IFTRIP
International Forum for Terrorism Risk (Re)Insurance Pools

GENEVA ASSOCIATION

Insurance and Chemical, Biological, Radiological, and Nuclear Risks

September 2025

GENEVA ASSOCIATION

Insurance and Chemical, Biological, Radiological, and Nuclear Risks

A joint report of the Geneva Association and the International Forum of Terrorism Risk (Re)Insurance Pools (IFTRIP)

Geneva Association

The Geneva Association was created in 1973 and is the only global association of insurance companies; our members are insurance and reinsurance Chief Executive Officers (CEOs). Based on rigorous research conducted in collaboration with our members, academic institutions and multilateral organisations, our mission is to identify and investigate key trends that are likely to shape or impact the insurance industry in the future, highlighting what is at stake for the industry; develop recommendations for the industry and for policymakers; provide a platform to our members and other stakeholders to discuss these trends and recommendations; and reach out to global opinion leaders and influential organisations to highlight the positive contributions of insurance to better understanding risks and to building resilient and prosperous economies and societies, and thus a more sustainable world.

Photo credits:
Cover page – Cash Macanaya for Unsplash

Geneva Association publications:
Pamela Corn, Director Communications
Hannah Dean, Editor & Content Manager
Jooin Shin, Digital Content & Design Manager

Suggested citation: Geneva Association and International Forum of Terrorism Risk (Re)Insurance Pools (IFTRIP). 2025. *Insurance and Chemical, Biological, Radiological, and Nuclear Risks*. September.

Contents

ACKNOWLEDGEMENTS

This report was prepared as a joint effort between the Geneva Association and the International Forum of Terrorism Risk (Re)Insurance Pools (IFTRIP). Editorial contributions were provided in particular by:

- Sina Nassiry and Corentin Gouache (Caisse Centrale de Réassurance)
- Frédéric Guyomard (Electricité de France)
- Staff of the Federal Insurance Office (FIO), US Department of the Treasury
- Darren Pain (Geneva Association)
- Carmen MacDougall, Hayley Severance, and Scott Roecker (Nuclear Threat Initiative)
- Steve Burr (Pool Re)

This report has also benefitted significantly from inputs and comments from various insurers, brokers, and other IFTRIP member organisations.

Foreword

This joint report of the Geneva Association and International Forum of Terrorism Risk (Re)Insurance Pools (IFTRIP) offers a timely and comprehensive analysis of the implications of chemical, biological, radiological, and nuclear (CBRN) risk for the re/insurance sector. Though CBRN malicious incidents are, thankfully, rare, their potential consequences are uniquely catastrophic. Emerging technologies such as drones and bioengineering are lowering the barriers for violent non-state actors (VSNAs) to access and operationalise CBRN materials. CBRN events have the power to destabilise societies and economies in ways few other threats can, and raise serious questions about preparedness, response, and financial resilience.

The report identifies significant gaps in traditional coverage for CBRN-related losses, with wide variation in how existing national insurance pools approach the threat. Strengthening CBRN resilience will demand greater dialogue and cooperation between governments, insurers, national pools, and international policy organisations, on concrete mechanisms to better assess and manage risks.

Against that background, this report also outlines practical pathways to help narrow the CBRN protection gap, improve modelling and scenario planning capabilities, and lay the groundwork for longer-term innovative solutions, notably in cross-border risk-sharing. We have an opportunity to boost societal resilience: by acting now, the global re/insurance community can help mitigate CBRN risks and ensure that future CBRN incidents do not result in devastating human loss or massive economic dislocation.

Jad Ariss
Managing Director,
Geneva Association

Steven Seitz
Chair, IFTRIP
Director, Federal Insurance Office (FIO),
US Department of the Treasury

Executive summary

CBRN risks are a growing threat to society, and the limited ability of re/insurers to absorb them creates a significant protection gap. Innovative public-private mechanisms would boost resilience and mitigate potential economic disruption.

The threat posed by chemical, biological, radiological, and nuclear (CBRN) incidents – particularly those stemming from terrorism – is a critical concern for policymakers and the re/insurance industry. While such events are rare, the rapidly evolving threat landscape, marked by rising geopolitical tensions, emerging technologies and increasingly capable violent non-state actors (VNSAs), demands sustained vigilance and strategic risk management. In 2021, the UK Government warned that a successful terrorist CBRN attack is likely by 2030 – an indication of growing unease about the escalation of global CBRN threats.

CBRN incidents remain rare but rising geopolitical tensions and new technologies are escalating threat levels.

The major loss accumulation potential associated with large CBRN-related incidents has typically restrained private re/insurers from covering such risks, except when property coverage is mandatory (such as in France and Spain). The scale and uncertainty of possible losses far outstrip what the re/insurance sector can safely and sensibly underwrite. As a result, most traditional property and casualty (P&C) policies, as well as corresponding reinsurance contracts, exclude coverage for CBRN-related losses or heavily sublimit the risk. Instead, different risk-sharing arrangements have emerged to pool and spread CBRN exposures across multiple balance sheets, both private and public.

However, should a major incident occur, innocent victims would face significant financial hardship and disruption. Such an event would likely place significant burdens on the resources of national, regional, and local governments to organise a recovery, meet any shortfall in finance, and compensate victims, which in turn could trigger fiscal strains and possible macroeconomic instability.

The potential scale and uncertainty surrounding losses from a CBRN incident limit how far re/insurers can cover these risks.

This report assesses recent shifts in the CBRN risk environment and the existing mechanisms available to manage these exposures. More specifically, it reviews the current insurance arrangements to respond to malicious CBRN attacks, determine what gaps exist in CBRN coverage within national re/insurance pools, and explore future directions for upgrading CBRN risk management frameworks.

The report focuses on CBRN terrorism risks relevant to P&C insurance, particularly attacks by VNSAs involving CBRN weapons or targeting CBRN facilities/distributors. It provides:

- An analysis of the changing CBRN threat landscape (section 2), including motivations, capabilities, and access by VNSAs to CBRN materials and facilities, with attention to the proliferation of technologies like drones, AI, and bioengineering that could enable more sophisticated attacks.
- A review of existing re/insurance arrangements (section 3), particularly the national re/insurance pools that have been formed to allow insurers to share nuclear and terrorism risks, highlighting differences in CBRN coverage across countries.
- Insights into risk modelling practices (section 4), showing how insurers and national pools use scenario simulations to assess potential CBRN impacts on their underwriting portfolios.

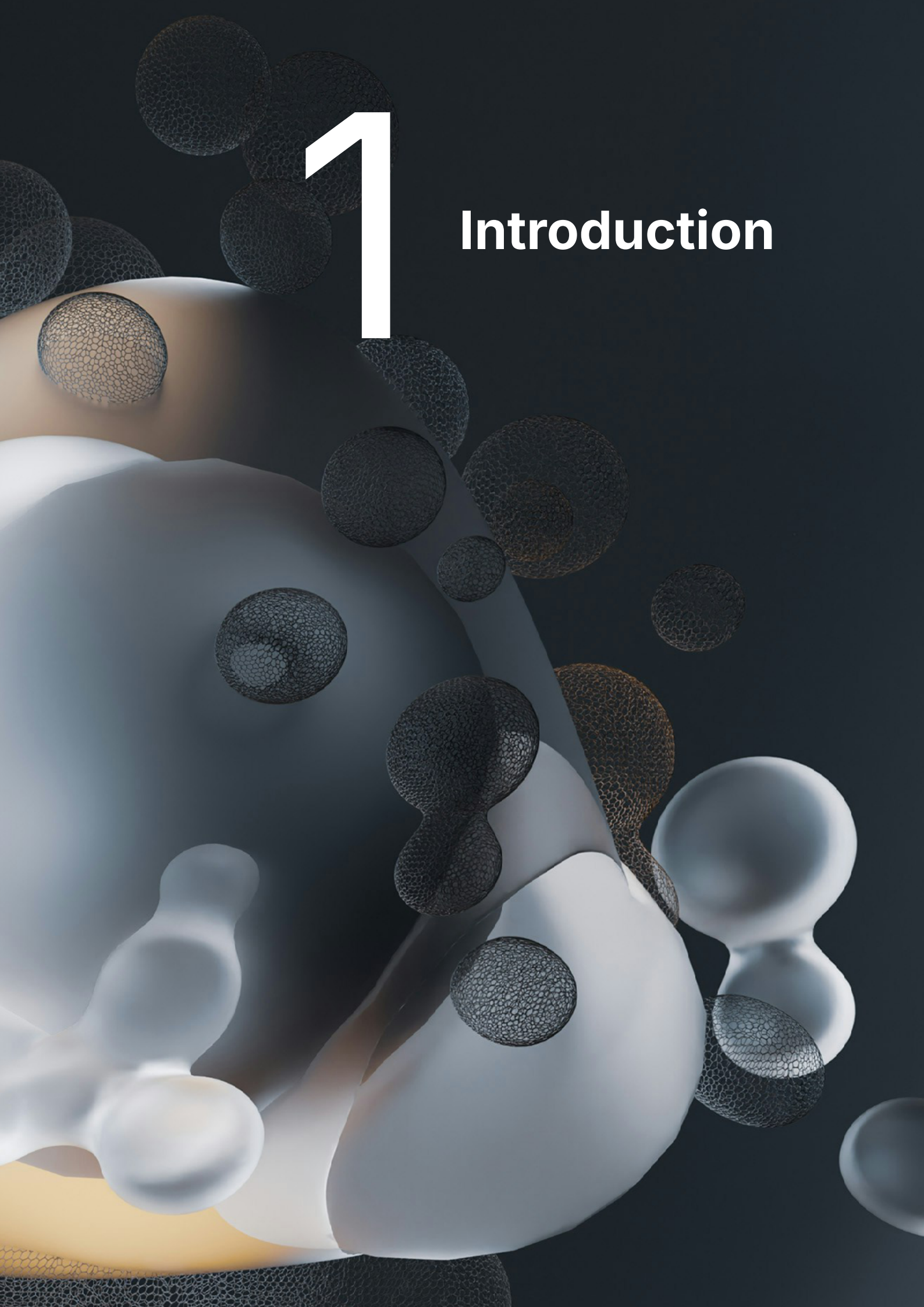
In concluding (section 5), the report discusses possible initiatives to help narrow the implied CBRN protection gap, improve CBRN risk management, and reduce the economic impacts of potential CBRN terrorist incidents.

Some areas for future consideration include:

- Sharing best practices among national terrorism pools, including experiences using alternative funding arrangements, and sponsoring terrorism risk modelling education and training.

- Exploring expanded international reciprocation arrangements for terrorism pools like those used in the nuclear power industry (although the current lack of standardised terrorism coverage and the national scope of existing pools is likely a major constraint).

- Fostering greater dialogue between re/insurers, governments, and international policymakers about CBRN exposures and innovative mechanisms to share associated risks.



1 Introduction

Introduction

CBRN threats have long been a concern for policymakers and re/insurers given the potential for long-term social and economic harm from such incidents.

The threat from a major chemical, biological, radiological, and/or nuclear (CBRN) incident has long concerned policymakers and re/insurers. The potential scale of destruction/disruption caused by such an incident and the fallout on households, businesses, and their insurers underscores the societal importance of the issue.

Amid rising geopolitical tensions and concerns about the ambition and capabilities of terrorist organisations to deploy CBRN weapons, this report assesses recent shifts in the CBRN risk landscape and the existing mechanisms available to manage these risks. More specifically, it reviews the current insurance arrangements to respond to CBRN-related perils, determines what gaps exist in CBRN re/insurance and national pool coverage, and suggests possible ways to upgrade CBRN risk management frameworks.

1.1 Defining CBRN

Since the 1990s, incidents related to chemical, biological, radiological, and nuclear agents that could cause harm through their accidental or deliberate release, dissemination, or impacts have been referred to as CBRN threats or events. The term 'CBRN' dates back to the cold war era, where it was first referred to as ABC (atomic, biological, chemical) and later as NBC (nuclear, biological, chemical).

There are various distinct classes of CBRN agents (Table 1). The health effects of an agent depend on several characteristics that impact not only the number and type of casualties but also how it is delivered, the type of emergency medical response, the physical protection required by responders, and other resources that might be needed such as decontamination capabilities or isolation areas.[1]

1 An agent's physical properties can vary across classes and influence key attack factors including the optimal delivery system, route of exposure, spread and ongoing presence in the environment (persistency), and the timing of the onset of effects (latency). See Bland 2013.

TABLE 1: CLASSES OF CBRN AGENTS

Agent	Main classes
Chemical	Nerve agents – highly poisonous chemicals that work by preventing the nervous system from working properly.
	Blister agents – chemical compounds that cause severe skin, eye, and mucosal pain and irritation.
	Cyanides (aka blood agents) – toxic chemical agents that affect the body by being absorbed into the blood.
	Choking/lung/pulmonary agents – chemicals that cause severe irritation or swelling of the respiratory tract (lining of the nose, throat, and lungs).
Biological	Live agents such as bacteria, including rickettsia and chlamydia, viruses and fungi.
	Toxins – chemical agents that are of biological origin and include those derived from bacteria, fungi, plants, and animals (venom).
Radiological	Ionising radiation – subatomic particles or electromagnetic waves that have sufficient energy to cause damage to cells and genetic material. Types include alpha, beta, and neutron particles; gamma rays; and X-rays.
Nuclear	Material involved in the nuclear power or weapon industry, or having fissile properties (i.e. capable of undergoing fission and generating energy, fission products, and neutron emissions).

Source: Geneva Association based on Bland and other publicly available sources[2]

1.2 Recent CBRN events

Malicious incidents involving CBRN materials remain rare. According to some experts, CBRN terrorism accounted for less than 0.25% of all terrorist attacks globally between 1970 and 2021.[3] However, while the number of CBRN attacks have generally been declining over the past two decades (see Box 1), the threat from violent non-state actors (VNSAs) persists and may even be worsening.

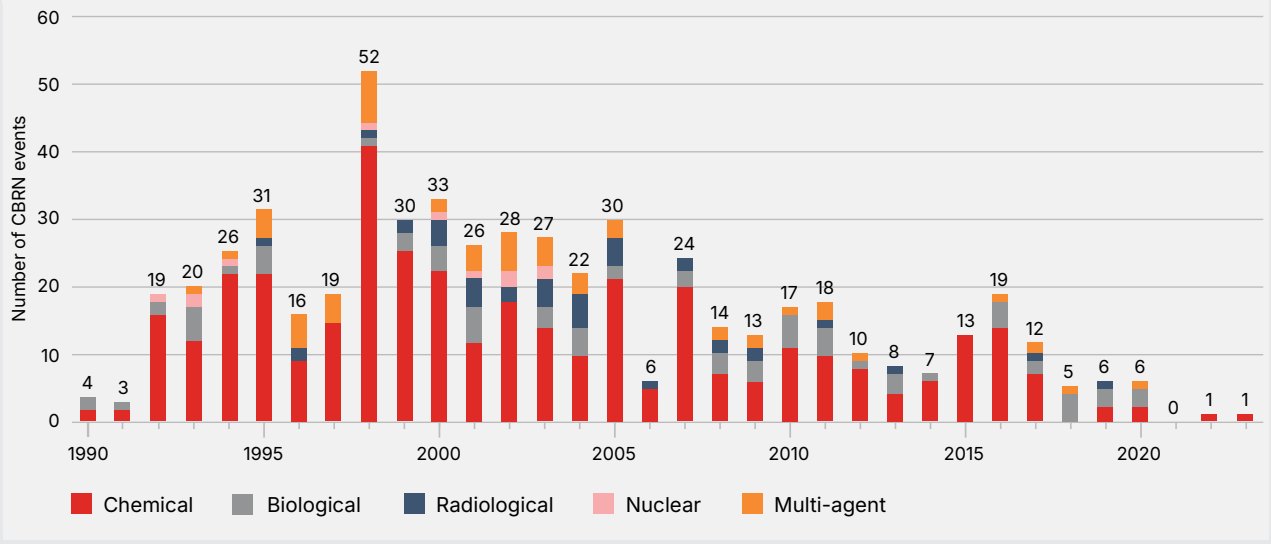
Box 1: Violent non-state actors and CBRN attacks

The VSNA CBRN Database[4] provides an historical record of CBRN events as documented from media reports and other terrorism event sources. VNSAs have been described as "any individual, group of individuals, or organization willing and capable of engaging in illicit acts and unsanctioned violence to achieve their goals. They neither directly nor officially represent a recognised state, but they may be supported by state actors."[5] This includes terrorist organisations, drug trafficking cartels, transnational criminal gangs, insurgents, and paramilitary groups. Such actors are normally distinct, although there can be overlap and, in some cases, they may share resources and capabilities to accomplish their respective goals.

Over the period 1990–2023 the database lists 566 CBRN VNSA 'events', with 379 involving chemical agents, 75 involving biological agents, 40 involving radiological agents, 11 involving nuclear agents, and 61 involving multiple agents (see Figure 1). Of these documented events, over half (293) were not successful in deploying CBRN agents but were planned attacks that were discovered before they were carried out or plots in the early stages of development.

