

**Project Title:** Methodology for Assessing States' Capacity for Countering the Hostile Misuse of CBRN Knowledge and Materials

**Acronym:** MASC-CBRN

**Reference:** 860679

**Call:** ISFP-2018-AG-CT-PROTECT

**Consortium:** Center for the Study of Democracy (CSD), Bulgaria  
Hochschule für den Öffentlichen Dienst in Bayern (BayHfoD), Germany  
Kentro Meleton Asfaleias (KEMEA), Greece  
Ibatech Tecnologia SL (IBATECH), Spain  
Gobierno Vasco – Departamento Seguridad (ERTZ), Spain

**Work Package:** CBRN risk mapping (WP 2)

**Deliverable:** D2.7 - Integrated directory on the CBRN risk spectrum

**Acknowledgement:** The authors' team would like to thank the members of the Evaluation and Monitoring Panel (EMP) set up as part of the MASC-CBRN initiative for the comments and suggestions provided at an earlier version of this report.



*This document was funded by the European Union's Internal Security Fund – Police. The content of this document represents the views of the author only and is their sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.*



## Table of Content

<b>Executive Summary .....</b>	<b>4</b>
<b>1 Preface .....</b>	<b>5</b>
1.1 Internal Security Fund Police (ISFP).....	5
1.2 MASC-CBRN Initiative .....	6
<b>2 Introduction .....</b>	<b>8</b>
<b>3 Methodology.....</b>	<b>9</b>
<b>4 CBRN Risk Spectrum .....</b>	<b>10</b>
4.1 Types of CBRN Risks .....	10
4.1.1 European context.....	10
4.1.1.1 Rapid and horizontal diffusion of CBRN-related knowledge and materials.....	10
4.1.1.2 Scientific and technological advancement in fields related to CBRN .....	11
4.1.1.3 Emerging nexus between crime and terrorism.....	12
4.1.1.4 Pandemic impact on terrorism .....	12
4.1.1.5 EU response to terrorism.....	14
4.1.2 Literature Review.....	16
4.1.3 Risk Perceptions.....	23
4.1.3.1 Chemical Risk Perceptions .....	23
4.1.3.2 Biological Risk Perceptions .....	24
4.1.3.3 Radiological/ Nuclear Risk Perceptions.....	25
4.1.4 Risk Sources.....	25
4.1.4.1 Potential Chemical Risk Sources .....	25
4.1.4.2 Biological Potential Risk Sources .....	26
4.1.4.3 Radiological/ Nuclear- Potential Risk Sources .....	27
4.1.5 Risk Factors .....	27
4.1.5.1 Factor per category of risk .....	27
4.1.5.2 Incentive and Potential factors .....	28
4.2 CBRN Risk Trajectories.....	30
4.2.1 Scientific and technological landscape .....	30
4.2.2 Risk Trajectory.....	33
4.2.2.1 Inception.....	33
4.2.2.2 Access to CBRN Materials and Information.....	33





4.2.2.3	Illicit trafficking of CBRN Materials .....	35
4.2.2.4	Unravelling CBRN attack plots .....	36
4.2.2.5	CBRN risk preparedness and response .....	36
<b>5</b>	<b>Conclusions and key points.....</b>	<b>39</b>
5.1	Conclusions .....	39
5.2	Key Points .....	40





## Executive Summary

---

Report D2.7 “Integrated directory on the CBRN risk spectrum” presents the results of the activities carried out as part of WP2, *CBRN Risk Mapping* within the framework of project *MASC-CBRN: Methodology for Assessing States’ Capacity for Countering the Hostile Misuse of CBRN Materials and Knowledge*. The MASC-CBRN project is funded by the EU’s Internal Security Fund – Police.

The results of the literature review, the mapping exercise, and the national surveys are combined for the development of a directory on the spectrum of CBRN risks related to the deliberate misuse of CBRN knowledge and materials in the EU context.

The report examines the types of CBRN risks and CBRN risk trajectories. The types of CBRN risks of relevance to the EU CBRN policy context are analysed in terms of perceptions, sources, and factors. CBRN risk trajectories are analysed in terms of the impact of CBRN-related scientific and technological advances, as well as the different stages of a CBRN deliberate incident from its inception to the conducting of an attack.

The report acknowledges that the CBRN risk spectrum is wide and that the trajectories of chemical, biological, radiological and nuclear risks may manifest differently.

Each CBRN category i.e. chemical, biological, radiological/ nuclear could pose a risk for the EU in a different level based on multiple factors. It is necessary to keep in mind that terrorist acts using CBRN materials could be, as any other terrorist acts, difficult to predict, could use either new technologies or old technologies in a new way, and could be very creative as indicated in relevant EU policy and strategic documents.

The prioritization of a risk assessment that is performed with appropriate tools is essential for strengthening regional, national, and international preparedness and assigning appropriate roles when faced with CBRN risks of any type. In responding to the CBRN risk spectrum, proactive thinking, synergies, and strategies, as well as resources and training are important.





# 1 Preface

---

## 1.1 Internal Security Fund Police (ISFP)

The Internal Security Fund Police (ISFP) is the instrument for financial support for police cooperation, preventing and combating crime and crisis management.

The general objectives of ISF-Police instrument<sup>1</sup> are:

- a) crime prevention, combating cross-border, serious and organised crime including terrorism, and reinforcing coordination and cooperation between law enforcement authorities and other national authorities of Member States, including with Europol or other relevant Union bodies, and with relevant third countries and international organisations.
- b) enhancing the capacity of Member States and the Union for managing effectively security-related risks and crises and preparing for and protecting people and critical infrastructure against terrorist attacks and other security-related incidents.

