrecht.
11. Sen, Mayukh. How a Cult Used Salad Bars to Orchestrate the Worst Bioterror Attack in US History. Vice. March 15, 2018. Available from: https://www.vice.com/en/article/kzp4n9/wild-wild-country-netflix-salad-bar-bioterror-attack
12. Shutterstock: Aum Shinrikyo: Images from the 1995 Tokyo Sarin attack. 6.6.2018 Available from: https://www.bbc.com/news/in-pictures-43629706
13. Smolarkiewicz M., Zwęgliński T., “Mitigation of risk at places of worship through vulnerability triggered reactions”, Zeszyty Naukowe SGSP (SGSP’s Scientific Papers), 2023 (in preparation to be published in 2023)
14. Spinning Nemtsov's Murder and Attempted Murders of Navalny and Skripal. United States Department of State. Global Engagement Center. 4 Oct, 2021. Available from: https://www.hsdl.org/c/abstract/?docid=870732
15. Tengelsen, Leslie. Coordinated Response to Reports of Possible Anthrax Contamination,

Idaho, 2001

16. The National Academy of Sciences. The Convergence of Violent Extremism and Radiological Security, Proceedings of a Workshop—in Brief, March 2019.
17. World Health Organization, “Public health response to biological and chemical weapons. WHO Guidance” second edition, Geneva 2004.

8. List of Attachments (files)

1. RMT_Scenario scheme with reaction model_clear template.xlsx
2. RMT_Scenario scheme with reaction model_reference scenario 1.xlsx
3. RMT_Scenario scheme with reaction model_reference scenario 2.xlsx
4. RMT_Scenario scheme with reaction model_reference scenario 3.xlsx
5. RMT_Scenario scheme with reaction model_reference scenario 4.xlsx
6. RMT_Scenario scheme with reaction model_reference scenario 5.xlsx
7. RMT_Scenario scheme with reaction model_reference scenario 6.xlsx
8. RMT_Scenario scheme with reaction model_reference scenario 7.xlsx