2 Bland 2013.
3 CHC Global 2023.
4 University of Maryland (n.d.)
5 Tin et al. 2023.

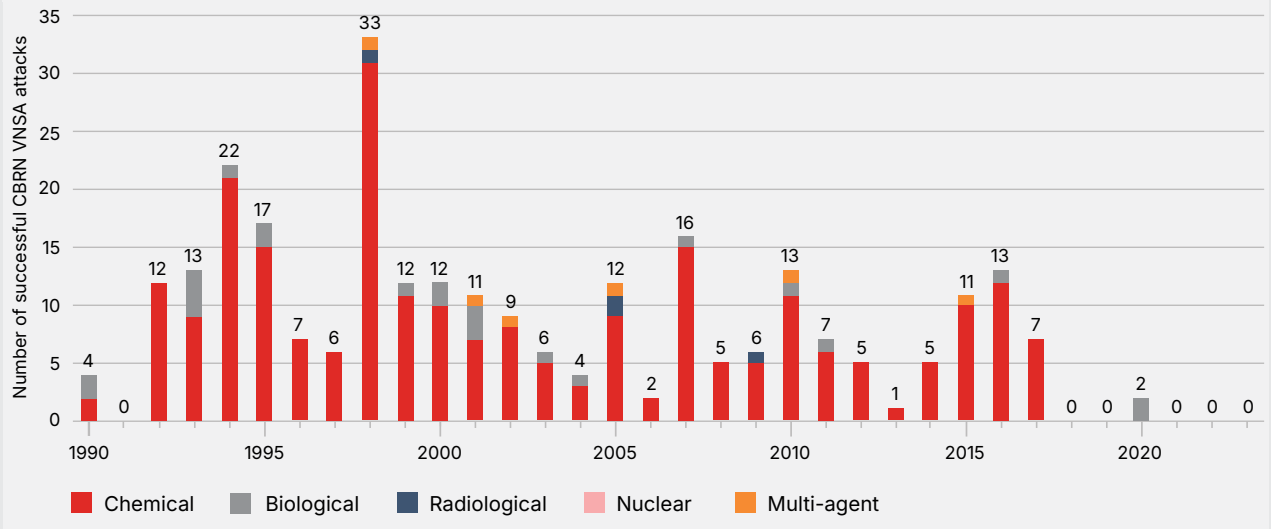
FIGURE 1: NUMBER OF CBRN EVENTS BY AGENT (1990–2023)



Source: University of Maryland[6]

During the same period, the database shows 273 attacks involving the successful deployment of CBRN agents, with nearly 90% involving chemical agents (244). While fewer in number, there have also been successful CBRN attacks involving biological (21), radiological (2), and multiple agents (6) including nuclear. There have only been two successful CBRN attacks since 2017, both involving biological agents in 2020.

FIGURE 2: NUMBER OF SUCCESSFUL CBRN VNSA ATTACKS (1990–2023)



Source: University of Maryland[7]

CBRN attacks have cumulatively caused 8,629 casualties, including 980 deaths and 7,649 injuries (Table 2); however, some were caused by non-CBRN agents such as guns and bombs. CBRN agents alone have caused 6,140 casualties, including 453 deaths and 5,687 injuries, with most coming from chemical agents (6,036 or 98.3%).

6 University of Maryland (n.d.)
7 Ibid.

TABLE 2: SUCCESSFUL CBRN ATTACKS AND CASUALTIES BY AGENT (1990–2023)

Agent(s)	Total attacks	No. killed (all)	No. wounded (all)	Total casualties (all)	No. killed (CBRN)	No. wounded (CBRN)	Total casualties (CBRN)
Chemical	240	961	7,540	8,501	438	5,598	6,036
Biological	23	15	59	74	15	39	54
Radiological	4	0	50	50	0	50	50
Nuclear	0	0	0	0	0	0	0
Multiple	6	4	0	4	0	0	0
Total	**273**	**980**	**7,649**	**8,629**	**453**	**5,687**	**6,140**

Source: University of Maryland[8]

Of the 273 total attacks, 207 (76%) took place in 10 countries (Table 3) and most occurred in the US (50). All told, attacks have occurred in 44 countries.

While having the highest number of CBRN attacks, the US experienced few casualties (132), with nearly all deaths recorded associated with one event – the 2001 'Amerithrax' attack. No casualties from CBRN attacks have occurred in any country since 2017.

TABLE 3: SUCCESSFUL CBRN ATTACKS AND CASUALTIES BY COUNTRY (1990–2023)

Country	Total attacks	Percent total attacks (CBRN)	No. killed (CBRN)	No. wounded (CBRN)	Total CBRN casualties	Percent total casualties (CBRN)
US	50	18%	5	127	132	2%
Iraq	34	12%	53	1,436	1,489	24%
Japan	27	10%	41	1,345	1,386	23%
China	22	8%	1	154	155	3%
Afghanistan	19	7%	12	987	999	16%
Cambodia	16	6%	228	507	735	12%
Russia	11	4%	44	202	246	4%
Colombia	10	4%	12	8	20	0%
Syria	9	3%	1	159	160	3%
Sri Lanka	9	3%	1	27	28	0%
Total top 10	**207**	**76%**	**398**	**4,952**	**5,350**	**87%**
Other (34 countries)	**66**	**24%**	**55**	**735**	**790**	**13%**
Total (all)	**273**	**100%**	**453**	**5,687**	**6,140**	**100%**

Source: University of Maryland[9]

Source: Contributed by FIO

8 University of Maryland (n.d.)
9 Ibid.

Some commentators highlight that the number of reports of propaganda and suspected terrorist attack preparations involving CBRN materials is increasing.[10] Particularly in Europe, arrests for suspected attack preparation using chemical materials and/or toxins have occurred in the last two years. In every case, the individuals were arrested before acquiring the necessary resources and knowledge to carry out an attack. The toxic materials involved were primarily hydrogen cyanide and ricin.

For example, in 2022, it was reported that a 16-year-old boy in Norway – motivated by Islamic State ideology – had manufactured nicotine poison in his garage.[11] Similarly, in Germany in early 2023, police arrested a 32-year-old Iranian man in the city of Castrop-Rauxel for allegedly plotting an islamist-motivated attack using cyanide and ricin.[12, 13, 14] Earlier that year, a man identified as the UK cell leader of the transnational neo-Nazi group Feuerkrieg Division (FKD), was sentenced to nine years and three months in prison for terrorism offences in the UK, which included research into the use of poisons.[15]

More generally, concerns about national security and safety from inadequate control or violent use of CBRN materials are intensifying. Threats include intentional attacks by state and non-state actors (e.g. terrorist movements), as well as the use of CBRN agents for smaller-scale crimes. In 2021, the UK Government made the alarming prediction that "it is likely that a terrorist group will launch a successful CBRN attack by 2030."[16]

Rising CBRN risks stem from intentional attacks, accidental release, and weak security safeguards.

The proliferation of potentially hazardous CBRN materials in different industries also raises the prospect of the unintentional release of and exposure to such agents. According to the Nuclear Threat Initiative (NTI), 34% of countries/areas have no regulatory requirements to protect their nuclear infrastructure/materials during a natural or human-caused disaster, and progress toward an improved security culture at nuclear facilities has almost ground to a halt.[17] This is occurring as many countries look to nuclear power generation as a potential alternative to fossil fuels. Similarly, 94% of countries have no national-level oversight for the dual use (i.e. civilian and military) of bioscience/biotechnology.[18]

1.3 Catastrophic loss potential

While focus on fatalities and bodily injuries in the wake of a malicious CBRN attack is natural, it likely only scratches the surface of the potential impact. Past incidents – although rare – indicate that the actual number of deaths was low (see Tables 2 and 3), surprisingly so given the toxicity of the material involved.[19] More broadly, the socioeconomic and human impacts of such events encompass direct and indirect effects, both of which can give rise to short-term and long-term costs (see Table 4).

10 Swedish Defence Research Agency 2024.
11 CHC Global 2023.
12 Radford 2023.
13 Some extremist groups espouse the 'accelerationist' philosophy – the idea that political goals can be achieved only via social collapse. One example is the neo-Nazi Atomwaffen group, which believes that modern, post-industrial society cannot be redeemed. Instead, its adherents think modern society ought to be driven into apocalyptic collapse so a white ethno-state or whites-only utopia can be constructed in its wake. In February 2023, Atomwaffen leader Brandon Russell and another member of the group were charged with attempting to blow up the Baltimore power grid. See Wendling 2023.
14 A social media post by Russell indicated that he had knowledge of how to build a nuclear bomb and may have been involved in plans to attack the Turkey Point nuclear power plant in Homestead, Florida in 2018. See Reitman 2018.
15 BBC 2023.
16 HM Government 2021.
17 NTI 2023a.
18 Millet 2024.
19 Integrity Initiative 2019.

TABLE 4: SOCIOECONOMIC AND HUMAN IMPACT OF CBRN EVENTS

Timeframe	Direct	Indirect
Short term	Crisis response costs (including emergency services)	Social upheaval in communities
	Damaged goods, destroyed property, damaged infrastructure	Reduced business trading in the vicinity of an incident, including evacuated areas and those affected by any government-imposed shutdowns
	Casualties and bodily injuries	Knock-on effects on economic supply chains, both upstream (suppliers) and downstream (customers)
	Costs of decontamination and reparation	Reduced consumer traffic, resulting in reduced activity
	Business interruption costs	
Long term	Long-lasting health (physical and mental) issues for victims, e.g. post-traumatic stress disorder	Lower potential economic growth from postponed/cancelled business investment, including foreign direct investment
	Permanent environmental contamination	'Psychological contamination' giving rise to fear and uncertainty, which deters spending in a region (e.g. inbound tourism) Increased transaction costs associated with heightened security measures

Source: Geneva Association

The full extent of any harm from CBRN agents need not solely arise from property damage or mass casualties or destruction. CBRN hazards have historically produced widespread dread within societies, which can have extensive social, macroeconomic, and environmental effects. These include the impact on public confidence and disruption to normal economic life, on top of the restoration and decontamination costs in affected and surrounding areas. In addition, unlike more conventional terrorist bomb attacks, small arms attacks, or industrial accidents, the consequences of a CBRN incident may transcend national borders and air spaces.

Exposure to a CBRN agent may not manifest immediately. Instead, the adverse health and environmental effects may reveal themselves only slowly over time. Moreover, uncertainty over such long-run consequences could act as a significant and persistent drag on economic activity in a region, as planned investment and consumer spending is delayed or curtailed. For example, a major CBRN terrorist incident could have a devastating long-term, negative impact on tourism in an area that would likely require extensive efforts to reverse.[20] It is difficult to measure the full economic impact of CBRN incidents, but past events underscore the potential devastating loss potential (see Box 2).

CBRN events can cause far-reaching societal, economic, and environmental disruption, even without mass casualties or large-scale property destruction.

20 Several studies have demonstrated the negative relationship between terrorism and tourism. Some stress that the 'memory effect' – the psychological phenomenon where individuals alter their usual behaviour as a result of past experiences or information – is heightened for terrorism incidents and can create a lasting negative impression in the minds of potential tourists. See for example the discussion in Chemli et al. 2024.

Box 2: Selected historical cases

Table 5 presents some estimates of the economic costs associated with past CBRN episodes (both accidental and malicious attacks), based on previous studies or news media reports. Different methods and computational assumptions – especially the scope of economic costs considered – make comparison across studies challenging. Nonetheless, at face value, past loss estimates vary widely, ranging from tens of millions of dollars to as much as USD 200 billion or more for directly affected countries, once the full macroeconomic impact is taken into account.[21]

TABLE 5: ESTIMATED ECONOMIC IMPACT OF PAST CBRN INCIDENTS

CBRN agent	Incident	Date	Description	Economic losses
Nuclear	Three Mile Island accident, Pennsylvania, US	March 1979	A combination of equipment malfunctions, design-related problems, and worker errors led to the partial meltdown of TMI-2 reactor and very small offsite releases of radioactivity. The TMI-2 accident was rated at Level 5 (accident with wider consequences).	The cleanup at TMI-2 cost approximately USD 973 million and took about 12 years to complete.
Chemical	Bhopal disaster, Bhopal, India	December 1984	Forty tons of methyl isocyanine leaked from an industrial plant due to a technical failure. 3,000–8,000 people died directly and approximately 20,000 died in the accident.	Recovery, reconstruction, and restoration came to USD 470 million.[22] Payments by the Indian Government in 1985 for food assistance and cash grants to families of the deceased totalled USD 40 million.[23] Litigation costs resulted in claims amounting to USD 3 billion.[24]
Nuclear	Chernobyl nuclear accident, former Soviet Union	April 1986	A sudden surge of power during a reactor systems test destroyed a reactor at the nuclear power station. The accident and the fire that followed released massive amounts of radioactive material into the environment.	Cleaning activities and decontamination costs were USD 17 billion.[25] Reparation costs in farming and the milk industry totalled USD 4.9 million.[26] Macroeconomic losses of Belarus from 1986–2015 came to USD 235 billion. International agricultural and horticultural losses (Sweden, Norway, and Germany) were USD 500 million.[27]
Chemical	Sarin subway incident, Tokyo, Japan	March 1995	The poisonous chemical weapon sarin was dispersed in five train cars on three subway lines that pass through Kasumigaseki Station in Tokyo during the morning rush hour.	More than 1,000 people were injured. The reason for the relatively small number of casualties was the low quality and ineffective employment of the sarin and the effective reaction of Japanese security forces.[28]

21 Samet and Sao 2016.
22 Kumar 1996.
23 Satyanand 2008.
24 Mahon and Kelly 1987.
25 Damveld 1996.
26 Steinhäusler 1988.
27 Shrivastava 1994
28 Pangi 2002.

CBRN agent	Incident	Date	Description	Economic losses
Biological	The Anthrax incidents, US	September 2001	In September and October of 2001, seven letters containing Bacillus anthracis (i.e. anthrax) were sent to political and media targets throughout the eastern US.	The direct costs of decontamination were estimated to be around USD 320 million, the majority of which was paid by the US government as most of the contamination was on federal property.[29] Medical spending totalled approximately USD 177 million.[30]
Nuclear	Fukushima Dai-ichi accident, Japan	March 2011	A 9.0-magnitude earthquake struck Japan about 231 miles northeast of Tokyo. Japan's Fukushima Dai-ichi facility lost all power from the electric grid, with diesel generators providing power for about 40 minutes. At that point, an estimated 45-foot-high tsunami hit the site, damaging many of the generators.	The Japanese Cabinet Office estimated the total damage at USD 210 billion, of which USD 129 billion was direct damage to buildings and facilities such as housing, offices, and plants, and USD 43.5 billion was for transport infrastructure, lifeline utilities, and critical infrastructure such as electricity, water, and communication. Damage to the tourism industry amounted to USD 8.7 billion.[31]
Chemical	Salisbury Novichok poisonings, Salisbury, UK	March 2018	Russian former double agent Sergei Skripal and his daughter Yulia were poisoned in Salisbury in March 2018. UK authorities subsequently announced that the nerve agent Novichok had been used.	The overall financial cost was reportedly well over GBP 150 million, with the bulk linked to reduced tourist income/ loss of business to the local economy, as well as significant spending on police and military involvement in the incident. Decontamination costs are estimated to be in the tens of millions of pounds.

Notes: According to research conducted by life sciences firm Antibodies.com[32]

Source: Geneva Association

29 Schmitt and Zacchia 2012.
30 Schmitt and Zacchia 2019.
31 Ranghieri and Ishiwatari 2014.
32 Hazardex 2019.

1.4 Scope and structure of the report

Although broad definitions of CBRN also include naturally occurring disasters and accidental incidents at hazardous installations, the focus of this report is on malicious attacks involving CBRN weapons or targeted at CBRN facilities/distributors. The emphasis is also on attacks carried out by VNSAs, although given the potential for covert state-sponsored (or at least tacitly supported) CBRN attacks, the lines between nation states and non-state perpetrators are often blurred.

This report investigates how losses from malicious CRBN attacks would be absorbed across public and private balance sheets and ways to enhance risk-sharing arrangements.

The report is structured as follows. Section 2 reviews and evaluates the current CBRN risk landscape in more detail, especially the likely source and extent of any threat and the key vulnerabilities that might be exploited by nefarious actors. This is followed in section 3 by an assessment of where such CBRN exposures probably reside. In particular, the scale of P&C losses that might ultimately fall on private versus public balance sheets from P&C risks, as well as the latest initiatives to quantify extreme CBRN risks. Section 4 discusses re/insurers' potential loss exposure, as estimated by selected terrorism modelling tools. Section 5 offers concluding remarks including avenues to upgrade CBRN risk management frameworks.

2 CBRN risk landscape

CBRN risk landscape

Declining nuclear security, vulnerable radiological sources, and emerging dual-use technologies heighten CBRN risks.

2.1 Terrorist motivations

The primary goal of most VNSAs is to create terror, generate media attention, and attract supporters to their cause. This can be done if an attack is successful, creates mass casualties, and causes significant damage. Conventional terrorism attacks using guns and bombs have often achieved these objectives but the use of CBRN weapons has the potential to escalate these outcomes by orders of magnitude. Even the threat of using a CBRN weapon may give a VNSA a psychological boost, provoking anxiety and alarm among potential targets[33] – a 'fear factor' that might further entice VNSAs to pursue CBRN weapons.[34]

CBRN weapons are a powerful fear multiplier, amplifying the psychological impact even if not successfully employed.

However, any decision to deploy CBRN weapons is complex. Terrorists must weigh the potential repercussions on their own operations. The use of such weapons is considered so irrational and morally reprehensible that it could alienate a group's support systems and international sponsors and discourage potential followers from being recruited.[35] Use of CBRN weapons would also likely provoke a severe retaliatory response from a state and the international community.

Some groups, possibly blinded by the fervour associated with their cause or led by a charismatic apocalyptic leader might nonetheless disregard any moral constraints against their use.[36] Large terrorist organisations, such as ISIS, may turn to CBRN weapons out of bravado, trying to orchestrate ambitious and spectacular attacks in Western cities to keep their supporters engaged. In addition, smaller groups or even individuals might, through desperation or grandiose ambition, decide to use crude CBRN weapons as a last-ditch effort to survive or gain notoriety for their cause, perhaps believing they are better able to avoid detection than more well-known adversaries.[37]

2.2 Access to CBRN materials

CBRN weapons are challenging and costly to develop and use. As well as procuring CBRN materials, VNSAs must also acquire the knowledge and technical skills needed to weaponise, safely assemble, and deploy a device. Large, well-financed groups have in the past attempted to buy complete weapons or weapon components from rogue nation states.[38]

According to the International Atomic Energy Agency (IAEA), the quantity of nuclear material needed to build a nuclear bomb is relatively small – just 8 kilograms of plutonium or 25 kilograms of highly enriched uranium (HEU).[39] Yet even if they can buy materials on the black market and find expertise through the dark web, VNSAs run the risk that their illicit operations are uncovered. There is considerable chance of detection throughout the entire CBRN armament process from funding,

33 CHC Global 2023.
34 Ibid.
35 Meulenbelt and Nieuwenhuizen 2016.
36 Apilado 2023.
37 Mihell-Hale 2023.
38 Broad 1997.
39 IAEA 2022.

procuring materials, hiring skilled workers, operating facilities, transporting a weapon, and avoiding security to deploy and trigger a device. The perpetrators must also be fearful of mishandling these materials and killing themselves.