The ISF-Police instrument constitutes a key element of the European Commission’s policy on enhancing EU protection against the terrorist threat, including through facilitating network-building, encouraging cross-border and public-private cooperation, and strengthening capacity building.<sup>2</sup> The priority to ensure protection against chemical, biological, radiological and nuclear (CBRN) threats is considered alongside with the need for enhancing the protection of public spaces and the resilience of critical infrastructure, as well as reducing the access to explosives. Specific attention is given to emerging threats related to the rapid progress of technology: “The illegal use of advanced technologies is a considerable challenge for the EU and its Member States. As terrorists adapt and change their techniques and modi operandi, it is necessary that law enforcement agencies are equally innovative. As needs arise, the European Commission will adapt its support to the Member States in keeping up with technological advances and confronting their use for malicious purposes.”<sup>3</sup>

The call ISFP-2018-AG-CT-PROTECT is intended to support research and development concerning CBRN threats. Its objective is to support projects aiming at

- improving the protection of public spaces and other soft targets in line with the EU Action Plan to improve the protection of public spaces;
- improving protection against CBRN attacks in line with the Action Plan to enhance preparedness against chemical, biological, radiological and nuclear security risks;

---

<sup>1</sup> See [https://ec.europa.eu/research/participants/data/ref/other\\_eu\\_prog/other/home/call-fiche/isfp-call-fiche-2018-ag-ct-protect\\_en.pdf](https://ec.europa.eu/research/participants/data/ref/other_eu_prog/other/home/call-fiche/isfp-call-fiche-2018-ag-ct-protect_en.pdf), p.3.

<sup>2</sup> See [https://ec.europa.eu/home-affairs/what-we-do/policies/counter-terrorism/protection\\_en](https://ec.europa.eu/home-affairs/what-we-do/policies/counter-terrorism/protection_en).

<sup>3</sup> See [https://ec.europa.eu/home-affairs/what-we-do/policies/counter-terrorism/protection\\_en](https://ec.europa.eu/home-affairs/what-we-do/policies/counter-terrorism/protection_en).





- enhancing the capacity of Member States' authorities and other stakeholders to implement the Regulation 98/2013, including addressing CBRN-E as well as emerging threats to critical infrastructure and public spaces.

Activities that were funded under 2018 scope of “Topic 4: call for proposals on the protection of public spaces, Chemical, Biological, Radiological and Nuclear (CBRN), Critical Infrastructure Protection (CIP), explosives and explosives precursors” have as objective:

- to support projects aiming at improving the protection of public spaces and other soft targets in line with the EU Action Plan to improve the protection of public spaces;
- improving protection against CBRN attacks in line with the Action Plan to enhance preparedness against chemical, biological, radiological and nuclear security risks;
- enhancing the capacity of Member States' authorities and other stakeholders to implement the Regulation 98/2013, including the Commission Recommendation on the implementation of Regulation 98/2013 and addressing CBRN-E as well as emerging threats to critical infrastructure and public spaces.<sup>4</sup>

Expected results are to improve protection of citizens and infrastructures (both critical and public spaces) against terrorist threats, including from CBRN-E and emerging threats.

## 1.2 MASC-CBRN Initiative

MASC-CBRN: Methodology for Assessing States' Capacity for Countering the Hostile Misuse of CBRN Knowledge and Materials is a European Commission-funded initiative that aims to inform the development of an integrated approach toward CBRN risk management for strengthening the prevention of deliberate CBRN events by elucidating the regulatory, structural (organisational), and normative elements required for the effective countering of the hostile misuse of CBRN knowledge and materials at a national level.

The proposed methodology for assessing states' capacity for countering risks related to the hostile misuse of CBRN knowledge and materials is intended to serve as a guiding framework to first responders and policy officials directly involved in the governance of CBRN issues for conducting gap and needs analysis and carrying out policy monitoring.

The MASC-CBRN initiative covers several cross-cutting priority areas of relevance to national security, including defence and counter-proliferation of WMD, counter-terrorism, combatting organised crime, health security, and civil protection.

To this end, the project seeks to uncover and analyse the key factors, drivers, and trends that have an impact on enabling such hostile misuse; to review and systematically categorise the existing different pertinent regulatory and policy arrangements at an international, EU, and

---

<sup>4</sup> See [https://ec.europa.eu/research/participants/data/ref/other\\_eu\\_prog/other/home/call-fiche/isfp-call-fiche-2018-ag-ct-protect\\_en.pdf](https://ec.europa.eu/research/participants/data/ref/other_eu_prog/other/home/call-fiche/isfp-call-fiche-2018-ag-ct-protect_en.pdf), p.4.





national level; and develop practical tools for facilitating national capacity building for first responders.

MASC-CBRN is underpinned by three interconnected objectives:

- to enhance understanding of the existing and emerging risks related to the hostile misuse of CBRN knowledge and materials and identify gaps, promising practices, and intervention points for strengthening the governance of CBRN risks;
- to develop practical tools for the implementation of strategies and measures for building sustainable capacity of policy officials and first responders against the hostile misuse of CBRN knowledge and materials;
- to form a multi-stakeholder community of practice for outreach, experience exchange, and peer learning by promoting the use of ICT mechanisms for data sharing and the exchange of best practices and lessons learned regarding the management of the risks of deliberate misuse of CBRN knowledge and materials.

The framework of the MASC-CBRN project is in line with the priorities of the EU and the four Countries (Bulgaria, Germany, Greece, Spain) regarding CBRN threats and risks.

Priorities include matters such as crime and terrorism within the context of international efforts to counter illicit trafficking and smuggling of CBRN knowledge and materials, export control, border monitoring, biosafety and biosecurity. MASC-CBRN is an ambitious program designed to enhance understanding of CBRN knowledge and materials' misuse and improve the capacity of relevant stakeholders.

The initiative is implemented by a consortium of partners from Bulgaria, Germany, Greece, and Spain. The consortium features a law enforcement agency, an engineering company, an academic institution, and two research think-tanks.

Further information about the initiative is available at the designated webpage: <https://masc-cbrn.eu/>.





## 2 Introduction

WP2 in MASC-CBRN project entails the following activities: literature review, a mapping exercise, and national surveys in order to identify, describe and organise CBRN risks. The outcome documents of these activities contain information from publicly available sources, as well as input from CBRN authorities, first responders, and civil society stakeholders.

This report, D2.7 “Integrated directory on the CBRN risk spectrum” presents the results of the activities carried out as part of WP2, CBRN Risk Mapping. The integrated Directory seeks to enhance understanding of the range (spectrum) of risks related to the deliberate misuse of Chemical, Biological, Radiological and Nuclear (CBRN) materials and knowledge in the EU context. The report is not intended as a representative empirical study but rather aims to offer insights into the complexity of CBRN risks by highlighting key factors and trajectories that impact on the EU security policy.

The next section (Methodology) elucidates the conceptual and practical aspects that underpin the development of the report.

The section titled ‘CBRN Risk Spectrum’ is divided into two subsections as follows:

- **Types of CBRN Risks** subsection examines the way in which CBRN risks are framed and analysed within the **EU policy context**. Examples of documented cases related to the hostile misuse of CBRN knowledge and materials in the EU are provided. The subsection further analyses CBRN risk **perceptions, sources and factors**.
- The **CBRN Risk Trajectories** subsection examines the diverse trends and drivers that impact on CBRN risks, including the progress of science and technology. The subsection highlights the importance of a comprehensive ‘cradle-to-grave’ approach to the prevention of the deliberate misuse of CBRN materials and knowledge covering all potential stages of a CBRN deliberate incident: Inception, Access to materials and Information, Illicit trafficking of Materials, Plotting and Conducting an attack, Risk preparedness and response.

The Conclusion (Section 5) summarises the key points raised throughout the report outlining their policy implications for effective protection against deliberate CBRN events in the EU.





### 3 Methodology

This section elucidates the conceptual and practical aspects that underpin the development of the report and it provides an overview of the reports' methodology.

**CBRN Risk Spectrum** is the product of an extensive literature review as well as publicly available and non-confidential input received from the country reports from all members of the consortium. All relevant points raised, experience and knowledge shared, as well as scenarios described and analyzed in the country reports have been considered in conjunction with extensive open-source literature research, in order to produce a thorough and cohesive CBRN Risk Spectrum.

All four of the CBRN category types were examined, while addressing Radiological and Nuclear threats together due to the similarities and the relatively limited probability of a nuclear incident in comparison to the other risks. Use cases per category are listed along with relative information, in order to provide a broad yet detailed enough view of the potential threats of the CBRN spectrum in order to develop a knowledgeable, integral registry of potential threats.

The Risk Spectrum is divided into two sub-sections covering **Types of CBRN Risk** and **CBRN Risk Trajectories**. The section draws upon the outcomes of the activities that have been conducted as part of WP 2, namely:

- A 2.1 Literature review – selected cases that have been identified as part of this activity and are relevant to the EU security context have been used to illustrate the range of potential CBRN risks.
- A 2.2 Mapping of the science and technology landscape with relevance to CBRN – the impact of key themes that have been identified as part of the mapping exercise is discussed with regard to the trajectory of CBRN risks.
- A 2.3 National surveys – the results of the four country reports have been taken into account in the analysis of risk perceptions, factors, and sources.

CBRN Risk Trajectory further examines the different stages of a potential CBRN deliberate incident from its beginning (Inception) all the way to its manifestation.

The country scenarios mentioned above are confidential and cannot be disclosed outside of the MASC-CBRN consortium. A total of 27 scenarios were examined as part of the national surveys: 13 scenarios addressing chemical risks, 8 scenarios addressing biological risks, and 6 scenarios addressing radiological/nuclear risks.





## 4 CBRN Risk Spectrum

This section outlines information relevant to the main types of risks related to the hostile misuse of CBRN knowledge and materials. The analysis exclusively focuses on the prevention of the risk of deliberate misuse of CBRN knowledge and materials regardless of whether this risk is posed by a State or non-State actor. Nevertheless, this analysis should be considered in conjunction with the all-hazard approach to CBRN risks, whereby risks arising from natural causes (e.g. incidents as a result of disasters) or accidents are also addressed. The underlying assumption is that strengthening protection against deliberate CBRN risks will have direct implications for the prevention and response to naturally occurring and accidental CBRN risks.

The **CBRN risk spectrum** is presented in two sections. The first presents Types of CBRN Risks and the second, CBRN Risk Trajectories.

### 4.1 Types of CBRN Risks

#### 4.1.1 European context

This part examines how CBRN risks are framed within the EU context. As indicated the MASC-CBRN GA, in analyzing the enabling factors of the hostile misuse of CBRN knowledge and materials, WP 2 focuses on three primary thematic areas, namely: 1) Rapid and horizontal diffusion of CBRN-related knowledge and materials; 2) Scientific and technological advancement in fields related to CBRN raising dual-use issues; and 3) the emerging nexus between crime and terrorism. In addition, the impact of the COVID-19 pandemic on terrorism and the EU general policy framework for terrorism response is examined.

##### 4.1.1.1 Rapid and horizontal diffusion of CBRN-related knowledge and materials

As far as the rapid and horizontal diffusion of CBRN-related knowledge and materials is concerned, the EU P2P (Partner to Partner) Programme for dual-use goods contributes to Chemical, Biological, Radiological and Nuclear (CBRN) risk mitigation and, as such, it is associated with the EU's Chemical Biological Radiological and Nuclear Risk Mitigation Centres of Excellence (EU CBRN CoE).<sup>5</sup> The EU CBRN Centres of Excellence Initiative (“the Initiative”), managed by the Directorate-General for International Cooperation and Development (DG DEVCO), is the main but not the only scheme for mitigating CBRN threats from outside the EU. DG DEVCO carries out other mitigating actions which include the reinforcement of export control systems in dual-use items (CBRN material with both civilian and military applications) and the reorientation of scientists having dual-use technology knowledge<sup>6</sup>. Measures to strengthen dual-use trade controls at export are also required for

---

<sup>5</sup> See <https://ec.europa.eu/jrc/en/research-topic/chemical-biological-radiological-and-nuclear-hazards/eu-p2p-outreach-programmes-export-control/dual-use-goods>.