2.2.1 Nuclear Security Index

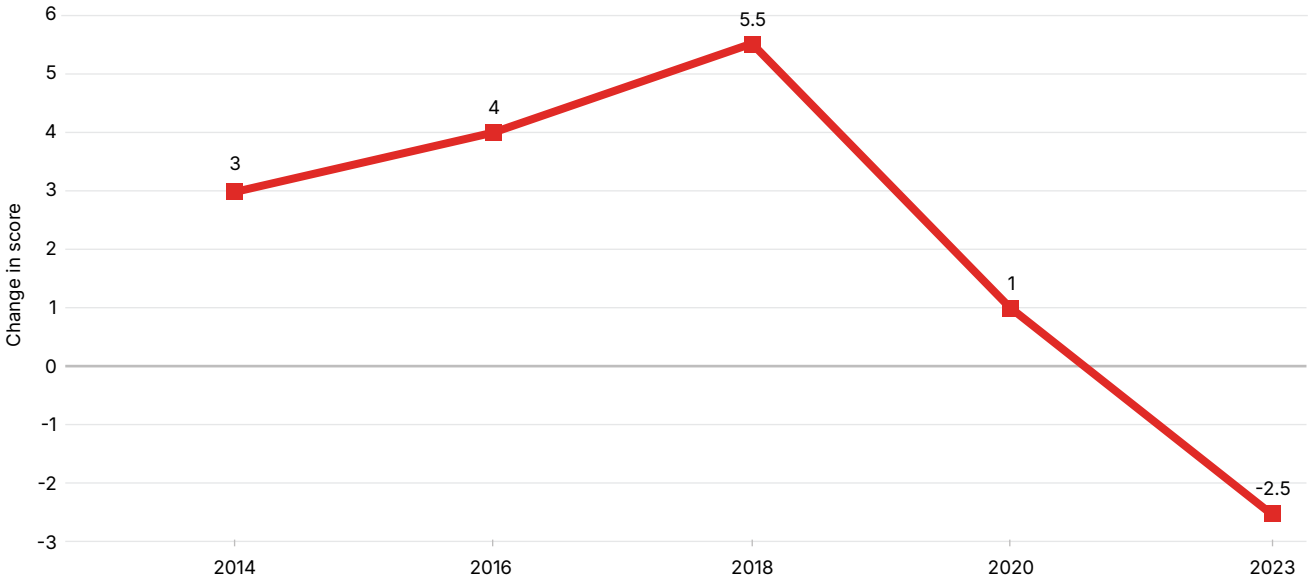
The NTI, a non-profit global security organisation, constructs indices to assess the nuclear and radiological security conditions in 176 countries (see Appendix 1 for more details). According to the NTI's 2023 Nuclear Security Index, '[t]errorist groups have shown clear interest in acquiring nuclear materials and sabotaging nuclear facilities, and disruptive technologies like unmanned aerial vehicles and hybrid threat capabilities pose new challenges.'[40] This is at a time when security for weapons-grade nuclear material seems to be loosening.

The 2023 NTI indices indicate several key trends that could have an impact on the ability of VNSAs to access CBRN materials. First, as shown in Figure 3, the median overall score of the 22 countries with weapons-usable nuclear materials declined by 2.5 points, showing that nuclear safety and security conditions have deteriorated in these countries.[41] This is part of a trend of declining index improvement rates since 2018 and per the NTI, 'comes at a time when risk environments are growing more dangerous because of a rise in instability, targeted political violence from non-state actors, and persistent cyber-attacks.'[42]

Weakening nuclear safety controls in countries with weapons-usable nuclear materials underscore growing CBRN risks.

Second, despite global efforts to limit weapons-usable nuclear materials, quantities of separated plutonium are growing rapidly, most notably at civilian facilities.[43] The 2023 NTI Index found that, since 2019, global inventories of separated civil plutonium have increased by 17,000 kilograms, enough material for more than 2,100 nuclear weapons.[44]

FIGURE 3: MEDIAN NTI SCORE AMONG COUNTRIES WITH WEAPONS-USABLE NUCLEAR MATERIALS

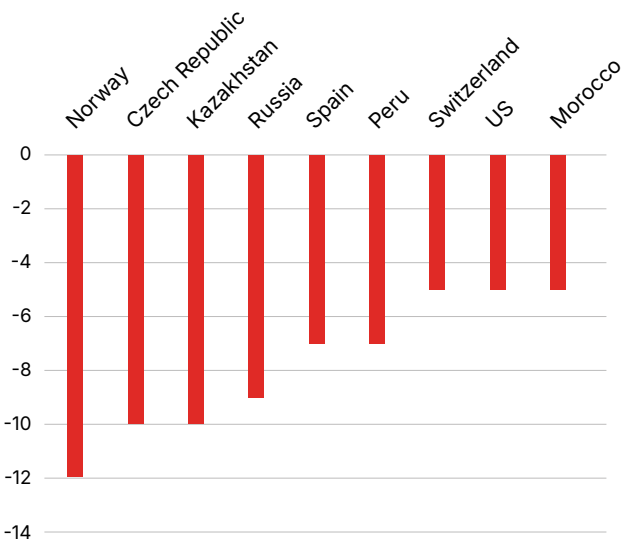


Note: An increase in NTI score indicates better overall nuclear security conditions.

Source: NTI

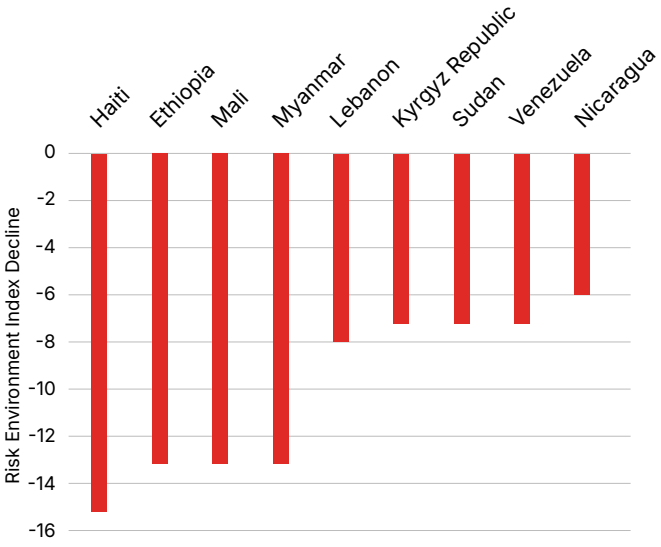
40 NTI 2023b.
41 Ibid. Although this decline is less pronounced if the focus is limited to Security and Control and Risk Environment factors, a downward trend is still observed even when the analysis is limited to these critical factors.
42 Ibid.
43 Ibid.
44 Ibid.

FIGURE 4: COUNTRIES WITH DECLINING NUCLEAR FACILITY SABOTAGE RISK SCORES



Source: NTI

FIGURE 5: COUNTRIES WITH DECLINING NUCLEAR MATERIALS THEFT RISK SCORES



Source: NTI

In 47 countries with nuclear power or research reactors, 26 had lower Sabotage Risk Environment scores than they recorded in the 2020 NTI Index. Nine countries had their score decrease by five points or more, including, surprisingly, several with advanced economies and with well developed nuclear generating capacity such as Norway, Russia, Spain, and the US (Figure 4). This indicates an increased opportunity for a VNSA to access and carry out sabotage at a nuclear facility, even in countries assumed to be secure.

Sabotage risks at nuclear facilities are also rising, even in advanced economies once considered highly secure.

Further, there are unprecedented risks facing all countries with nuclear materials – from political instability to full-scale war – a fact clearly reflected in the 2023 NTI Index Nuclear Materials Risk Environment Theft scores, which decreased for 120 of the 176 countries that the NTI Index ranks, including nine countries which had their score decrease by more than five points (see Figure 5).[45] This indicates a higher opportunity for a VNSA to acquire nuclear materials for a CBRN event.

2.2.2 The Radioactive Source Security Assessment

Besides nuclear power operations, radioactive materials are present in nearly every country and are used in a wide range of settings, from hospitals to oil fields. Although these sources cannot be used to fuel a nuclear weapon, they can be used to build a radiological explosive device, or 'dirty bomb', and they are generally stored in far less secure facilities than weapons-usable nuclear materials.[46]

Compared with a nuclear weapon, a radiological weapon requires less technical sophistication to build, and its detonation will likely result in far fewer direct casualties. However, a dirty bomb is still capable of causing significant harm, including widespread panic, environmental contamination, and significant social, economic, and financial costs.[47]

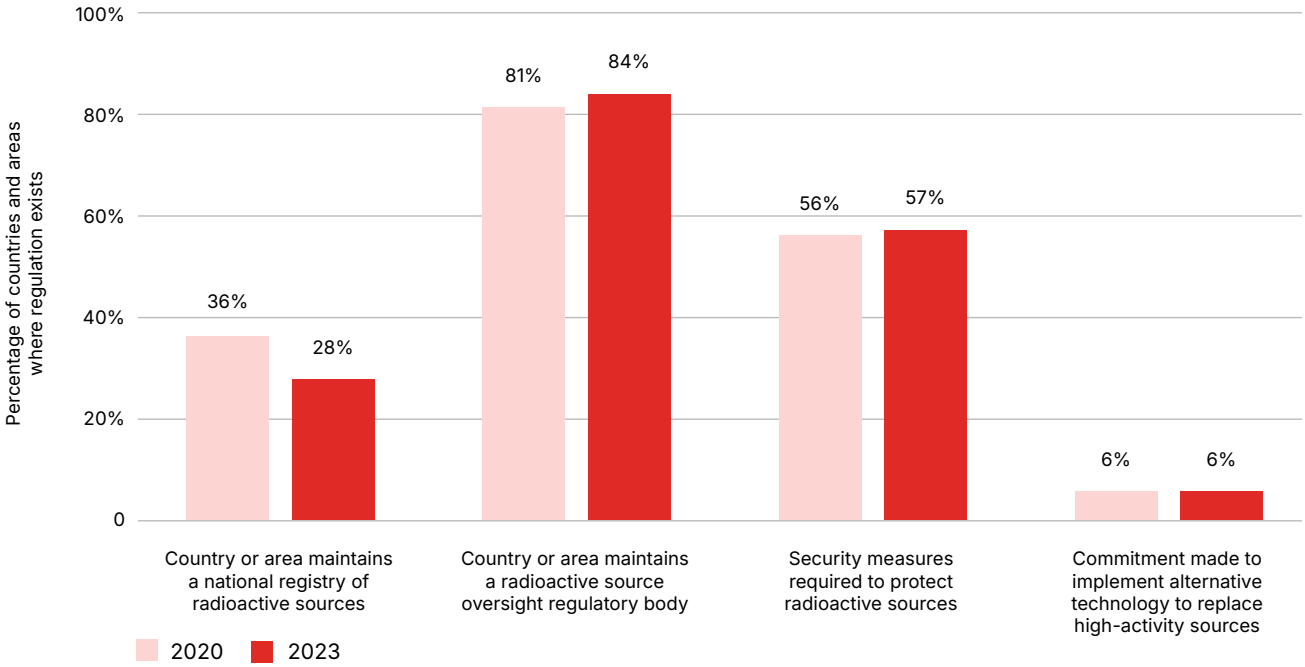
Radioactive material is generally easier to access than nuclear material, and can be used to build dirty bombs.

The 2023 NTI Index also includes a Radioactive Source Security Assessment (RSSA) that evaluates, but does not score or rank, national policies, commitments, and actions to secure radioactive sources (see Appendix 1). The latest RSSA found that radiological security has suffered from a lack of political attention in recent years, leaving many radioactive sources more vulnerable to theft than weapons-usable nuclear materials. Consistent with that

45 NTI 2023b.
46 Ibid.
47 Ibid.

trend, in 2023, the data for key measures showed countries have made little progress on improving the security of radioactive sources since 2020, the only other year in which data were collected (see Figure 6).[48]

FIGURE 6: ADHERENCE TO KEY RADIOACTIVE SOURCE SECURITY MEASURES (2020 VS. 2023)



Source: NTI

Of the 176 countries assessed, 76 have not implemented basic legal requirements to protect radioactive sources and 127 do not maintain national registries to track the movement of such sources, leaving them vulnerable to theft by nefarious actors.[49]

2.3 New capabilities and innovation

Rather than stealing or purchasing CBRN material via the dark web, VNSAs may be able to develop and deploy their own devices. Typically, this would require financial resources, skilled workers, a hidden specialised facility for construction, a safe means to transport the weapon to the target area, and a means to evade detection until the weapon is triggered. Until now, these capabilities have remained outside of the realm of most VNSAs.

However, developments in technology, including the off-the-shelf availability of unmanned aerial vehicles (UAVs) or 'drones', use of malware for cyberattacks, 3D printing, bioengineering, and AI could bring about radical innovation in the production and operationalisation of CBRN weapons by VNSAs.

Technological developments mean that it may become easier for perpetrators to develop and deploy their own CBRN weapons.

One of the key characteristics of these emerging technologies is their dual use. The same equipment and technical knowledge used for legitimate research and societal benefit can conversely be used for harmful purposes such as the manufacture of CBRN weapons (see Table 6). This makes it difficult to control who has access and to monitor whether these technologies are being used for good or evil pursuits.[50]

48 The NTI RSSA 'measures national policies, commitments, and actions in 176 countries related to securing radioactive sources to prevent a dirty bomb. The framework includes relevant laws and regulations, support for global norms, commitment, and capacity for replacing high-activity radioactive sources with alternative technology, and the risk environment.' NTI 2023b.
49 Ibid, p. 57.
50 Koblentz 2020.

TABLE 6: DUAL-USE TECHNOLOGY AND CBRN THREATS

Technology	Description
Drones	• Drones have been part of the arsenal of VNSAs for decades. The first documented case of a VNSA considering using an unmanned remote-controlled helicopter was the Japanese cult Aum Shinrikyo in 1994, apparently looking to use them to deliver chemical and possibly biological agents.[51] • Drones are particularly well-suited for the delivery of CBRN agents, with low-speed, low-altitude flight paths allowing them to evade detection and bypass enemy defences to disperse small payloads of chemical, biological, or radiological materials.[52] Drones are now regularly used for pesticide dispersal, and this crop-dusting ability could easily be adapted to spray biological or chemical agents over a target area.[53]
Computer and networking technology	• Computer systems and networking technologies have become an indispensable tool for human communication, offering an abundance of information and a great variety of applications. However, these technologies also offer ample opportunities for VNSAs to carry out CBRN attacks that can cause serious damage and casualties. • Globalisation and digitalisation are allowing new technologies and the knowledge needed to use them to disseminate farther and faster than ever before.[54] Technological capabilities allow VNSAs to share information, evade detection, plan, and carry out more organised CBRN attacks.[55] • VNSAs can also use the darknet and social media to source and purchase CBRN materials and recruit expertise to help develop and deploy CBRN weapons.[56] • There are concerns that a VNSA could use malware in a cyberattack against an industrial facility that produces or stores CBRN materials.[57]
Bioengineering	• The increasing pace of progress, from low-cost DNA sequencing to precision genome editing, has led to significant advances in medicine. However, it has made potential biological weapons more powerful and more accessible.
	• Through advances in biotechnologies, including the commercialisation of clustered regularly interspaced short palindromic repeats (CRISPR) and other genetic engineering tools, the plausibility of VNSA-made bioweapons is becoming more likely.[58]
	• Using this technology, pathogens found in the environment, such as those causing anthrax or smallpox, can be engineered in a laboratory to increase their resistance to existing countermeasures, virulence, or transmissibility.
	• Biological toxins such as ricin have been found for sale on the darknet[59] and there is a growing cadre of amateur DIY biologists and rogue scientists willing to sell their bioweaponisation skills to the highest bidder.[60]
	• Gain-of-function research studies the enhancement of pathogens by either increasing transmissibility or severity. Access to DNA sequencing, which makes this possible, has increased due to reduced costs and the availability of 'lab-in-a-box' set ups, which do not require specialised and expensive lab technologies. What was typically only accessible to resource-rich state actors are now accessible to non-state actors.

Source: IFTRIP

51 Kallenborn et al. 2023.
52 Ibid.
53 Lambert 2020.
54 Ibid.
55 Syahputra et al. 2024.
56 Ibid, p. 844.
57 Ibid, p. 181.
58 Cheng et al. 2023.
59 United States Attorney's Office 2014.
60 Koblentz 2020.

As noted by the NTI, nefarious actors, including VNSAs, with sufficient expertise, training, and laboratory infrastructure could use benchtop DNA synthesis devices or DNA synthesis services 'to create pathogens or toxins from scratch (de novo) or engineer pathogens with new, more dangerous traits.'[61] Further, as highlighted in Box 3, the NTI identifies three strategies whereby VNSAs might inflict significant harm using biotechnology:

- Assembling a full pathogen genome, i.e. generating DNA that encodes the pathogen's full genetic blueprint;
- 'Booting up' a pathogen, i.e. creating a functional pathogen from the DNA that encodes its genetic blueprint;
- Altering or enhancing the properties of a pathogen beyond those found in nature, for example, by making it more transmissible or virulent and/or resistant to medical countermeasures.[62]

Box 3: NTI biotechnology insights and concerns

In 2019, the NTI, in collaboration with the Johns Hopkins Center for Health Security and the Economist Intelligence Unit (EIU), first published the Global Health Security Index (GHS Index) – an assessment of global health security capabilities in 195 countries (see Appendix 1 for more details). The latest data were collected in 2021.