<sup>6</sup> See <https://op.europa.eu/webpub/eca/special-reports/cbrn-14-2018/en/>.





preventing potentially malicious actors (state and non-state) to access dual-use / CBRN items through trade<sup>7</sup>.

#### 4.1.1.2 Scientific and technological advancement in fields related to CBRN

Scientific and technological advancement in fields related to CBRN offers prospects for human betterment but also new opportunities for criminals and terrorists. The illegal use of advanced technologies is a considerable challenge for the EU and its Member States.<sup>8</sup> The 2020 Europol report states that the handling and containment of biological agents has been a challenge for terrorists.<sup>9</sup> Nevertheless, technological advances along with knowledge shared online have reduced these barriers. In addition, the report highlights the following points:

- During 2019, a pro-IS group launched a campaign via a cloud-based instant messaging service promoting the use of biological weapons. Some of the content provided instructions on how to produce biological weapons and suggested how and where to deploy them.
- No incidents using radiological isotopes for terrorist purposes were reported in 2019. However, stolen or lost nuclear and radioactive materials, known as ‘out of regulatory control’, continued to be a long-standing global concern.
- Criminals continued to attempt to exploit the illicit demand for nuclear and radioactive materials. In such cases they claimed to be able to supply non-existent radionuclides or misrepresented the nature or quantity of the trafficked material. In December 2019, for example, a joint Austrian – Moldovan operation led to the arrest of an individual claiming to be smuggling radiological materials<sup>10</sup>.

The EC Action Plan highlights that it should be noted that whilst the term CBRN is used, the likelihood of a nuclear-weapon attack by any non-State actor is considered lower than that of chemical, biological or radiological attacks<sup>11</sup>.

According to Interpol, “the threat from bioterrorism is real, with current reports indicating that individuals, terrorist groups and criminals have both the capability and intention to use biological agents to cause harm to society. Access to knowledge and data is also increasingly

---

<sup>7</sup> See Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Action Plan to enhance preparedness against chemical, biological, radiological and nuclear security risks, COM/2017/0610 final, <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52017DC0610>, 2017, p.6

<sup>8</sup> See [https://ec.europa.eu/home-affairs/what-we-do/policies/counter-terrorism/protection\\_en](https://ec.europa.eu/home-affairs/what-we-do/policies/counter-terrorism/protection_en).

<sup>9</sup> See Europol, European Union Terrorism Situation and Trend Report (TE-SAT), 2020, European Union Agency for Law Enforcement Cooperation 2020, p.21, <https://www.europol.europa.eu/activities-services/main-reports/european-union-terrorism-situation-and-trend-report-te-sat-2020>.

<sup>10</sup> See Europol, European Union Terrorism Situation and Trend Report (TE-SAT), 2020, European Union Agency for Law Enforcement Cooperation 2020, p.21 <https://www.europol.europa.eu/activities-services/main-reports/european-union-terrorism-situation-and-trend-report-te-sat-2020>.

<sup>11</sup> Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Action Plan to enhance preparedness against chemical, biological, radiological and nuclear security risks, COM/2017/0610 final, <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52017DC0610>, 2017, p.2.





available through the Internet, and criminals use hidden and anonymous streams of communication, such as the Darknet, to buy, sell and share data and communicate with each other. The damage caused by such an event could reach untold magnitude, causing widespread illness and death, and instilling fear and panic on a global scale.”<sup>12</sup> With the increased use of the Darknet to acquire, transfer or smuggle biological material or weapons becoming a major concern for the law enforcement community worldwide, Interpol’s Bioterrorism Prevention Unit recently introduced Project Pandora to increase capability of police and intelligence analysts to investigate bioterrorist related activities using the Darknet.<sup>13</sup> Also, in order to assist law enforcement officers to detect triggers and indicators of potential criminal activity related to the access and trade of biological and chemical materials using the Darknet, Interpol has produced a relevant manual for law enforcement use only.<sup>14</sup>

#### 4.1.1.3 Emerging nexus between crime and terrorism

As far as the emerging nexus between crime and terrorism and its pertinence to the illicit trafficking and smuggling of CBRN knowledge and materials is concerned, Europol states that in the EU, there is little evidence to suggest that a nexus between organised crime and terrorism exists on a systematic and formalised basis.<sup>15</sup> However, there are indications of a transaction-based convergence of low-level criminals and extremists, who frequently overlap socially in marginalised areas:

- Skills and experience acquired from involvement in criminal activities, such as handling weapons, avoiding detection and familiarity with violence, make criminals attractive potential recruits for terrorist organisations.
- EU Member States observed that a substantial number of terrorists have a prior criminal record, mainly in different forms of non-organised crime.
- Illicit acquisition of material resources, such as theft of weapons and documents, has been identified as directly contributing to terrorist activity.<sup>16</sup>

#### 4.1.1.4 Pandemic impact on terrorism

UNITAR, Division of Peace, states that the global COVID-19 pandemic has brought a significant threat to the safety, health and wellbeing of societies and communities around the

---

<sup>12</sup> See <https://www.interpol.int/Crimes/Terrorism/Bioterrorism>.

<sup>13</sup> See <https://www.interpol.int/en/News-and-Events/News/2018/International-experts-meet-on-potential-threat-posed-by-new-technologies>.

<sup>14</sup> See INTERPOL, Operational Manual on Investigating Biological and Chemical Terrorism on the Darknet, general manual description, as found in <https://www.interpol.int/Crimes/Terrorism/Bioterrorism>.

<sup>15</sup> See Europol, European Union Terrorism Situation and Trend Report (TE-SAT), 2020, European Union Agency for Law Enforcement Cooperation 2020, p.21, <https://www.europol.europa.eu/activities-services/main-reports/european-union-terrorism-situation-and-trend-report-te-sat-2020>.

<sup>16</sup> See Europol, European Union Terrorism Situation and Trend Report (TE-SAT), 2020, European Union Agency for Law Enforcement Cooperation 2020, p.21, <https://www.europol.europa.eu/activities-services/main-reports/european-union-terrorism-situation-and-trend-report-te-sat-2020>.





world.<sup>17</sup> In the light of the crisis, the UN Secretary-General António Guterres has recently called out for a global ceasefire and pleaded nations to focus on fighting the pandemic. Meanwhile, violent extremists across the ideological spectrum view the global pandemic as an opportunity for expansion. Relevant positive and negative trends and their impact are thoroughly analysed in the same report.

Counter-Terrorism Committee Executive Directorate (CTED)<sup>18</sup> presents the short-term impact of COVID-19 on terrorists and terrorist groups, how UN Member States' COVID-19 responses have affected or intersected with counter-terrorism and counter-violent extremism and the potential long-term impacts of COVID-19 on terrorism, counter-terrorism and counter violent extremism. The same paper aims to provide a global picture of the potential and actual impacts, while recognizing that – as with the impact of COVID-19 itself – those impacts are unlikely to be experienced consistently by all Member States or across all regions.

In July 2020, the UN Secretary General, Antonio Guterres noted in his remarks to the UN Security Council that “the pandemic also highlights the risks of bioterrorist attacks, and has already shown some of the ways in which preparedness might fall short if a disease were to be deliberately manipulated to be more virulent, or intentionally released in multiple places at once.”<sup>19</sup> He further pointed out that serious attention had to be devoted to preventing the deliberate use of diseases as weapons.

The Committee on Counter-Terrorism (CDCT), the key coordinating body for the Council of Europe activities to combat terrorism has developed the Council of Europe Counter-Terrorism Strategy for 2018-2022 focusing on prevention, prosecution and protection. The strategy is based on the Council of Europe legal framework and standards and sets out a series of actions and tools to assist Member States.<sup>20</sup> The Council of Europe notes that the Covid-19 pandemic has demonstrated the vulnerability of modern societies to viral infections and their potential for disruption.<sup>21</sup> The intentional use of a pathogen or other biological agent for the purpose of terrorism may prove highly effective and cause damage – both human and economic – on a far grander scale than “traditional” terrorist attacks, paralyzing societies for prolonged periods, spreading fear and sowing distrust far beyond those communities immediately affected. All countries are vulnerable to bioterrorism. Its damage is rapid and potentially global. It is necessary to strengthen preventive bioterrorism measures by means of competent

---

<sup>17</sup> See [https://www.unitar.org/sites/default/files/media/file/COVID-19%20and%20Its%20Impact%20on%20Violent%20Extremism%20and%20Terrorism%20Factsheet\\_0.pdf](https://www.unitar.org/sites/default/files/media/file/COVID-19%20and%20Its%20Impact%20on%20Violent%20Extremism%20and%20Terrorism%20Factsheet_0.pdf).

<sup>18</sup> See <https://www.un.org/sc/ctc/wp-content/uploads/2020/06/CTED-Paper%E2%80%9393-The-impact-of-the-COVID-19-pandemic-on-counter-terrorism-and-counter-violent-extremism.pdf>

<sup>19</sup> See <https://www.un.org/sg/en/content/sg/statement/2020-07-02/secretary-generals-remarks-security-council-open-video-teleconference-the-maintenance-of-international-peace-and-security-implications-of-covid-19-delivered>.

<sup>20</sup> See <https://www.coe.int/en/web/counter-terrorism>.

<sup>21</sup> See <https://www.coe.int/en/web/counter-terrorism/-/covid-19-pandemic-the-secretariat-of-the-committee-on-counter-terrorism-warns-against-the-risk-of-bioterrorism>.





interinstitutional intervention and effective international cooperation. The CDCT currently has no concrete evidence of a heightened risk of bioterrorist attack due to the pandemic but it continues to support Member States in strengthening preparedness for emerging threats.<sup>22</sup>

Mike Catchpole, chief scientist at the European Centre for Disease Prevention and Control (ECDC) states in EURACTIV that ECDC recognises that there is a growing concern in many sectors about a possible increase in threats of this kind.<sup>23</sup> He states that such dangers require a coherent community response but stresses that deliberate release events are unlikely to be of the same scale in terms of geographical impact as we are seeing with the current pandemic of a new respiratory virus. He further notes that the experience with COVID-19 has highlighted the importance of preparedness plans, particularly thinking about scenarios that might develop and what kinds of capacities may be needed. This really requires early alerting – sometimes those alerts do not turn into major threats – but an important principle of preparedness is early alerting on what could be potential threats, not waiting until it is clearly a known threat that could overwhelm the system. It is necessary to continue to strengthen the operational and strategic collaboration between the health sector, public health, clinical sector and other sectors, particularly in security and law enforcement.<sup>24</sup>

The Council of Europe has noted that the multiplicity and variety of the responders require an interconnection of communication systems, which are essential tools for crisis management. The training of civil security and health actors on different types of scenarios is a fundamental element in the effective implementation of a plan to combat biological attacks. The response should also include health and legal monitoring based on a common surveillance system capable of detecting suspicious cases.<sup>25</sup>

Based on the above, Covid-19 has demonstrated States' vulnerability to biological threats, including the risk of bioterrorism. Measures to prepare against deliberate attacks and respond to such threats are necessary and important and are, therefore, highlighted.