According to the NTI, the risk of malicious or accidental release of harmful biological agents remains a concern. One hundred and thirty-eight countries (70.8%) have GHS Index scores for biosecurity capacity – policies and practices that protect against the deliberate misuse of biology to cause harm – of less than 25 (on a scale of 1–100, with 100 being the most secure, see Figure 7). This includes nine countries[63] with scores of zero, all of which are ranked as very high risk for terrorism.[64] Similarly, 126 countries (64.6%) recorded scores for biosafety – working practices associated with safe handling of biological materials – of less than 25 (Figure 8). Per a report published by the NTI in 2023, 'DNA synthesis technology can enable researchers to study and engineer biological systems to better understand how they work, but it may also empower malicious actors by providing the building blocks of potentially dangerous biological agents.'[65]

FIGURE 7: 2021 GHS INDEX BIOSECURITY CAPACITY SCORES BY % COUNTRY, (n=195)

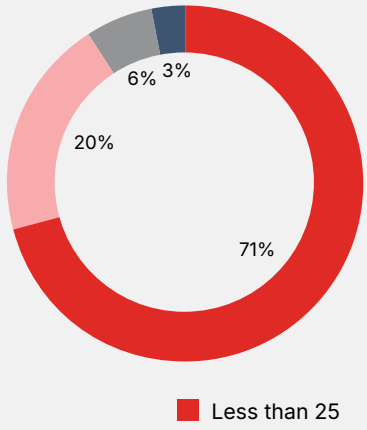
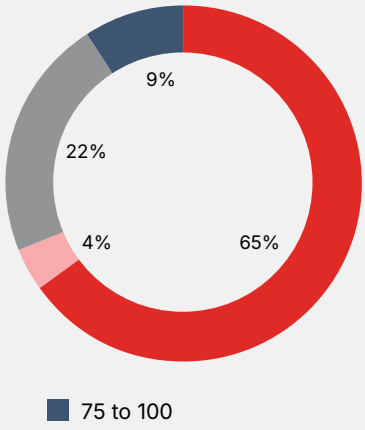
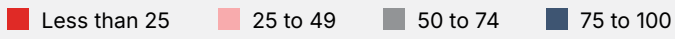


FIGURE 8: GHS INDEX BIOSAFETY CAPACITY SCORES BY % COUNTRY, (n=195)





Source: NTI

AI tools and technologies are also enabling the engineering of biological systems (AI-bio) for both legitimate and illegal uses.[66] In particular, knowledge and capabilities for producing well-known toxins, pathogens, or other biological agents could be deployed to cause significant harm. Without appropriate safeguards, a terrorist with little expertise in biology could use AI to become familiar with potentially harmful pathogens and learn how to obtain such agents. Malicious actors could also use AI-bio tools to develop novel biological agents not found in nature or more harmful than versions that may evolve naturally.

Source: NTI

61 In 2018, the NTI established the Biological Innovation and Risk Reduction Initiative to address emerging biological risks associated with rapid technology advances. See NTI 2023c.
62 Ibid, p. 23.
63 Afghanistan, Burkina Faso, Chad, Iraq, Libya, Niger, Somalia, Syria, and Yemen.
64 NTI 2021.
65 NTI 2023c.
66 Ibid.

2.4 CBRN infrastructure vulnerabilities

People are typically the primary target of CBRN terrorism. Thus, VNSAs will often prioritise locations where many people congregate, including public facilities such as stadiums, concert venues, shopping malls, places of worship, transportation centres, and office buildings in the central business district of cities. VNSAs may also launch attacks against critical infrastructure such as nuclear power plants, chemical processing and manufacturing facilities, or biological research facilities that could release radiation, toxic gas, or deadly pathogens, contaminate nearby areas and effectively turn the facility into a CBRN weapon.[67]

Besides physical attacks, intrusions could be initiated by an insider with expert knowledge who can sabotage key components and safety systems, leading to the release of harmful materials. Likewise, external cybersecurity breaches could create serious disruption. The vulnerability could be as small as a bug in a software programme, exploited by a hacker, that disables an industrial control system and disrupts its operation (see Box 4).

Disruption at a CBRN facility would likely cause physical damage to affected property and financial losses/expenses. The latter include not only the costs of dealing with the incident (including emergency responses and decontamination efforts) but also the disruption to business trading at victim firms and those in the surrounding area or affected supply chains. Depending on the scale and geographical fallout of the attack, many firms and individuals might look to insurance to cover some of the associated losses, a topic taken up in the next section.

67 Between 2015 and 2019, there were at least 57 drone incursions at 24 nuclear power plants in the US, and the UK government has recently revealed multiple drone sightings near British nuclear facilities between 2021 and 2023. See Beatty 2024.

Box 4: Energy critical infrastructure and cyber risks

As critical infrastructure (CI) increasingly becomes digitalised and networked, it is more vulnerable to multiple threats, including both physical and cyberattacks by terrorists or hackers. Maintaining ageing systems alongside developing robust protocols to secure complex supply chain issues only intensifies the cybersecurity challenges. Compromises can occur via digital tools – e.g. deployment of viruses/malware to disrupt operational technology (OT) systems – or physical threats, including drones for spying or carrying bombs.

Energy facilities may be intrinsically no more prone to cyberattack than other CI sectors, but the consequences of a major incident are potentially devastating, especially if they lead to the release of CBRN materials. Robust risk management arrangements that assess the potential for combined digital and physical intrusions at such installations are essential (not only at CBRN facilities themselves but across their suppliers) to avoid widespread 'cascading' effects that could bring cities and their citizens to a standstill.

Ransomware, malware, social engineering, threats against data integrity, or supply chain attacks may impact critical entities' essential functions. Hybrid threats could produce even stronger consequences because of the opportunity to use some temporary weaknesses or software vulnerability to penetrate and exploit many far-ranging targets.

Geopolitical instability

The Ukrainian conflict shows that the energy domain – especially nuclear power plants – remains an important target of cyber adversaries. Before the beginning of the invasion many incidents were detected. Power systems and the electrical grid and components have been targeted, and the first massive attempts took place as far back as December 2015 (BlackEnergy) and December 2016 (Industroyer) which were then followed in 2017 by NotPetya.[68] This mixture of traditional kinetic warfare with cyber-focused capabilities has created a new testbed for increased threat capabilities worldwide.[69]

Even outside of war zones, the threat from malicious attack on energy facilities (including nuclear power plants) appears to be growing. Despite security efforts in certain sectors, attackers continue to exploit the same technical weaknesses to gain access to networks. Exploiting 'day-zero' (i.e. previously unknown weaknesses in software or hardware) and 'day-one' vulnerabilities (i.e. known security flaws that remain unaddressed) remains a prime entry point for attackers, who all too often still take advantage of poor administration practices, delays in applying patches, and the absence of encryption mechanisms.

Evolving threat environment

According to cybersecurity commentators, the adversaries involved in attacks on CI vary widely in terms of their sophistication, technical capabilities, and objectives.[70] Some threat groups use highly advanced methods, including 'living off the land' techniques, whereby hackers use legitimate tools and features already present in the target system to avoid detection and ultimately carry out malicious activities. Conversely, some adversaries target easily accessible, internet-enabled devices that lack robust security protocols.

The motivation for attacks is also manifold, from activism and financial extortion to disruption or sabotage of key operations to serve political aims. A sizeable number of operations occurred during 2023, where the actions of cybercriminals, state-sponsored threat groups and hacktivists can be traced back to geopolitical developments.[71]

Tighter security regulations

Against that background and to support the resilience needs of CI, regulatory frameworks and compliance regimes have been tightened. The US Cybersecurity and Infrastructure Security Agency and the EU NISv2 (DIR 2022/2555) have established cybersecurity requirements for operators of essential services, including power generating companies. The North American Electric Reliability Corporation (NERC) and International Electrotechnical Commission (IEC) also provide strong recommendations to comply with NERC CIP and IEC 62443 standards.

Source: Contributed by Frédéric Guyomard, EDF R&D

68 Office of Budget Responsibility 2022.
69 Dragos 2024.
70 Ibid.
71 Ibid.

3 Existing CBRN re/insurance arrangements

Existing CBRN re/insurance arrangements

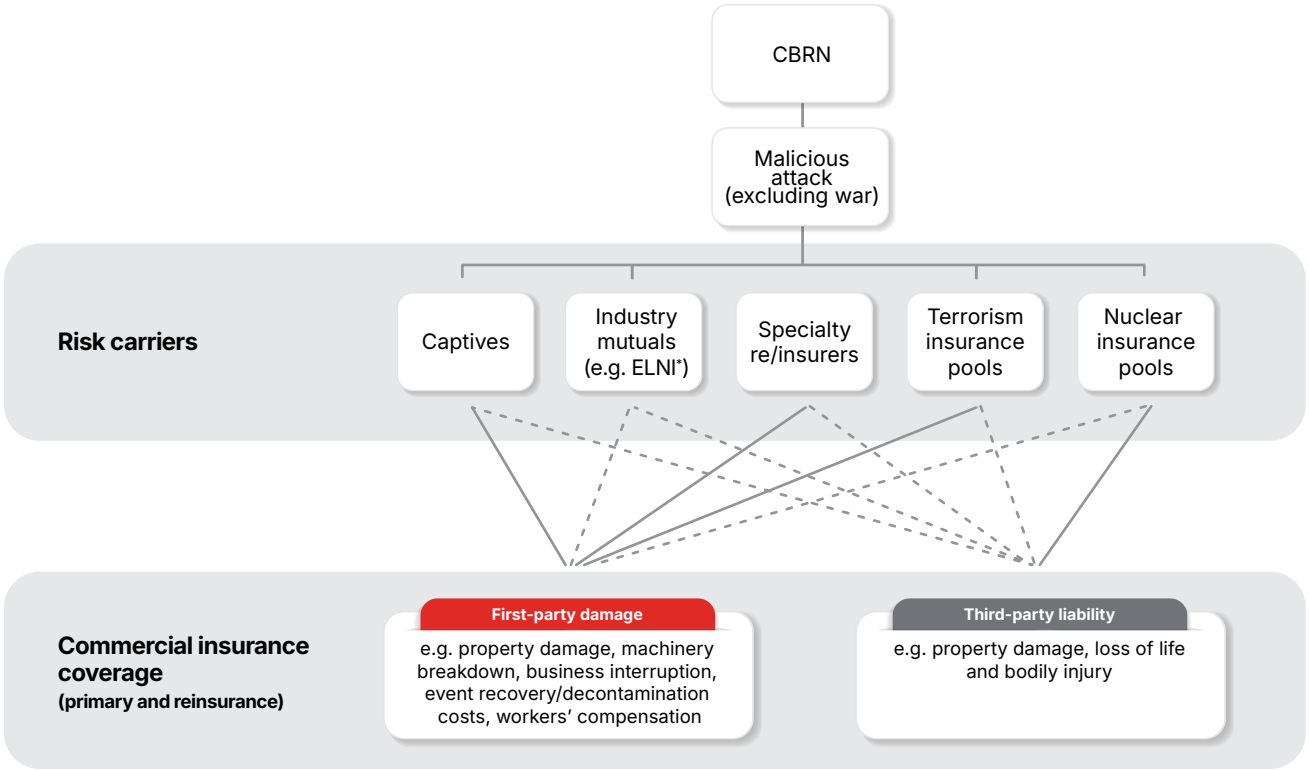
The potential for large-scale losses means CBRN risks are largely excluded from regular insurance policies, leading to significant coverage gaps.

The major loss accumulation potential of CBRN-related incidents has typically restrained private re/insurers' appetite for such risks. As a result, most traditional P&C policies (as well as their corresponding reinsurance) exclude coverage for CBRN-related losses or heavily sublimit CBRN exposures. Different exclusions often apply to each of the CBRN agents and policy wordings may vary by jurisdiction. But collectively these clauses severely restrict first- and third-party insurance coverage for losses from CBRN events regardless of their cause (i.e. whether accidental or intentional). For example, many re/insurance contracts will bar coverage for nuclear risks, including nuclear reactions, radiation, and radio-active contamination, although exclusions may not apply to liability arising from radioactive isotopes, the most common commercially used nuclear materials.

While specialty insurance is available that might respond in the case of certain CBRN incidents, especially malicious acts or involving particular facilities, individual policy limits are generally far lower than the limits available for conventional perils. Instead, different risk-sharing arrangements have emerged to pool and spread CBRN exposures across multiple balance sheets, both private and public, through a collection of self-insurance (including captive insurers), insurance, coinsurance, and international reinsurance mechanisms.

As a result, working out where CBRN risks ultimately reside globally, and which balance sheets are exposed in the event of an extreme CBRN incident, is difficult in advance of an event taking place. This is not least because different policies may respond if the CBRN incident is malicious, and only then if the attack was not part of an escalation of hostile activity between nation states or state-sponsored actors, when war exclusions could apply (Figure 9).

FIGURE 9: CBRN COVERAGE



** ELINI is a Belgian mutual insurance association formed in December 2002 to provide insurance capacity for nuclear liability risks to its members.*
Solid line: CBRN coverage (full or partial) typically available, at least in principle.
Dashed line: CBRN coverage sometimes available, but varies by country, insurance classes and perils.

Source: Geneva Association

3.1 Primary cover for malicious CBRN incidents

In the first instance, firms with significant CBRN terrorism exposure may choose to retain the associated risks, both direct losses they may face themselves as well as liabilities to third parties. Companies self-insure by building up funds to absorb potential future losses from attacks on their facilities or operations. While rare, this may include forming their own captive insurance companies to manage the firm's CBRN exposure and that of its affiliates. As well as covering risks that may be difficult to insure, captives can be a capital-efficient way to consolidate exposures and access reinsurance capacity to spread risks.[72]

In certain industries, businesses cooperate to combine risk-absorbing capacity. Different institutional arrangements exist, including group captives (where a collection of like-minded companies band together to form an insurance facility) and industry mutuals (where an insurer is owned and governed by its member insureds, who operate within a specific industry).

Most obviously, nuclear power facilities participate in long-standing mutual arrangements to share incurred losses that arise from an accident or a deliberate terrorist attack on their operations. These mutuals typically involve nuclear operators from different countries, although scheme membership and the extent and type of coverage varies. For example, the European Mutual Insurance for Nuclear Installations (EMANI) principally underwrites losses related to property damage, while the European Liability Insurance for the Nuclear Industry (ELINI) is focused on liability – however, their normal capacity is limited (EUR 650 million for EMANI and EUR 200 million for ELINI).[73]

72 Captives can write primary and excess insurance on a direct basis and may also operate as reinsurers. They may underwrite a wide variety of first- and third-party risks, including property, general liability, professional liability, surety, employer's liability, crime, and auto liability.
73 The coverage also follows original policies, which suggests that there could be further exclusions or limitations for terrorism. The retention for members is protected by reinsurance.

Firms heavily exposed to CBRN risks often self-insure or form mutuals to share risks, but coverage remains limited.

Although domiciled in Europe, both EMANI and ELINI also provide co-insurance for nuclear operators outside the region. In the case of harm arising from incidents at nuclear power plants, third-party liability is governed by national legislation and international conventions (see Box 5). These attribute sole liability to the nuclear installations, regardless of their culpability and/or the involvement of external suppliers or contractors.

Dedicated CBRN terrorism insurance also exists either as a standalone product or embedded within other P&C policies (i.e. an endorsement to a standard contract), including terrorism/political violence insurance. Such cover enables companies which are vulnerable to CBRN-related attacks – not just those in the nuclear industry – to transfer some of their exposure to private insurers. This, however, is a niche market – most insurers will generally exclude CBRN risks in their policies – and the scope of coverage is restrictive, more so than for conventional terrorism cover, with modest individual policy limits.

Box 5: Legal liability regimes for CBRN-related harms

Legal frameworks surrounding CBRN activities and events are scattered throughout a multiplicity of international, regional, and sectoral laws. In some areas, like liability for damage caused by a nuclear accident, international treaties are well established, although these sit alongside a patchwork of national laws and regulations where individual countries may implement their own regimes.[74] Beyond nuclear energy safety (and oil transportation), however, international liability conventions have struggled to gain traction, leaving victims to pursue claims through civil litigation.[75] This can be challenging, not least given the transboundary nature of any damage, uncertainty over attributing an incident and the appropriate jurisdiction, as well as the potential difficulty in establishing a defendant responsible for any harm.

Nuclear liability principles

While country details differ, most international conventions and national laws regarding third-party liability of nuclear operators (e.g. a power plant, enrichment/fuel facility, reprocessing facility) generally adhere to the following principles:[76]

Strict liability: The operator is liable whether or not any fault or negligence can be proven.

Exclusive liability: Through so-called legal channelling all claims can be brought solely against the operator, regardless of the cause of damage.

Non-discrimination: Victims should not be excluded from pursuing compensation based on nationality, domicile, or residence.

Mandatory financial coverage: The operator is obliged to maintain insurance cover or another type of financial security.

Exclusive jurisdiction: Only courts of the country in which the nuclear accident occurs have jurisdiction.

Limitation of liability: The operator is only liable up to a given financial amount and claims must be brought within a certain period of time following an incident.

Nuclear liability regimes do not generally differentiate between safety incidents such as accidents or natural disasters and security incidents involving deliberate acts intended to cause harm or unauthorised access; civil liability attaches in the same way. There may though be scope for exceptions where the damage is caused by armed conflict, hostilities, civil war, or insurrection, but this does not extend to acts of terrorism.[77]

Source: Geneva Association (based on published sources)

74 The two main international instruments are the Vienna Convention on Civil Liability for Nuclear Damage and the Paris Convention on Third Party Liability in the Field of Nuclear Energy. However, not all countries have ratified these agreements and operate their own nuclear liability regimes. For example, the US legal framework is based on The Price-Anderson Act.
75 Schmalenbach et al. 2023.
76 World Nuclear Association 2021.
77 IAEA (n.d.)