#### 4.1.1.5 EU response to terrorism

According to EUROPOL, no terrorist incidents with chemical, biological, radioactive or other nuclear (CBRN) materials were reported in 2019 in the EU but there are credible indications suggesting that terrorist groups might have the intention of acquiring CBRN materials or

---

<sup>22</sup> See <https://www.coe.int/en/web/counter-terrorism/-/covid-19-pandemic-the-secretariat-of-the-committee-on-counter-terrorism-warns-against-the-risk-of-bioterrorism>.

<sup>23</sup> See <https://www.euractiv.com/section/defence-and-security/news/has-covid-19-increased-the-threat-of-bioterrorism-in-europe/>.

<sup>24</sup> This paragraph is based on the following source: <https://www.euractiv.com/section/defence-and-security/news/has-covid-19-increased-the-threat-of-bioterrorism-in-europe/>.

<sup>25</sup> This paragraph is based on the following source: <https://www.coe.int/en/web/counter-terrorism/-/covid-19-pandemic-the-secretariat-of-the-committee-on-counter-terrorism-warns-against-the-risk-of-bioterrorism>.





weapons and are developing the knowledge and capacity to use them.<sup>26</sup> For example, the intention to carry out terrorist attacks using CBRN materials continued to appear on terrorist online forums and social media. Closed online forums were used to discuss possible moduli operandi and to share knowledge via handbooks, manuals, posters and infographics containing recipes to produce and disseminate various agents.<sup>27</sup>

The EU response to the risk of CBRN terrorism falls within the remit of the 2005 EU Counter-Terrorism Strategy. The Strategy comprises four strands of work that aim to ensure a balanced approach to countering terrorism while respecting human rights:

- Prevent people from turning to terrorism and stop future generations of terrorists from emerging;
- Protect citizens and critical infrastructure by reducing vulnerabilities against attacks;
- Pursue and investigate terrorists, impede planning, travel and communications, cut off access to funding and materials and bring terrorists to justice;
- Respond in a coordinated way by preparing for the management and minimisation of the consequences of a terrorist attack, improving capacities to deal with the aftermath and taking into account the needs of victims.<sup>28</sup>

In 2014, the European Commission published a communication document on a new approach to the detection and mitigation of CBRN-e risks which sought to “better assess the risks, to develop countermeasures, to share knowledge and best practices, test and validate new safeguards with the ultimate goal of adopting new security standards”.<sup>29</sup> The document notes that the proposed new approach will be implemented step by step, taking into account each type of threat and environment, with the aim to:

- improve the detection of risks;
- improve the usage of results of research, testing and validation;
- promote awareness raising, training sessions and exercises;
- promote Lead Country initiatives and engage with industry and other stakeholders in security;
- take into account the external dimension, when appropriate.

---

<sup>26</sup> Europol, Terrorism Situation and Trend report (TE-SAT) 2017, p. 16, available at: [www.europol.europa.eu/sites/default/files/documents/tesat2017.pdf](http://www.europol.europa.eu/sites/default/files/documents/tesat2017.pdf) . As found in Action Plan to enhance preparedness against chemical, biological, radiological and nuclear security risk states, 2017

<sup>27</sup> Europol, European Union Terrorism Situation and Trend Report (TE-SAT), 2020, European Union Agency for Law Enforcement Cooperation 2020, p20,21

<sup>28</sup> See <http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2014469%202005%20REV%204>.

<sup>29</sup> See [https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/crisis-and-terrorism/explosives/docs/20140505\\_detection\\_and\\_mitigation\\_of\\_cbrn-e\\_risks\\_at\\_eu\\_level\\_en.pdf](https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/crisis-and-terrorism/explosives/docs/20140505_detection_and_mitigation_of_cbrn-e_risks_at_eu_level_en.pdf).





The 2017 EU Directive on combating terrorism obliges Member States to ensure that “the manufacture, possession, acquisition, transport, supply or use of explosives or weapons, including chemical, biological, radiological or nuclear weapons, as well as research into, and development of, chemical, biological, radiological or nuclear weapons” are defined as terrorist offences when committed with the intent to seriously intimidate a population, unduly compel an authority perform or abstain from performing any act, or seriously destabilise or disrupt the functioning of a country or international organisation.<sup>30</sup>

The 2017 EU CBRN Action Plan notes that the EU is facing a range of terrorist threats and attacks of a violent nature, from both networked groups and lone actors and that the potential of CBRN attacks features prominently in terrorist propaganda.<sup>31</sup> The Action Plan aims to set out a more focused and coordinated approach to CBRN risk mitigation based on four priority areas of action:

- Reducing the accessibility of CBRN materials;
- Ensuring a more robust preparedness for and response to CBRN security incidents;
- Building stronger internal-external links in CBRN security with key regional and international EU partners; and
- Enhancing knowledge of CBRN risks.

The EU Security Union Strategy 2020-2025 highlights the importance of developing EU civil protection response capacities and the key role of cooperation with third countries in enhancing a common culture of CBRN safety and security.<sup>32</sup>

#### 4.1.2 Literature Review

The risk spectrum is informed by the literature review carried out within WP2 of the project. The relevant deliverable provides an overview of the literature on the historical context of the hostile misuse of CBRN knowledge and materials compiling a database of documented cases involving the deliberate misuse of CBRN knowledge and materials.

The prime objective of D2.1 Literature review activity was:

- to identify and review literature concerning the historical context of the hostile misuse of CBRN knowledge and materials; and
- to create a database of documented cases involving the deliberate misuse of CBRN knowledge and materials.

---

<sup>30</sup> See <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32017L0541>.

<sup>31</sup> See [https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20171018\\_action\\_plan\\_to\\_enhance\\_preparedness\\_against\\_chemical\\_biological\\_radiological\\_and\\_nuclear\\_security\\_risks\\_en.pdf](https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20171018_action_plan_to_enhance_preparedness_against_chemical_biological_radiological_and_nuclear_security_risks_en.pdf).

<sup>32</sup> See <https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1596452256370&uri=CELEX:52020DC0605>.





The analysis of the selected literature revealed potential CBRN threats.

The report, D 2.1 Literature Review is thematically organised.<sup>33</sup> Five indicative themes that signify different manifestations of the deliberate misuse of CBRN knowledge and materials have been selected, to build a comprehensive picture of the CBRN risk spectrum as far as non-State actors are concerned. The themes include:

- i. Physical safety and security breaches
- ii. Illicit trafficking in CBRN materials and/or information
- iii. WMD/CBRN terrorism
- iv. CBRN crimes and sabotage
- v. Cybercrime and disinformation.

Indicative case studies that have been identified during the literature review and are directly pertinent to the EU context are presented per theme below.

### **i. Physical safety and security breaches**

The theme on physical safety and security breaches covers cases related to the theft, loss, misplacement, misappropriation, and/or unauthorised possession, storage, or acquisition of CBRN knowledge and materials (Box 1).<sup>34</sup>

#### **Box 1: Theft of radioactive material**

In 2001, a nuclear reprocessing plant in Karlsruhe in western Germany was investigated for suspected breaches of internal security rules following the arrest of a man who allegedly stole radioactive waste from the plant. An employee of the plant had been under suspicion for weeks after both he and his apartment were found to have been exposed to high levels of radiation. The man's partner and her daughter were also found to have been contaminated with plutonium and had to receive medical attention. The stolen radioactive material was found buried at a disused military base near the French border. The plutonium in the Karlsruhe plant was not weapons-grade, nor was it suitable for turning into weapons-grade material. However, local radio alleged that other nuclear material had previously disappeared from the plant unnoticed and was never recovered. At the time of the incident, the plant had already been undergoing dismantling.<sup>35</sup>

---

<sup>33</sup> MASC- CBRN D2.1 Literature Review, p.2.

<sup>34</sup> MASC- CBRN D2.1 Literature Review, p.2.

<sup>35</sup> Kate Connolly, 'Inquiry into the Theft of Radioactive Waste', *The Guardian*, 16 July 2001, available at <https://www.theguardian.com/world/2001/jul/16/kateconnolly>; Hagen Hofer, *Clean-up of a Giga-Bq-Pu Contamination of Two Apartments, Contaminated by the Pu Theft at the WAK (Pilot Reprocessing Plant) Karlsruhe, Hofer & Bechtel GmbH*, available at [https://www.eu-alara.net/images/stories/pdf/program7/Session%20C/C2\\_Hoefe.pdf](https://www.eu-alara.net/images/stories/pdf/program7/Session%20C/C2_Hoefe.pdf).





## ii. Illicit trafficking in CBRN materials and/or information

The theme on illicit trafficking of CBRN materials and/or information covers cases related to the unauthorized transport, transfer, shipment etc. of CBRN materials and information (Box 2).<sup>36</sup>

### Box 2: Nuclear “black” market

In 2015, Associated Press published an investigative report on the nuclear black market in Moldova. In February that year, a smuggler offered a huge cache of deadly caesium and specifically sought a buyer from the Islamic State group. Following an undercover operation that was built on a partnership between the FBI and a small team of Moldovan investigators, a vial of caesium was recovered which ultimately proved to be less radioactive than initially advertised by the smugglers.<sup>37</sup>

States can report on a voluntary basis to the International Atomic Energy Agency (IAEA) incidents of illicit trafficking and other unauthorized activities and events involving nuclear and other radioactive material outside of regulatory control. In 2019, six Group I incidents related to trafficking or malicious use were reported to the IAEA Incident and Trafficking Database (ITDB). As of 31 December 2019, the ITDB contained a total of 3,686 confirmed incidents reported by participating States since 1993. Of these 3,686 confirmed incidents there are 290 incidents that involved a confirmed or likely act of trafficking or malicious use; 1,023 Group II incidents for which there is insufficient information to determine if it is related to trafficking or malicious use; and 2,373 Group III incidents that are not related to trafficking or malicious use.<sup>38</sup>

<sup>36</sup> MASC- CBRN D2.1 Literature Review, p2

<sup>37</sup> Desmond Butler and Vadim Ghirda, ‘AP Investigation: Nuclear Smugglers Sought Extremist Buyers’, *Associated Press*, 7 October 2015, available at <https://apnews.com/688d82738c6f4e89b9636edfbc868de6/ap-investigation-nuclear-smugglers-sought-terrorist-buyers>; Amelia Armitage and Sharon Squassoni, *Nuclear Smuggling: From Moldova to ISIS?*, 9 October 2015, Center for Strategic and International Studies, available at <https://www.csis.org/analysis/nuclear-smuggling-moldova-isis>; Alex Schmid and Charlotte Spencer-Smith, ‘Illicit Radiological and Nuclear Trafficking, Smuggling and Security Incidents in the Black Sea Region since the Fall of the Iron Curtain – an Open Source Inventory’, *Perspectives on Terrorism*, vol. 6:2 (2012), available at <http://www.terrorismanalysts.com/pt/index.php/pot/article/view/schmid-illicit-radiological/html>.

<sup>38</sup> International Atomic Energy Agency, *Incident and Trafficking Database*, 2019, available at <https://www.iaea.org/resources/databases/itdb>; International Atomic Energy Agency, ‘IAEA Database Shows Continued Incidents of Trafficking and Loss of Control of Nuclear and Other Radioactive Material’, *Press Release*, 13 February 2020, available at <https://www.iaea.org/newscenter/pressreleases/iaea-database-shows-continued-incidents-of-trafficking-and-loss-of-control-of-nuclear-and-other-radioactive-material>; International Atomic Energy Agency, ‘IAEA Incident and Trafficking Database: Incidents of Nuclear and Other Radioactive Material out of Regulatory Control’, *2020 Fact Sheet*, 13 February 2020, available at <https://www.iaea.org/sites/default/files/20/02/itdb-factsheet-2020.pdf>. See also CNS Global Incidents and Trafficking Database, *2018 Annual Report*, July 2019, available at <https://www.nti.org/analysis/articles/cns-global-incidents-and-trafficking-database/>.