3.2 Reinsurance and retrocession

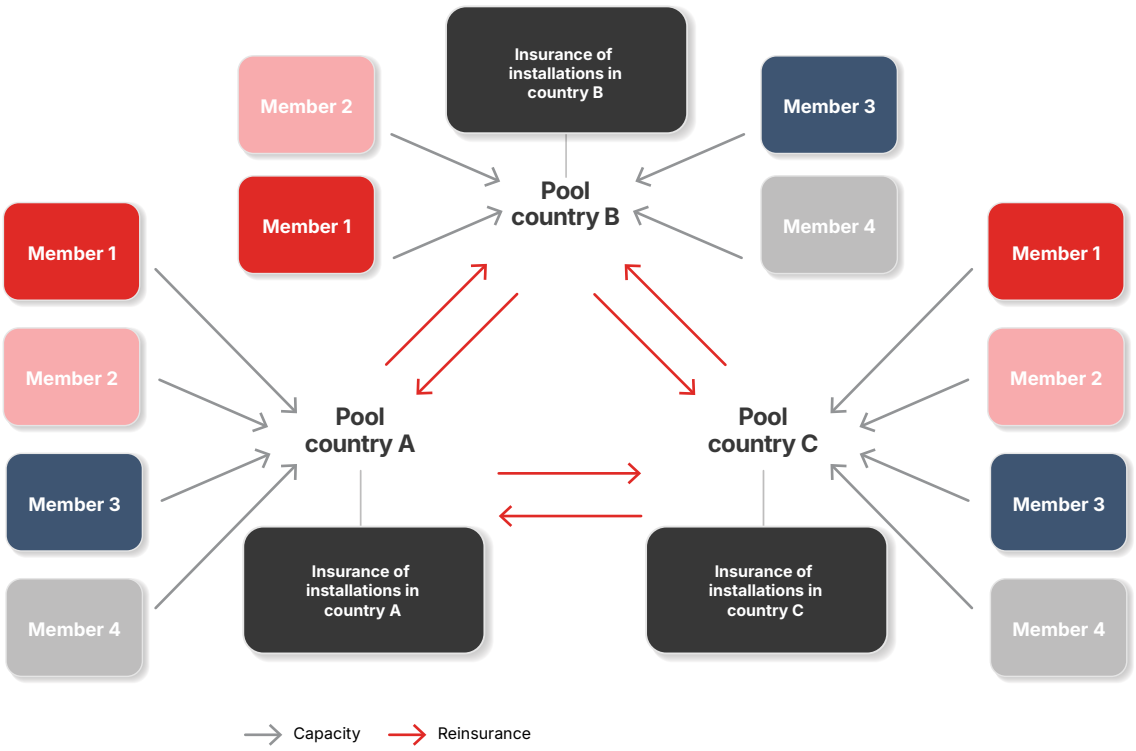
Insurers, whether captives, mutual insurance companies, or private insurers, typically seek to transfer some of their CBRN exposure to reinsurers, who in turn can retrocede some risk to other parties, including financial market investors (e.g. by means of securitisation). The array of reinsurance and retrocession is, however, complex, not least because it usually involves wholesale subscription markets (where the risk is split up and spread among multiple insurers) as well as international reciprocation arrangements.

The transfer of nuclear-power-related risks often takes place directly within nuclear insurance pools – formal groups of re/insurers dedicated to jointly underwriting losses resulting from nuclear incidents. Focused mostly on civil liability claims in connection with the use, construction, and decommissioning of nuclear installations, nuclear insurance pools may also underwrite property damage, machinery breakdown, business interruption, and terrorism risks of their insureds. Large nuclear operators sometimes also cede risk to the pools alongside regular reinsurance.

There are currently 28 nuclear pools providing third-party liability and, in some cases, first-party property and business interruption coverage to domestic nuclear. In addition to insuring the nuclear risk in their own countries, they also provide reinsurance capacity to each other. There are also several global mutual groups that exclusively offer nuclear reinsurance, including the Nuclear Industry Reinsurance Association and BlueRe. In some countries the terrorism coverage of nuclear plants is covered in whole or in part by the local terrorism pool (e.g. US).

The nuclear pools are organised along national lines, although often reciprocation agreements allow pools to share insured losses among themselves (see Figure 10). Sometimes, the pools lay off some of their risks to private re/insurers, including industry mutuals – for example, in the US, Nuclear Electric Insurance Limited (NEIL), a US mutual insurer owned by utility companies, reinsures a significant portion of the liability programme of the US insurance pool American Nuclear Insurers (ANI), while ANI reinsures a significant portion of NEIL's nuclear property programme.[78, 79]

FIGURE 10: NUCLEAR INSURANCE POOL BUSINESS FLOWS



Source: Nuclear Risk Insurers

78 See: https://www.amnucins.com/insurance/.

79 In 2019, ANI's members retained 66% of the liability exposure under each policy, ceded 27.1% to NEIL, and ceded 6.9% to reinsurers around the world. ANI's reinsurers include similar pooling operations in several foreign countries – each comprising their own native group of member insurance companies. United States Nuclear Regulatory Commission (USNRC) 2021.

National insurance pools have also been formed to allow insurers (including captives) to share terrorism risks. Data gathered from IFTRIP member countries (see Box 6) shows CBRN coverage differs across the terrorism pools. Most offer some form of property damage and business interruption cover for CBRN risks. In some schemes such as Pool Re, (the UK terrorism pool), GAREAT (the French terrorism pool) and Consorcio (the multi perils Spanish insurer) this includes losses arising from a cyberattack that leads to physical damage, provided the incident meets the legal criteria of terrorism. Third-party liability costs, however, are not generally covered by national terrorism insurance pools.

To the extent that they offer cover, terrorism pools often retrocede some risks back to the private reinsurance market. For instance, Pool Re has a retrocession programme involving more than 50 international reinsurers, including property damage arising from CBRN attacks.[80] Similarly, the Australian Reinsurance Pool Corporation buys retrocession cover – although losses or liabilities arising from the hazardous properties of nuclear fuel, material, or waste are not eligible for inclusion in the terrorism pool.[81]

National terrorism pools also share some CBRN risks, but coverage varies and third-party liability is typically excluded.

Though less common, insurance linked securities (ILS) have been used to transfer terrorism risks to capital markets, including CBRN exposure. Pool Re sponsored the first standalone terrorism risk catastrophe bond in 2019, which was subsequently renewed in 2022.[82] Also, GAREAT issued a EUR 100 million bond in late 2024 which protects from physical property damage caused by terrorism in France and its territories.[83]

80 The three-year retrocession agreement is structured as an aggregate excess of loss treaty which will respond if Pool Re's losses, individually or in aggregate, exceed GBP 400 million in any year. See Pool Re 2022a.
81 Australia's Terrorism Reinsurance Pool (ARPC) 2023.
82 The latest ILS transaction provides Pool Re with a three-year source of fully collateralised retrocessional capacity worth GBP 100 million. This covers the pool against losses from terror attacks, both conventional terrorism, such as blast damage, as well as non-conventional events such as CBRN and cyber terrorism. Pool Re 2022b.
83 Evans 2024.

Box 6: Comparison of IFTRIP CBRN country coverage

In 2024, IFTRIP carried out a survey of CBRN coverage across its member organisations. The results are summarised in Table 7.

TABLE 7: SUMMARY OF TERRORISM POOL CBRN COVERAGE

Country	Acronym	Mandatory availability	Mandatory take-up	CBRN coverage	CBRN property coverage	CBRN business interruption	CBRN liability coverage	CBRN workers' compensation coverage
Australia	ARPC	No	No	Chemical & biological only	Chemical & biological only	Chemical & biological only	No bodily, other for chemical & biological only	No
Austria	VVO	No	No	No	No	No	No	No
Belgium	TRIP	No	No	Yes for eligible risks	Yes for eligible risks	Yes, excluding specific business classes (nuclear facilities, energy, railway rolling stock, aircraft, and ships)	Yes, excluding third-party liability for nuclear energy	Yes. Has a limitation on indemnity, but not applicable to workers' compensation insurance
Denmark	N/A	Mandatory for Danish and foreign insurance companies operating in Denmark, which provide fire insurance for assets covered by the scheme	No	Yes	Yes, own property damage is covered but only for CBRN terrorism events and provided the property has fire insurance	Yes, covers business interruption losses related to property that is insured under a fire insurance policy. However, non-damage business interruption is excluded	No	No
France	GAREAT	Yes	No	Yes, all property policies	Yes	Yes	No	No
France	CCR	No	No	Yes, all property policies	Yes	Some kinds covered by the compulsory coverage	No	No
Germany	Extremis	No	No	No	Yes	No	No	No
India	IMTRIP	All non-life insurance companies underwriting property business are required to cede terrorism risk business	No	No	No	No	No	No
Netherlands	NHT	Participation is elective but 95% of all insurance companies in the Netherlands are members	No	All except nuclear	Yes for eligible risks	Yes	Yes, but only liability of others than the terrorist themselves	No workers' compensation but with employer's liability claims any outlays by the insurer are covered
South Africa	Sasria	No	No	No	No	No	No	No
Spain	CCS	Yes	Yes	Yes	Yes	Yes	No	No
UK	Pool Re	No	No	Yes	Yes	Yes	No	No
US	TRIP	Yes	No	If not excluded from primary	If not excluded from primary	If not excluded from primary	If not excluded from primary	Yes, in nearly all cases

Source: IFTRIP

The data show that:

- Several national pools provide some form of property coverage for CBRN losses. However, while some provide comprehensive property damage and business interruption coverage for CBRN terrorism events, others offer only partial indemnity protection – for example, the ARPC terrorism pool covers events involving chemicals and biological agents but not radiological or nuclear.
- CBRN exposure is usually capped, although in two countries – Spain and the UK – the amount of funds available is unlimited for certain lines of business based upon state guarantees. These schemes involve different funding mechanisms, including the collection of premiums or post-event surcharges, retrocession agreements with the national government, and purchase of ILS.
- Third-party liability and workers' compensation claims are not typically covered by national terrorism pools. A major exception is the US, where the US Terrorism Risk Insurance Program (TRIP) does provide CBRN terrorism coverage in connection with workers' compensation insurance losses as well as under fire policies in all US states with so-called 'fire following' laws (both on account of mandates imposed by existing state insurance laws in the US).

Source: FIO (based on input from IFTRIP member organisations)

3.3 Public-private schemes

Since aggregated potential losses from a nuclear or CBRN terrorism incident may exceed available private-sector risk-absorbing capacity, governments sometimes put in place some form of ex ante financing facility to cover large-scale, catastrophic insurance losses. The precise design and operation of such public-private partnerships (PPPs) varies across countries, although the main ones involve either a publicly owned direct insurer, a state-run reinsurance facility, or a government (retrocession) guarantee for private-sector pools.[84]

Governments may provide backstop finance for extreme CBRN risks, typically through a publicly owned insurer, a state-run reinsurer, or an explicit state-backed guarantee for a private-sector pool.

The ultimate size of a government's exposure to CBRN-related insurance losses (and hence its potential contingent fiscal liability) depends on the underlying peril and the terms of a PPP's funding arrangements. In some countries there is either no explicit state backstop (e.g. for civil liability arising from an accident at a large nuclear facility); in others it is capped at a certain amount – for example:

- The US TRIP limits total terrorism payments in any one year (government and private industry combined) to USD 100 billion and any government reimbursement payments within this amount are subject to recoupment through subsequent levies against commercial policyholders.[85]
- Also in the US, The Price-Anderson Act makes government indemnification up to USD 500 million available to small nuclear facilities with rated capacity less than 100 MW(e).[86] For operating commercial nuclear power reactors with rated capacity of 100 MW(e) or greater, government indemnity obligations under The Price-Anderson Act were phased out from 1975. For a description of the current US nuclear insurance regime, see Box 7.

84 For an overview of the features of different public-private partnership schemes for national terrorism, nuclear, and natural catastrophe risks, see the Appendix in Geneva Association 2022.
85 In the event of a terrorist attack on a nuclear facility, the US nuclear liability insurance pool (ANI) would be reimbursed for any amounts it paid from the state-backed TRIP, subject to a pre-determined deductible and retention. USNRC 2021.
86 Ibid.

Box 7: The Price-Anderson Act and nuclear insurance in the US[87]

The Price-Anderson Act of 1957, 42 U.S.C. § 2210, was enacted to indemnify the emerging nuclear industry from catastrophic third-party liability losses associated with a major nuclear accident. The law established accident liability limits for owners and operators of nuclear power reactors and their suppliers, and a mechanism to ensure that bodily injury and property damage compensation would be readily available within those limits.

ANI

ANI, a joint underwriting association and managing agent for a syndicate of insurers, provides third-party liability insurance to all US commercial nuclear power plants. It also administers a secondary retrospective programme established by Congress in 1976. ANI provides USD 500 million per site in primary coverage. Any damage to the public from a nuclear incident exceeding the site's USD 500 million limit is distributed equally among all 94 operating commercial power reactors. These retrospective premiums are currently capped at USD 158 million per reactor. There is also a 5% surcharge equal to USD 7.9 million per reactor that may be imposed on the retrospective premium, raising the total to USD 165.9 million per reactor. The total available compensation is USD 16.097 billion – the current limit of liability.

NEIL

The Price-Anderson Act only applies to third-party liability and not to first-party property coverage. After the Three Mile Island accident in 1979, the USNRC required all commercial nuclear power plants to carry a minimum of USD 1.06 billion in property coverage to cover the operator's obligation to stabilise and decontaminate the reactor site after an accident.[88] NEIL provides first-party nuclear property and power outage policies that insure nuclear power plants for physical losses, decontamination expenses, and costs associated with electric power generation interruptions caused by both nuclear and non-nuclear events. NEIL provides member companies with up to USD 1.5 billion per site of primary coverage and USD 1.25 billion per site in excess coverage, for a maximum property coverage level of USD 2.75 billion per site per occurrence. NEIL also provides up to USD 4.5 million per reactor per week in power interruption coverage, with a coverage limit of USD 490 million per reactor for a nuclear outage event. The coverage starts following an initial deductible period ranging from 8–26 weeks.

ANI, NEIL, reinsurance, and TRIP

ANI and NEIL reinsure each other and also provide/receive reinsurance from other global nuclear pools and commercial reinsurers. Notably, both ANI and NEIL offer terrorism insurance subject to TRIP. Therefore, in cases where an act of terrorism is certified, they both could be reimbursed for up to 80% of their exposed policy limits (USD 500 million in the case of ANI and USD 2.75 billion for NEIL) after application of their respective TRIP deductibles.

Source: FIO (based on published sources)

87 Federal Insurance Office 2024.
88 Comptroller General of the United States 1980.

4 Re/insurers' loss exposure

Re/insurers' loss exposure

Re/insurers' exposure to CBRN risks is complicated by potential for silent coverage, unpredictable attack dynamics, and difficulties with risk quantification.

Given prevailing insurance cover for CBRN risks, past episodes have not translated into major insured losses. A recent example is the Novichok attacks in Salisbury, UK in 2018. The incident was not designated a terrorist attack (instead the UK government concluded the Russian State was responsible[89]) and hence terrorism insurance policies were not triggered. Moreover, the bulk of the financial losses arose from the economic harm to the region in terms of denial of access, loss of attraction, and clean-up costs. These were not covered by business interruption policies that largely limited cover to business interruption losses arising from actual physical damage to the covered commercial property.[90]

Nonetheless, re/insurers must routinely reassess their exposure to CBRN incidents. This includes any scope for 'silent' coverage – where CBRN risk is not explicitly excluded and therefore could trigger claims under certain conditions. As explained in Box 8, this requires an assessment of both the likelihood of an incident occurring as well as the severity of any attack. Such considerations help re/insurers frame the scope of coverage made available, the size of individual policy limits, and the amount of capital they must set aside to cover unexpectedly large, accumulated claims.

Compared with other types of exposures, constructing reliable risk metrics for potential CBRN losses is much more complicated. Terrorist risks are not random; they are intentional, and the attack characteristics are not likely to be constant, as adversaries adjust their strategies. This means that there is often an insufficient basis for estimating the probable frequency of attacks, including CBRN attacks, relying largely on expert judgment to gauge the materiality of threats and vulnerabilities. In addition, re/insurers struggle to measure (or even clearly identify) the full costs of a CBRN attack. The severity of an incident often depends on a host of factors, which are highly uncertain and may interact in complex ways to affect the scale of potential losses. For example, the nature of the immediate target, the chosen attack vector, and even atmospheric conditions in the immediate aftermath of the attack could all influence the transmission of CBRN materials in an area and hence the number of victims.

Complex underlying drivers and limited data complicate loss estimation and exposure modelling of CBRN risks, making them difficult to assess and quantify.

Terrorism modelling, both for conventional bomb blasts and CBRN attacks, has advanced over time (see Box 8). This includes the use of a state-of-the-art 3D computational fluid dynamics (CFD) models to calibrate where and how hazardous material disburses after it is released, as well as downward counterfactual analysis – an alternative realisation of the past where things turned out much worse to provide perspectives on the frequency and severity of possible attacks.[91] However, these tools typically do not provide a comprehensive estimate of all potential economic losses from a CBRN event – including such significant losses as clean up of the agent or losses resulting from a decline in business at firms affected by the event.

89 Allen 2018.
90 Pool Re 2018.
91 RMS 2002.

Box 8: Quantifying CBRN terrorism insurance risks

Researchers often operationalise terrorism risk assessment as the product of threat, vulnerability, and consequences.[92] More specifically, threat is usually defined as the probability of an attack (A), vulnerability as the probability of an attack's success (S) given that it occurs, and consequences (C) are the losses that occur (fatalities, injuries, direct and indirect economic impacts, among others) given a successful attack. That is:

$RISK = Prob(A) \times Prob(S|A) \times C$

The same framework can be applied when thinking about CBRN terrorist incidents, although compared with conventional attacks, uncertainties around each of the three elements are arguably even more pronounced.

Likelihood of an attack

The sparse history of CBRN attacks means that the frequency of past incidents alone is unlikely to be a meaningful measure of probability. Moreover, even with more comprehensive data, previous episodes might not be a good guide to the future, not least because quantifying the probability of a CBRN attack requires knowledge about the motivations, intent, and capabilities of malicious actors, as well as the availability of the harmful material. Instead, it is common to consider possible future scenarios that could occur, drawing on domain expertise, for example, from the intelligence community and academia.

It is important though that such scenarios are plausible. Whilst thinking through worst case outcomes can sometimes be helpful in stress testing different balance sheets, loss estimates must still be realistic. It is always possible to design a scenario that generates extreme catastrophic losses, but if the scenario is so unlikely it is difficult to know how much weight (if any) to place on the resulting estimated losses. Hence, modellers must guard against excessive pessimism. Peer review is essential to build credible scenarios, including taking account of the full range of losses that might occur from different sized events.[93]

In general, smaller-scale scenarios will likely be more readily achievable and realistic given the complexity involved in executing large-scale attacks. It may be possible to approximate the entire range of outcomes by using a limited number of discrete points (as modelled by a range of scenarios for a threat). While assigning probabilities to scenarios is very subjective, it can often be more informative than considering only extreme scenarios.

Vulnerabilities

If bad actors have the wherewithal to carry out CBRN attacks, expert judgment is still needed to assess how far they might succeed in causing damage and disruption. This in turn depends on the robustness of organisations that they target and the defences in place to counteract and mitigate the impact of an attack. In an increasingly digital environment, effective defence is not just having physical security safeguards in place but also adequate cybersecurity measures to prevent and frustrate attackers.

The potential target catalogue is wide. Often, modelled scenarios will focus on sites with clear links to the petrochemical or nuclear industries given the clear potential for widespread harm from such a CBRN attack. However, nefarious actors increasingly look for weaknesses in less obvious places. Radioactive materials, for example, are commonly used for medical, industrial, and research purposes and, in the hands of terrorists, even a small amount could be used to construct a radiological dispersal device, or dirty bomb, causing serious widespread harm.[94]

Consequences

In sizing the potential impact of a CBRN attack, it is important to consider all elements that may lead to a loss. These include, for example, areas of damage, areas that need to be decontaminated, and areas where access is denied for a certain period. This spatial and temporal 'footprint' of an incident will have an important bearing on the overall economic costs that might be incurred.

Depending on the nature of a chosen scenario, statistical models can help inform about the dispersal of the CBRN agent and potential for physical damage at and beyond the immediate target area. Such models can be complex, using, for example, CFD to model blast pressure and impulse, and plume models that simulate and predict how airborne contaminants spread in the atmosphere after release and measure the extent of an area affected.[95] Both CFD and plume models consider the 3D nature of buildings or cityscape of the area and can incorporate features such as wind direction, wind speed, amount of explosive, and amount of contaminant.

92 Ezell et al. 2010.
93 There is extensive literature regarding methods for eliciting uncertain probability judgments (often as probability distributions) from experts. See discussion in Hora 2007.
94 A dirty bomb uses conventional explosives to spread radioactive material.
95 Chemical, biological, and radiological events typically have a minimal blast component – unless delivered with an explosive – and the main focus is often on estimating decontamination cost. Nuclear events, in contrast, are likely to include a significant blast element.

Mapping the physical consequences of a CBRN incident into measurable economic (and insured) losses is challenging. Decontamination times and costs are particularly hard to predict, as is any government response and associated priority given to such an event. If the area impacted is large, there simply may not be sufficient expertise locally or even worldwide to tackle the issue in a timely manner, which will only extend the duration of any economic disruption.

Insurers typically make simplifying assumptions about how insurance losses might escalate, especially how long access to certain areas may be denied in the event of an evacuation or the imposition of police cordons, as well as the time taken to decontaminate. Business interruption claims are often based on observable metrics such as the extent of property damage and/or the length of any downtime. However, considerable uncertainty surrounds such cost estimates, especially when there is no physical damage because insured business interruption losses may be subject to complex policy conditions.

Source: Geneva Association and Pool Re

4.1 Modelled scenario insurance loss estimates

By careful evaluation of different scenarios, re/insurers hope to gain increased visibility on the possible size of overall insured losses that they may face and their likelihood. Such scenarios are often informed by the judgement of external experts, both about the plausibility of the threat as well as the potential scale of damage that might ensue, especially given the mitigation techniques in place to reduce the spread of harm. The following describes loss modelling results for selected scenarios proposed by experts in France and the US.

4.1.1 Dirty bomb on the Champs-Élysées in Paris[96]

The envisaged scenario involves a dirty bomb attack on premises along Paris's main commercial street, a highly populated area with high-value properties. The scenario involves a homemade dirty bomb, small enough to be carried in a backpack or launched by a drone. Since the dispersion of the contaminants mainly depends on the wind (speed and direction), several simulations were used for each scenario to test various weather conditions; however, the impact of precipitation is not studied (see Appendix 2 for more details).

TABLE 8: INSURED LOSSES FOR THE DIRTY BOMB SCENARIO BY INSURANCE CLASS (EUR MILLION)

Scenario	Residential	Commercial		Industrial		Relocation	Total
		Prop.	BI	Prop.	BI		
Champs-Elysées	807	1,938	498	5,265	1,688	479	**10,675**

Source: CCR

Table 8 summarises the estimated insured losses for the proposed scenario. These are broken down into property (prop.), business interruption (BI), and relocation losses and between residential, commercial, and industrial losses. Property losses predominate – 7,000 Parisian buildings covered by more than 36,000 insured policies require decontamination, which represents about 75% of total losses. Bodily injuries or deaths arising from the incident are not included in the scenario.

The French public-sector reinsurer Caisse Centrale de Réassurance (CCR) would absorb some of the losses incurred by private re/insurers, as would GAREAT and the French State if any apportioned losses exceeded the CCR's financial reserves to cover terrorist risks.[97] Table 9 illustrates the spread of the losses projected by the proposed scenario. CCR and the French State would cover just over half of the total insured losses while insurers and private reinsurers would each cover less

96 Scenario analysis prepared by Sina Nassiry and Corentin Gouache (CCR).

97 GAREAT reinsures terrorism for property and some related lines, with very few exclusions within two schemes on an unlimited basis by CCR and the state, without payback provisions. All industrial risks (including nuclear plants) and commercial risks above EUR 20 million are covered by the large risks scheme with a market share close to 100%. The second scheme for small and medium risks protects small insurers (joined in clusters for optimisation) for risks under EUR 20 million with a market share around 20%, and is variable according to area.

than a quarter of this total.[98] In terms of primary insurers, 82% of their estimated losses (EUR 2,599 million) are due to small and medium risks, which are assets with less than EUR 20 million of insured value. On the contrary, 93% of private reinsurers' share (EUR 2,306 million) is due to large risks, which are assets with more than EUR 20 million of insured value.

TABLE 9: BREAKDOWN OF INSURED LOSSES FOR THE DIRTY BOMB SCENARIO BY RISK CARRIER (EUR MILLON)

Scenario	Insured losses	State & CCR's share	Private reinsurers' share	Insurers' share
Champs-Elysées	10,675	5,770 (54%)	2,306 (22%)	2,599 (24%)

Source: CCR

4.1.2 Terrorist attacks on a US commercial nuclear power plant[99]

To illustrate the potential insurance consequences arising from a terrorist attack on a nuclear power facility, the US Treasury in a 2024 report evaluated the results of two types of terrorist attack – aircraft collision and nuclear sabotage – at the Indian Point nuclear power plant.

Scenario 1: Terrorist aircraft crash into a commercial nuclear power reactor

The modelled aircraft collision scenario is based on the 9/11 commercial jet hijackings and subsequent collisions with the World Trade Center towers and the Pentagon. Under the scenario, a large commercial jetliner is deliberately crashed into the containment dome of one reactor on a nuclear power plant site. The footprint of the attack has a 1,500-metre radius, destroying the reactor but not the reactor safety systems, thus preventing a large release of radiation affecting nearby populations.

Assuming this aircraft collision is declared a terrorist event, TRIP would provide coverage for 59% of the overall loss of USD 4.562 billion (after deductibles and co-pays by insurers). Private insurers (and their reinsurers) would be responsible for 16% of the losses, covering their TRIP deductibles and 20% share of the property, business interruption, and workers' compensation up to the limits of those policies. The remaining 25% of the loss would be uninsured.

TABLE 10: BREAKDOWN OF LOSSES FOR THE AIRCRAFT COLLISION SCENARIO BY RISK CARRIER (USD MILLION)

Scenario	Insured losses	Private re/insurers' share	TRIP share	Uninsured share
Aircraft collision	4,562	730 (16%)	2,692 (59%)	1,140 (25%)

Source: FIO

98 GAREAT's share of potential losses is dispersed across the two right-hand columns of the table. GAREAT competes with private insurers (protected by private reinsurers and CCR) for coverage of risks under EUR 20 million sum insured. Thereby, GAREAT provides market coverage through various insurer clusters, the composition of which remains confidential. Accordingly, its share fluctuates depending on the scenario. For risks above EUR 20 million sum insured, GAREAT almost completely covers the French market.

99 Federal Insurance Office 2024.

Scenario 2: Nuclear sabotage of a nuclear power plant with major radioactive release

The second scenario involves an armed suicide attack on a multi-reactor commercial nuclear power plant, again styled on Indian Point. This disables the safety systems and allows a major radioactive release that lasts several days, involving 15–20% of the plant's radioactive inventory.[100] While there is considerable damage to the power plant itself as well as onsite workers (comparable to the losses in Scenario 1), most of the impact is on the communities south of the nuclear power plant. The plume is assumed to spread with high radiation levels 50 miles to the south over large population centres. This causes widespread contamination, radiation illnesses, major disruption of business activities, and related insurance claims.

As shown in Table 11, the projected property and workers' compensation losses total USD 245.9 billion, with only 0.4% being covered by insurance and private reinsurance, and 1.4% by TRIP. After TRIP's coverage, the retrospective coverage arrangements required under The Price-Anderson Act would respond to the next portion of the losses up to the USD 16.1 billion statutory limit of liability (see Box 7) or 6.5% of the loss. Given that standard P&C policies typically, although not always, exclude CBRN risks, the remaining 91.7% of losses will likely be uninsured. However, The Price-Anderson Act has a provision where the federal government, with congressional approval, would fully and promptly compensate all claims above the Act's aggregate limit of liability.[101]

TABLE 11: BREAKDOWN OF LOSSES FOR THE SABOTAGE SCENARIO BY RISK CARRIER (USD MILLION)

Scenario	Insured losses	Private re/insurers' share	TRIP share	Retrospective assessment share	Uninsured share
Sabotage	245,900	984 (0.4%)	3,443 (1.4%)	15,984 (6.5%)	225,490 (91.7%)

Source: FIO

In summary, both nuclear power plant scenarios would generate significant losses, but these would be materially larger if the footprint of the attack extended well beyond the immediate site. In such a case, the scale of residual losses that would fall to the US government would increase substantially.

4.2 Beyond better risk models

Ultimately, there are limits to quantifying CBRN risks given the impossibility of fully anticipating all possible outcomes and ambiguity surrounding the likelihood and/or severity of an event. Despite these challenges, there may be ways to extend the scope of available insurance while remaining within the envelope of insurability. This is especially the case if existing risk-sharing arrangements, including the role of governments in providing backstop finance, can be improved to help narrow existing coverage gaps. In this way, risks may be transferred away from those less able to cope with the economic fallout from a major CBRN incident to those with more expertise and stronger balance sheets to absorb potentially large-scale losses. Greater scrutiny by external insurance carriers would also provide an additional set of actors with an incentive to pressure users of CBRN materials to upgrade their security.[102]

Improved risk-sharing and public backstops could expand the insurability of CBRN risks and strengthen security incentives.

In drawing overall conclusions, the final section briefly explores future directions for upgrading CBRN risk management frameworks.

100 Precedents include a left-wing commando raid on the Atucha nuclear power plant north of Buenos Aires in 1973, and several Basque separatist attacks on nuclear power plants in Spain during the late 1970s, although neither of these attacks resulted in a major radioactive release.
101 USNRC 2021.
102 Pomper 2014.

5 Conclusions and recommendations

Conclusions and recommendations

Strong public-private risk-sharing is essential to narrow the protection gap for CBRN risks and minimise economic disruption from any future incident.

While CBRN terrorism events have thankfully remained rare, the evolving threat environment, including the appearance of new perpetrators and their ability to deploy new technologies, cautions that a wave of CBRN violence could be on the horizon. Should that risk crystallise in a major incident, a significant share of economic losses may not be covered by insurance. This gap can ultimately leave innocent victims facing significant financial hardship, place significant burdens on the resources of national governments, and trigger possible systemic disruption to the global economy.

CBRN terrorism remains rare but future attacks could cause large uninsured losses, strain governments, and disrupt the global economy.

What can policymakers, IFTRIP pools, and the global re/insurance industry do to improve CBRN risk management, reduce the economic impacts of potential future CBRN terrorist events, and narrow the implied protection gap?

Private insurers' balance sheets alone are ill-placed to deal with such risks. The scale of possible accumulated claims – across policyholders, geographies, insurance lines etc. – are simply too large and/or uncertain for re/insurers to sensibly underwrite. Hence, significant risk sharing with governments is crucial.

There is unlikely to be a unique way to structure a PPP to underwrite CBRN terrorism risks.[103] This is not least because individual governments will determine how far they are willing to recognise such contingent liabilities ex ante rather than deal ex post with the fallout of a CBRN incident. Risk financing and transfer solutions that may be workable and enjoy support in one country may not be realistic in another.

Nonetheless, there may be lessons to learn from existing risk-sharing insurance schemes about what might work well in managing CBRN terrorism exposures. Three areas in particular stand out.

5.1 Develop best practices among IFTRIP members

Some national terrorism pools and their governments appear to be better prepared than others. For example, special provisions implemented by IFTRIP members, such as CBRN risk protection for workers' compensation and fire-following coverage (US), mandatory take-up in some circumstances (France and Spain), and coverage of nuclear plants in some countries, show that critical political support can be mustered to expand CBRN insurance when national programmes come up for renewal. Having such arrangements in place before a CBRN event happens brings much needed clarity to insurance contracts, especially in terms of the scope and interpretation of policy exclusions/endorsements, In turn, this reduces the potential for coverage disputes and unanticipated liability for re/insurers and governments.

Some existing PPP schemes may offer guidance on how best to extend coverage to include CBRN terrorism risks.

Similarly, the recent issuance of placements by Pool Re and GAREAT of alternate funding mechanisms like ILS and catastrophe bonds demonstrate the appetite

103 One of the current major difficulties is that risk managers, policymakers, insurance supervisors, and rating agencies generally do not consider potential large CBRN scenarios in their projections.

of financial investors to assume peak terrorism risks. Suitably designed, future transfer arrangements for CBRN risk might be developed to tap the deeper risk-absorbing capacity of capital markets alongside traditional re/insurance.

Expanding CBRN coverage requires political will, capital market innovation, and better risk modelling across national terrorism pools.

More cooperation among IFTRIP pools, especially regarding formal modelling of CBRN risks, could also increase capital availability for underwriting CBRN terrorism. In some cases, national terrorism re/insurance pools, including Pool Re in the UK, US TRIP, and CCR in France, use modelling tools to evaluate the possible losses from both conventional and CBRN terrorist attacks. However, not all re/insurers or national re/insurance pools have access to modelling tools or trained personnel to run and evaluate the modelled results. IFTRIP could sponsor CBRN terrorism risk modelling education and training, and those national pools which have developed such tools could provide modelling support for those pools that do not.

5.2 Explore expanded international reciprocation arrangements

Existing mechanisms for risks faced by nuclear power plants expressly allow for international risk sharing. Given the potential cross-border spillover from a variety of CBRN terrorism incidents, it makes sense to investigate whether similar mutualisation arrangements could be put in place for risks arising outside of the nuclear power sector.

In the current conjuncture, the adoption of a full inter-pool reinsurance scheme for CBRN terrorism risks might be politically challenging. The lack of standardised terrorism definitions and disparate CBRN coverage across the pools would also need to be overcome. Nevertheless, further international cooperation and engagement in this direction will only serve to make national pooling arrangements better prepared, including sharing risk response and mitigation information that might be useful in the event of a CBRN incident.[104] It might also help catalyse moves to harmonise terrorism definitions and coverage. In turn, this will provide the foundations for collective resilience benefits across all member countries.

Greater international cooperation on CBRN risks could strengthen national pools and lay the groundwork for future cross-border risk-sharing frameworks.

5.3 Strengthen dialogue between re/insurers and international policymakers

CBRN risk management has been the focus of many conventions, agreements, frameworks, and guidelines negotiated through international organisations like the UN, the IAEA, the International Maritime Organization, and the OECD, as well as regional organisations such as the EU, the Organization of American States, and the Association of Southeast Asian Nations. But re/insurance has not always been a central consideration, or at least re/insurers have not always had a prominent role in discussions.

Active engagement from re/insurers in global CBRN policy discussions would help improve risk management understanding and strengthen disaster preparedness.

IFTRIP members, on a multilateral or unilateral basis, could therefore engage proactively with some of these organisations with a view to encourage increased involvement of terrorism pools and the global re/insurance community in future discussions involving CBRN and other man-made disaster risk management. This would promote better understanding within the international policymaking community on how insurance can help evaluate and manage potential catastrophic risk, including the emerging threat of the use of CBRN weapons by VNSAs.

The International Nuclear Pools Forum, through re/insurance and convention interactions, provides a potential model for IFTRIP member countries to further collaborate on CBRN terrorism risk, safety guidelines, claims processing, emergency response, and potentially inter-pool reinsurance agreements. They could also engage with governments and international agencies in the negotiation and adoption of a CBRN international convention or other conventions that could reduce the risk of a CBRN terrorism event and associated potential catastrophic economic and re/insurance losses.

104 Such an initiative to leverage the insights from the nuclear insurance sector for designing effective international reciprocation arrangements for terrorism pools could build on and extend the cooperation and dialogue between IFTRIP and the International Nuclear Pools Forum which started informally in 2018.

Appendix 1 – Nuclear Threat Initiative Security Scores

The NTI regularly assesses global nuclear and radiological security across 175 countries and Taiwan. It uses a scoring system, with a higher score indicating better security. The NTI evaluates three areas of vulnerability: theft, sabotage, and the RSSA. In addition, in collaboration with the Johns Hopkins Center for Health Security and the EIU, the NTI publishes the Global Health Security Index – an assessment of global health security capabilities in 195 countries.

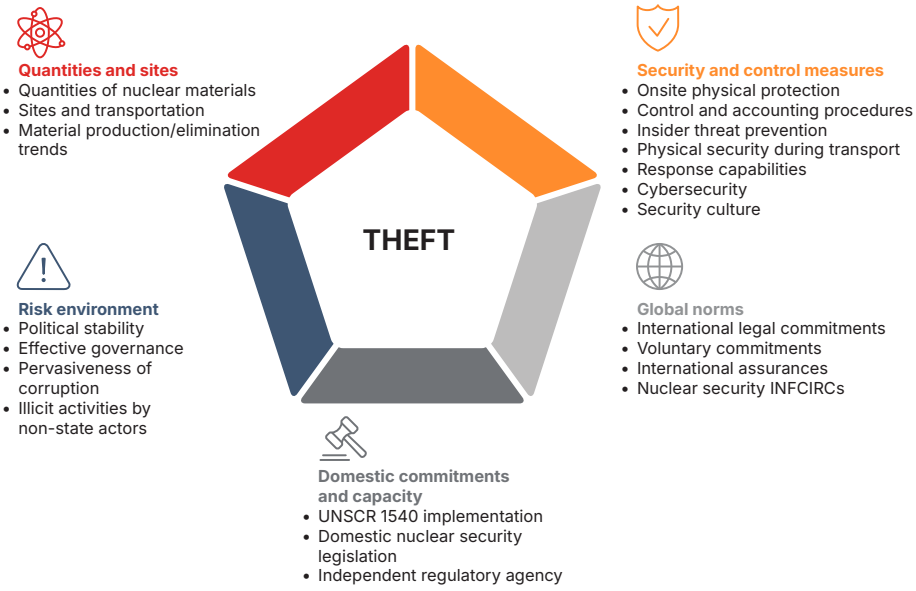
The NTI Index

The main index comprises three assessment rankings and is underpinned by contributions from an international panel of experts. Two theft rankings assess nuclear security conditions with respect to securing nuclear materials and supporting global nuclear security efforts, and a sabotage ranking assesses nuclear security conditions with respect to protecting nuclear facilities.[105]

As shown in Figure 11, NTI's Theft: Secure Materials ranking assesses countries with weapons-usable nuclear materials based on five categories – quantities of weapons-usable nuclear materials and number of sites, nuclear security and control measures, support for global norms, actions to implement international commitments, and a country's risk environment. Its Theft: Support Global Efforts ranking assesses nuclear security conditions in 153 countries and Taiwan with less than 1 kilogram of or no weapons-usable nuclear material based on a subset of the categories in Figure 11. Although these countries have no weapons-usable nuclear materials to secure, they do have a responsibility to prevent smuggling and trafficking of nuclear materials in and across their territories. Thus, the presence of terrorist groups capable of stealing nuclear materials also poses a global and regional risk.[106]

The NTI Index also factors in a ranking assessing the security conditions at nuclear facilities in 46 countries and Taiwan protecting against sabotage attacks. As shown in Figure 12, the index considers policies, actions, and other factors related to protecting nuclear facilities against the risk of sabotage. Its categories are similar to those in the Theft: Secure Materials ranking with extra emphasis on the number of sites, security and control measures (e.g. physical protection, insider threat prevention and cybersecurity), and compliance with global norms such as hosting the IAEA missions that offer peer review of nuclear security arrangements.

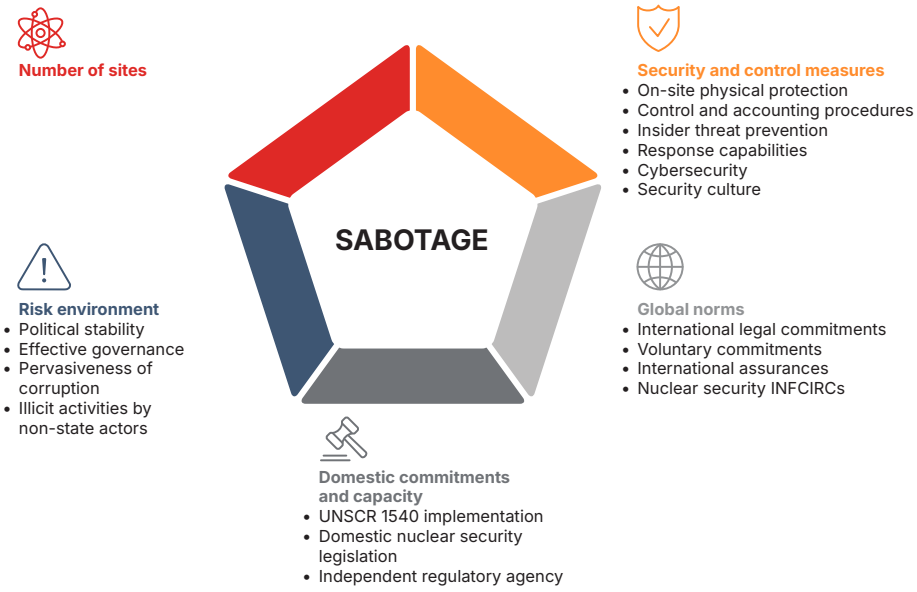
FIGURE 11: THEFT SECURE MATERIALS CATEGORIES



Source: NTI

105 NTI 2023a.
106 Ibid.

FIGURE 12: SABOTAGE PROTECT FACILITIES CATEGORIES

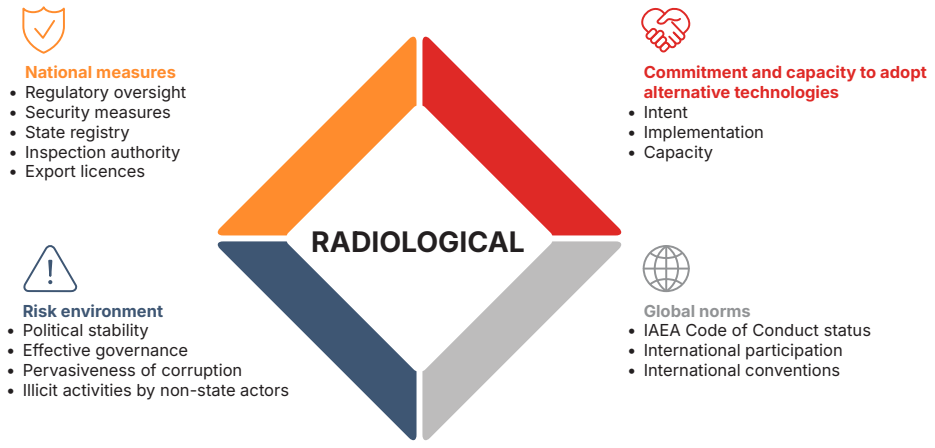


Source: NTI

Radioactive Source Security Assessment (RSSA)

The NTI Index also includes an RSSA that evaluates, but does not score or rank, national policies, commitments, and actions to secure radioactive sources and prevent dirty bombs in 175 countries and Taiwan. As shown in Figure 13, the RSSA assesses countries and areas on radiological security based on four categories. Like the Nuclear Security Index Theft and Sabotage assessments, the RSSA includes categories on country/area adherence to global norms and the overall risk environment. The other two categories focus on national measures enacted by the government to manage radiological materials, and commitment and capacity to adopt alternative technologies which would reduce the need to use radiological materials.

FIGURE 13: RADIOACTIVE SOURCE SECURITY ASSESSMENT CATEGORIES



Source: NTI

Global Health Security Index

The GHS Index is based on key indicators about biosecurity capacities – including those related to national tracking of dangerous pathogens, biosecurity training and practices, personnel vetting, regulating access to sensitive locations, and the secure and safe transport of infectious substances – and biosafety capacities such as the implementation and enforcement of laws and regulations for the oversight of dual-use technologies and monitoring of the sale of synthesised DNA, as well as relevant capacity measurements to prevent the potential use of biological agents by VNSA actors.

Appendix 2 – Detailed dirty bomb loss scenario (France)

Methodology

The estimation of insured losses caused by a dirty bomb attack is based on three modules: hazard, vulnerability, and damage.

Hazard module

The goal of this part of the model is to generate a map of the concentration (in Becquerel per cubic metre, $Bq.m^{-3}$) of the radionuclide used in the dirty bomb. This is done by using the RISTER software developed by SUEZ ARIA Technologies.[107,108] This software first produces the vertical plume generated by the explosive charge of the bomb (in kg of TNT or equivalent) and distributes the initial quantity of radioactive elements (in Bq) within this plume. Then, the plume is spread in the vicinity of the explosion using the atmospheric dispersion equations. The results depend on various parameters such as weather conditions (e.g. wind direction and speed, precipitation), topography, ground roughness, interaction with obstacles (e.g. buildings), and the intrinsic behaviour of the radionuclide used (i.e. mass, friction capacity). After a while, the radionuclides in the plume spread out into the atmosphere and eventually fall back to the ground. Thus, the software proposes a dispersal map of radionuclide deposit (in $Bq.m^2$) at a chosen resolution (fixed at five metres in this study).

Simulations can be launched with the following radionuclides: ^{60}Co, ^{137}Cs, ^{131}I, ^{192}Ir, or ^{210}Po. In this study, we only focus on a single radionuclide (^{137}Cs) to be better able to compare the identified scenarios.

Vulnerability module

The vulnerability module extracts all the buildings in the impacted zone, i.e. in the concentration map obtained in the hazard module. Then, for each of these buildings, insurance policies are associated with the insured value of the given building. This insured value is split into three categories: building, contents (that were part of the 'property'), and business interruption (only for professional assets). Finally, a radionuclide's activity (in Bq) is estimated in each building by applying its surface against the deposition map.

Damage module

The last part of the model aims to determine the cost for each building by combining the effects of the vulnerability and the hazard results. This is done by using damage curves that link concentrations of the radionuclide to damage ratios according to the type of insured value: building, contents, and business interruption (one curve by type). Then, the cost of the attack for a given building and a given type is obtained by multiplying the damage ratio with its insured value. The damage ratio goes from 0 to 1 and represents the 'degree of damage' of the building from 0% to 100%. For this type of event, damage is not measured by physical destruction but represents the cost of decontamination. These curves have been defined for each type (building, contents, and business interruption) based on data from the Fukushima disaster.

It is important to note that only property damage, business interruption, and relocation losses are modelled. Estimated costs thus do not include such elements as vehicle damage, human impacts including death and bodily injury, and cascading effects such as container explosions, leaks, and contingent business interruption.[109]

This model was applied in three scenarios with different bomb locations.

- **The Champs-Élysées in Paris, near the Arc de Triomphe.** An area with many five-star hotels, jewellers, and luxury brand stores, referred to in Paris as 'the Golden Triangle' (le Triangle d'or), in this neighborhood, there is a mix of residential and commercial buildings. The bomb is composed of 1kg of TNT (or equivalent) and 100TBq of ^{137}Cs (approximatively 32g of pure product).

- **La Défense, the business centre of Paris, in front of the Grande Arche.** Comparable to any downtown area in the US or the City of London, most of the buildings are commercial and include several floors of office space. Following the Bataclan attack in November 2015 in Paris, it was reported that there were plans for a suicide attack in La Défense.[110] The scenario involves a homemade dirty bomb, small enough to be carried in a backpack. This bomb is composed of 1kg of TNT (or equivalent) and 100TBq of ^{137}Cs (approximatively 32g of pure product).

107 https://www.aria.fr/index.php
108 https://www.suez.com/fr/groupe/qui-sommes-nous/air-climat
109 Torpey 2019.
110 France24 2015.

- **Near the European Parliament in Strasbourg.** Due to the vicinity of political institutions such as the European Parliament, the Council of Europe, and the European Court of Human Rights, this attack represents a politically motivated terrorist attack. We focus on an attack carried out by a dissident terrorist group involving an explosive charge of 1kg of TNT (or equivalent) and 1,000TBq of ^{137}Cs (approximatively 315g of pure product).

Since the dispersion of the contaminants depends mainly on the wind (speed and direction), several simulations were used for each scenario to test various weather conditions. However, the impact of precipitation was not studied here.

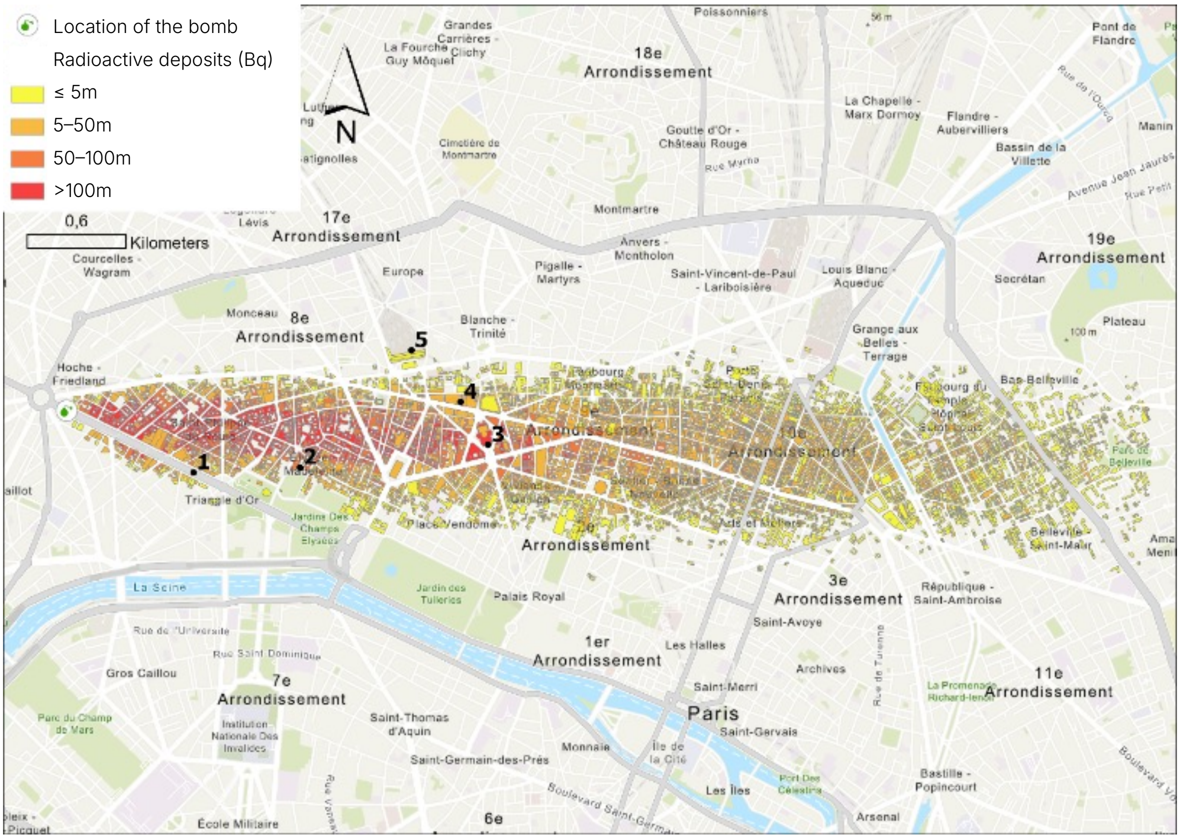
Results

Figure 14 presents the concentration of contaminants obtained in each building using the worst meteorological conditions for the Champs-Elysées.

For this scenario, over the 48 wind parameterisations tested (two wind speeds and 24 wind directions), the worst climate conditions are a wind from the west with a wind speed of 1m/s (39.4inch/s). The Arc de Triomphe is in the western part of Paris, so wind from the west impacts the most properties in the city, as observed below. For this scenario, 0.37TBq is deposited over 9.5km² (5.9mi²).

A lower wind speed impacts a smaller area, but concentrations of insured assets in this area may be higher, meaning larger damage ratios. Thus, scenarios involving lower wind speeds often lead to worse insurance losses. Easterly winds also lead to lower losses (<EUR 2 billion) due to the small amount of assets (<3,000 vs >10,000 for the other wind directions), e.g. a large part of the contaminants will be dispersed in the Bois de Boulogne where practically no insured assets are present.

FIGURE 14: CONTAMINANT CONCENTRATION (IN Bq) IN BUILDINGS FOR THE CHAMPS-ELYSÉES SCENARIO

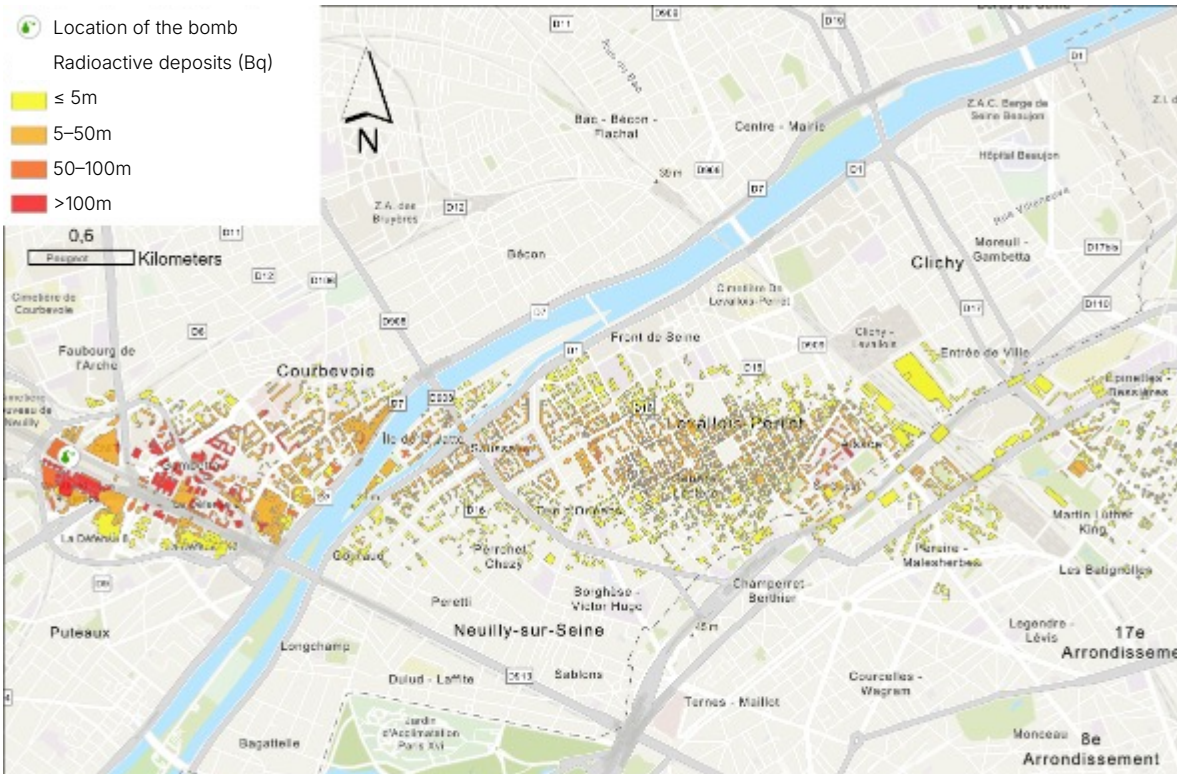


1. Champs-Elysées, 2. Élysée Palace, 3. Opéra Garnier, 4. Haussmann Department stores, 5. Saint-Lazare Railway station.
Notes: Wind speed 1 m/s; wind direction from the west; no precipitation. Results from SUEZ ARIA Technologies software.

Figures 15 and 16 present the concentration of contaminants obtained in each building using the worst meteorological conditions for the La Défense and European Parliament scenarios, respectively.

For the La Défense scenario, over the 24 wind parametrisations tested (two wind speeds and 12 wind directions), the worst climate conditions are a wind from the west and a wind speed of 1m/s (39.4inch/s). The same explanation applies as for the Champs-Elysées scenario since La Défense is in the west of Paris, as observed in Figure 15. Here, 0.26TBq of ^{137}Cs is deposited over 9.5km² (5.9mi²).

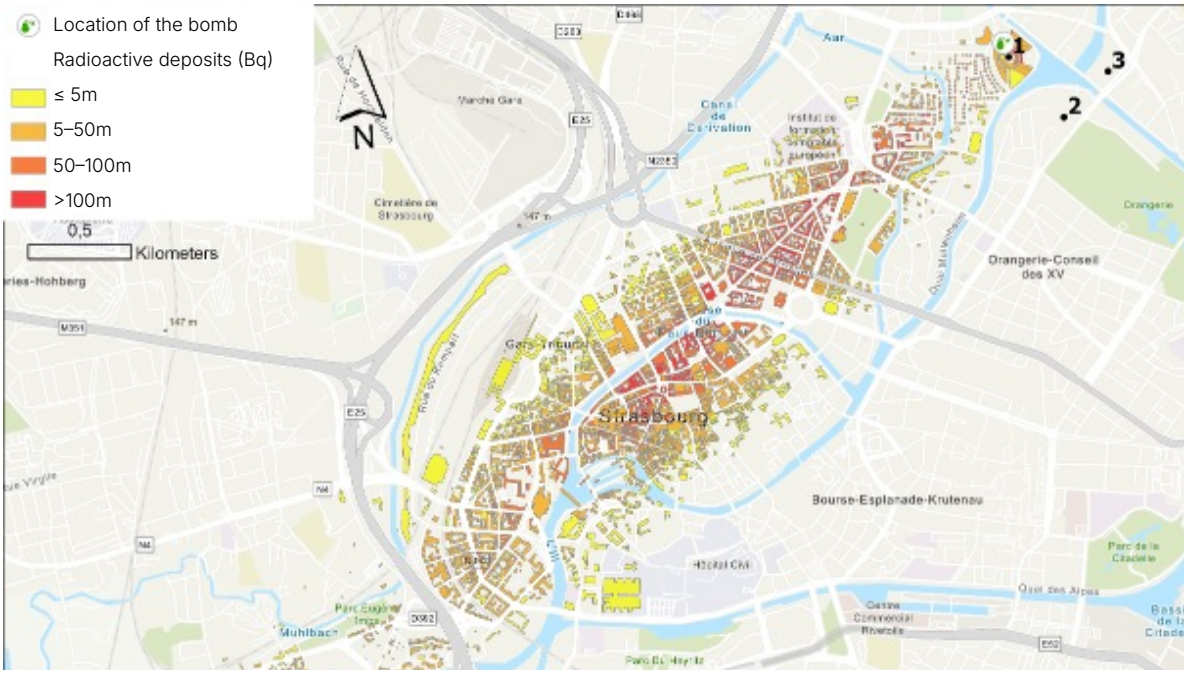
FIGURE 15: CONTAMINANT CONCENTRATION (IN Bq) IN BUILDINGS FOR THE LA DÉFENSE SCENARIO



Notes: Wind speed 1 m/s; wind direction from the west; no precipitation. Results from SUEZ ARIA Technologies software.

For the European Parliament scenario shown in Figure 16, over the 14 wind parametrisations tested (two wind speeds and seven wind directions), the worst climate conditions are a wind from the north east with a wind speed of 1m/s (39.4inch/s). As Strasbourg is to the south west of the European Parliament, a north easterly wind impacts the most assets in the city (Figure 16). For this scenario, 1.87TBq of ^{137}Cs is deposited over 7.5km² (4.7mi²).

FIGURE 16: CONTAMINANT CONCENTRATION (IN Bq) IN BUILDINGS FOR THE EUROPEAN PARLIAMENT SCENARIO



1. European Parliament, 2. Council of Europe, 3. European Court of Human Rights
Notes: Wind speed 1 m/s; wind direction from the north east; no precipitation. Results from SUEZ ARIA Technologies software.

Table 12 summarises the insured losses induced by the three proposed scenarios, broken down into property (prop.), business interruption (BI), and relocation losses and between residential, commercial, and industrial losses. For the Champs-Elysées scenario, 7,000 Parisian buildings covered by more than 36,000 insured policies require decontamination. Property losses are dominant (75%). For the La Défense scenario, since it is the business centre of Paris, many multinationals are affected, which explains the higher proportion of business interruption losses than for the Champs-Elysées scenario (25.5% vs 20.5%). In contrast, many more of the 27,000 policies affected in the Champs Elysee scenario relate to residential assets. Moreover, a large part of these residences is in the upmarket commune of Levallois-Perret. The European Parliament scenario principally induces property losses (80%) due to the proximity of Strasbourg, concentrating a large part of the 20,000 insured policies hit.

TABLE 12: INSURED LOSSES FOR THE THREE PROPOSED SCENARIOS BY INSURANCE CLASS (EUR MILLION)

Scenario	Residential	Commercial		Industrial		Relocation	Total
		Prop.	BI	Prop.	BI		
Champs-Elysées	807	1,938	498	5,265	1,688	479	**10,675**
La Défense	325	561	178	3,726	1,470	212	**6,472**
European Parliament	791	899	248	1,147	450	93	**3,560**

Regarding the average losses per claim, the Champs-Elysées scenario leads with EUR 279,000 followed by the La Défense scenario with EUR 231,000, and the European Parliament scenario with EUR 168,000. This is consistent with the mean insured value in each of the areas mainly impacted, i.e. Paris, Levallois-Perret, and Strasbourg, respectively.

To put these results into perspective, the costs obtained for each of these scenarios can be compared with natural disasters in France:

- The Lothar and Martin tempests in 1999 is considered the most expensive natural event recorded in recent French history. Costs totalled about EUR 15 billion and impacted approximately 77% of French cities. The Champs-Elysées scenario has a slightly lower cost but only impacts the city of Paris.
- The losses induced by the hailstorms of May 2022 reached EUR 5.1 billion. The event hit 50% of French cities. The La Défense scenario has a slightly higher cost while impacting only a few cities and less than 30,000 assets.
- The drought/subsidence in 2022 is the most expensive natural disaster covered under the French catastrophe scheme. Costs came to EUR 3.5 billion and impacted up to 120,000 assets. Although the losses of the European Parliament scenario are comparable, it only concerns 20,000 policies (six times lower than the drought/subsistence).

The French reinsurance pool covering terrorism helps insurance companies to cover terrorist attacks by distributing the losses induced by such acts between these insurers, private reinsurers, CCR, and the French State. Table 13 illustrates the spread of the losses induced by the three proposed scenarios. The first observation is that the higher the total loss, the higher the state and CCR's share. On the contrary, the lower the total loss, the higher the insurers' share. The high share for private reinsurers (38%) for the La Défense scenario is because many large risks (insured values ≥ EUR 20 million) are exposed that are mostly covered by private reinsurance. In fact, the priority for private reinsurers in the case of large risks is fixed between EUR 500 million (lower amounts are covered by insurers) and EUR 2.8 billion (higher amounts are covered by the state and CCR), i.e. EUR 2.3 billion.

TABLE 13: BREAKDOWN OF LOSSES OF THE THREE PROPOSED SCENARIOS BY RISK CARRIER (EUR MILLION)

Scenario	Insured losses	State & CCR's share	Private reinsurers' share	Insurers' share
Champs-Elysées	10,675	5,770 (54%)	2,306 (22%)	2,599 (24%)
La Défense	6,472	2,381 (36%)	2,438 (38%)	1,653 (26%)
European Parliament	3,560	71 (2%)	904 (25%)	2,585 (73%)

According to the French reinsurance pool covering terrorism, the French State would intervene if the CCR's share ever exceeded its financial reserves to cover terrorist risks.

References

Allen, J. 2018. The Russian State was responsible for the attempted murder...and for threatening the lives of other British citizens in Salisbury. UK Government. 14 March.

Apilado, N. 2023. Chemicals and Creeds: CBRN weapon use and religious-based terrorism. *Governance: The Political Science Journal at UNLV 7:* 1.

ARPC. 2023. ARPC Finalises 2023 Terrorism Retrocession Program.

BBC. 2023. Neo-Nazi Luca Benincasa Locked Up for Terror and Child Sex Crimes. 25 January.

Berg, A. 2021. The Internet's Relationship to CBRN Incidents by Lone Actors: A study on the evolving threat. *Master's Thesis, Johns Hopkins University.*

Bland S.A. 2013. Chemical, Biological, Radiological and Nuclear (CBRN) Casualty Management Principles. *Conflict and Catastrophe Medicine* 18: 747–770.

Broad, W. 1997. Seismic Mystery in Australia: Quake, meteor or nuclear blast? *New York Times*. 21 January.

Chemli, S., Toanoglu, M., and Valeri, M. 2024. Tourism Takes a Hit: The devastating impact of terrorism on iconic destinations. *Tourism and Hospitality Management* 30 (1): 119–131.

Cheng 2023.

CHC Global. 2023. *CBRN Risk Report: January–June*.

Comptroller General of the United States. 1980. *Three Mile Island: The Financial Fallout*.

Damveld, H. 1996. Chernobyl – 10 years after – The consequences. *Greenpeace, Chernobyl Papers No. 4.*

Dragos. 2024. *OT Cybersecurity: The 2023 year in review*.

Evans, S. 2024. GAREAT Secures €100m Athéna I Re Terrorism Cat Bond, Priced Within Guidance. *Artemis*. 21 November.

Ezell, B. et al. 2010. Probabilistic Risk Analysis and Terrorism Risk. *Risk Analysis* 30: 4.

Federal Insurance Office. 2024. *Report on the Effectiveness of the Terrorism Risk Insurance Program*.

France24. 2015. Paris Attacks Organiser 'Targeted Business District' in Bomb Plot. 24 November.

Geneva Association. 2022. *Insuring Hostile Cyber Activity: In search of sustainable solutions*. Authors: Rachel Anne Carter, Darren Pain, and Julian Enoizi. January.

Hazardex. 2019. Novichok Costs Estimated at More Than £150 million. 21 September.

Hora, S.C. 2007. Eliciting Probabilities from Experts. In *Advances in Decision analysis: From foundations to applications*, ed. W. Edwards, R.F. Miles, Jr., and D. von Winterfeldt, pp. 129–153. Cambridge University Press.

HM Government. 2021. *Global Britain in a Competitive Age: The Integrated Review of Security, Defence, Development and Foreign Policy*.

IAEA. *Nuclear Liability Laws*.

IAEA. 2022. *IAEA Safeguards Glossary*.

Integrity Initiative. 2019. The Social and Economic Impact of Chemical Weapons Attacks. *Medium*. 15 February.

James Martin Center for Non-proliferation Studies. 2014. *Mind the Gap: The role of liability and insurance regimes in strengthening radiological security*.

Kallenborn, Z. et al. 2023. A Plague of Locusts? A preliminary assessment of the threat of multi-drone terrorism. *Terrorism and Political Violence* 35 (7): 1556–1585.

Koblentz, G. 2020. Emerging Technologies and the Future of CBRN Terrorism. *The Washington Quarterly* 43 (2): 177–196.

Kumar, S. 1996. Bhopal Disaster Victims' Case Reopened. *The Lancet* 347.

Lambert, C. 2020. The Chemical and Biological Attack Threat of Commercial Unmanned Systems. *Association of the United States Army*.

Mahon. J., and Kelley, P. 1987. Managing Toxic Wastes – After Bhopal and Sandoz. *Long Range Planning* 20 (4): 50–59.

Meulenbelt, S., and Nieuwenhuizen, M. 2016. Non-State Actors' Pursuit of CBRN Weapons: From motivation to potential humanitarian consequences. *International Review of the Red Cross* 97 (899). 841.

Mihell-Hale, O. 2023. Desperate and Opportunistic: CBRN terrorists and civilian radiological material. *Journal of Strategic Security* 16 (2).

NTI. 2021. 2021 GHS Index: Advancing Collective Action and Accountability Amid Global Crisis.

NTI. 2023a. *The 2023 NTI Nuclear Security Index*.

NTI. 2023b. *2023 NTI Nuclear Security Index, Falling Short in a Dangerous World*.

NTI. 2023c. *The Convergence of Artificial Intelligence and the Life Sciences*.

NTI. 2024. International Biosecurity and Biosafety Initiative for Science (IBBIS).

Office of Budget Responsibility. 2022. Cyber-attacks During the Russian Invasion of Ukraine.

Pangi. R. 2002. Consequences Management in the 1995 Sarin Attacks on the Japanese Subway System. *Studies in Conflict & Terrorism* 25: 421–448.

Pomper, M. 2014. Mind the Gap: The role of liability and insurance regimes in strengthening radiological security. *James Martin Center for Non-proliferation Studies*.

Pool Re. 2018. *Terrorism Frequency 2/2018*.

Pool Re. 2022a. Pool Re Completes Expanded Terrorism Retrocession Placement.

Pool Re. 2022b. Pool Re Completes Successful ILS Cat Bond Placement.

Radford, A. 2023. Iranian Man Held in Germany Over Suspected Chemical Attack. *BBC*. 8 January. Ranghieri, F., and Ishiwatari, M. 2014. Learning from Megadisasters: Lessons from the Great East Japan Earthquake. *World Bank*.

Reitman, J. 2018. All-American Nazis. *Rolling Stone*. 2 May.

RMS. 2002. The Lasting Impacts of 9/11 on the Insurance Industry: A twenty-year retrospective of terrorism risk modelling.

Samet, J., and Sao, J. 2016. The Financial Costs of the Chernobyl Nuclear Power Plant Disaster: A review of the literature. *University of Southern California*.

Satyanand, T. 2008. Aftermath of the Bhopal Accident. *The Lancet* 371.

Schmalenbach, K. 2023. International Standards for National Environmental Liability Regimes. In *Corporate Liability for Transboundary Environmental Harm*, ed. P. Gailhofer et al. Springer: Cham.

Schmitt, K., and Zacchia, N.A. 2012. Total Decontamination Cost of the Anthrax Letter Attacks. *Biosecurity and Bioterrorism: Biodefense Strategy, Practice, and Science* 10 (1): 98–107.

Schmitt, K., and Zacchia, N.A. 2019. Medical Spending for the 2001 Anthrax Letter Attacks. *Disaster Medicine and Public Health Preparedness* 13 (3): 539–546.

Shrivastava, P. 1994. Technological and Organizational Roots of Industrial Crises: Lessons from Exxon Valdez and Bhopal. *Technological Forecasting and Social Change* 45 (3).

Steinhäusler, F. Et al. 1988. Chernobyl and its Radiological and Socioeconomic Consequences for the Province of Salzburg, Austria. *Environment International* 14: 91–111.

Swedish Defence Research Agency. 2024. CBRN Threats and Incidents Involving Non-state Actors – 2023 annual report.

Syahputra, A. et al. 2024. Contemporary Perspective on Terrorism: A literature review. *Journal of Management, Leadership and Educational Supervision* 9 (1): 347–366.

Tin, D. et al. 2023. A Descriptive Analysis of the Use of Chemical, Biological, Radiological, and Nuclear Weapons by Violent Non-State Actors and the Modern-Day Environment of Threat. *Prehospital and Disaster Medicine*.

Torpey, D. 2019. Contingent Business Interruption: Getting all the facts. *IRMI*.

UK Government. 2023. *Safety and Security Risks of Generative Artificial Intelligence to 2025 (Annex B)*.

United Nations Office on Drugs and Crime. 2024. Addressing the Links between Organized Crime and Terrorism. In *Global Terrorism Index 2024*.

United States Attorney's Office. 2014. Florida Man Admits Role in International Murder Conspiracy and Sale and Smuggling of Deadly Toxins.

United States Government. 2002. Pub. L. No. 107-297. Terrorism Risk Insurance Act of 2002. 116 Stat. 2322, as amended.

University of Maryland. Violent Non-State Actor Chemical, Biological, Radiological, and Nuclear (VNSA CBRN) Event Database, Version 1.0.

USNRC. 2021. The Price-Anderson Act: 2021 report to Congress. NUREG/CR-7293.

Wendling, M. 2023. Brandon Russell: Leader of neo-Nazi Atomwaffen group charged with Baltimore power grid plot. *BBC*. 6 February.

World Nuclear Association. 2021. Liability for Nuclear Damage.

World Nuclear Association. 2024. Fukushima Daiichi Accident.


INSURANCE FOR A BETTER WORLD
www.genevaassociation.org