### iii. WMD/CBRN terrorism

The theme on WMD/CBRN terrorism covers cases related to the illicit use of WMD/CBRN materials and information for the purpose of carrying out mass casualty politically motivated attacks (Box 3). Terrorism is treated as a separate type of criminal activity, in order to underscore the specific modus operandi of groups that engage in ideologically (including religiously) inspired politically motivated violence.<sup>39</sup>

#### Box 3: The Ricin Plot

There have been reports that individuals and groups affiliated to ISIS (the Islamic State of Iraq and Syria, Daesh) have attempted to acquire biological agents and plot attacks. In 2018, German police conducted searches in a tower block in Cologne where a Tunisian man was suspected of having kept highly toxic ricin. The operation was prompted after the police stormed the flat of a 29-year old man identified as Sief Allah H and found ricin in large quantity. Two other flats that were rented by the suspect were also searched, as well as six empty flats and some public areas in the same building. The suspect was investigated after he bought over 3000 castor beans used to extract ricin and an electric coffee grinder using his wife's online accounts. The couple followed instructions that ISIS disseminated online on how to make a ricin bomb. Both the suspect and his wife were arrested and charged with planning a biological weapon attack.<sup>40</sup>

### iv. CBRN sabotage

The theme on CBRN sabotage covers cases related to the illicit use of CBRN materials and information other than terrorist attacks, such as the misuse of CBRN materials and knowledge for immediate personal and/or financial gain, including murder and/or the infliction of bodily injury. Unlike terrorist attacks that are generally characterised with indiscriminate violence against civilians, the acts discussed in this section target specific persons and have been investigated for possible State involvement (Box 4, 5, and 6).<sup>41</sup>

---

<sup>39</sup>MASC- CBRN D2.1 Literature Review, p2

<sup>40</sup> 'Ricin Threat: Cologne Anti-Terror Police Search Flats', *BBC News*, 15 June 2018, available at <https://www.bbc.com/news/world-europe-44494010>; 'Ricin Attack Plot Trial Starts for Tunisia-German Couple', *DW News*, 7 June 2019, available at <https://www.dw.com/en/ricin-attack-plot-trial-starts-for-tunisian-german-couple/a-49097871>; Florian Flade, 'The June 2018 Cologne Ricin Plot: A New Threshold in Jihadi Bio Terror', *CTC Sentinel*, Vol 11:7 (2018), pp. 1-5, available at <https://ctc.usma.edu/june-2018-cologne-ricin-plot-new-threshold-jihadi-bio-terror/>; Justin Huggler, 'Islamist Extremist Ricin Plot Foiled by German Police', *The Telegraph*, 14 June 2018, available at <https://www.telegraph.co.uk/global-health/terror-and-security/islamist-extremist-ricin-plot-foiled-german-police/>.

<sup>41</sup> MASC- CBRN D2.1 Literature Review, p2.





#### Box 4: The case of Georgi Markov

In September 1978, Mr Georgi Markov, a Bulgarian national working as an announcer for Radio Free Europe (RFE) in the UK died of ricin poisoning. Mr Markov was allegedly jabbed with an umbrella while waiting at a bus stop in downtown London. During the autopsy, a tiny metallic sphere was located in the wound of the jab raising suspicions that the death had been caused by a pellet that contained ricin. It is suspected that the Bulgarian State Security Service and the Soviet KGB were jointly responsible for the incident.<sup>42</sup>

#### Box 5: The Skripal and Navalny cases

In March 2018, former Russian spy Sergei Skripal and his daughter Yulia were exposed to a toxic nerve agent known as ‘Novichok’ in Salisbury, UK. Both were found unconscious on a bench in the city. A police detective sergeant identified as Nick Bailey was also affected by the nerve agent whilst conducting an investigation at Skripal’s house. In the end of June, there were two more cases of ‘Novichok’ poisoning in Amesbury located not far from Salisbury. The victims were two British nationals, one of whom died in hospital about 10 days after being exposed to the agent. The couple in Amesbury likely got exposed to the chemical after picking up a perfume bottle. The same bottle was allegedly used during the poisoning of Sergei Skripal and his daughter. The highest concentration of Novichok was found at Skripal’s house. Three Russian nationals with suspected links to the Russian intelligence service were identified as the likely perpetrators of the attack against the Skripals. To date, Russia has systematically denied the allegations.<sup>43</sup>

---

<sup>42</sup> W. Seth Carus, *Bioterrorism and Biocrimes: The Illicit Use of Biological Agents Since 1900*, Working Paper, 2001, Center for Counterproliferation Research, National Defence University, Washington DC, available at <https://apps.dtic.mil/docs/citations/ADA402108>; Lajos Rozsa and Kathryn Nixdorff, ‘Biological Weapons in Non-Soviet Warsaw Pact Countries’ in Mark Wheelis et al. *Deadly Cultures: Biological Weapons Since 1945*, Harvard University Press, 2006, pp. 157-169.

<sup>43</sup> Alastair Hay, ‘Novichok: The Deadly Story behind the Nerve Agent in Sergei Skripal Spy Attack’, *The Independent*, 26 March 2018, available at [https://www.independent.co.uk/news/long\\_reads/deadly-story-behind-the-nerve-agent-in-sergei-skripal-spy-attack-russia-uk-salisbury-a8266856.html](https://www.independent.co.uk/news/long_reads/deadly-story-behind-the-nerve-agent-in-sergei-skripal-spy-attack-russia-uk-salisbury-a8266856.html); ‘Novichok: Murder Inquiry after Dawn Sturgess Dies’, *BBC News*, 9 July 2018, available at <https://www.bbc.com/news/uk-44760875>; ‘Amesbury: Novichok Found in Perfume Bottle, Says Victim’s Brother’, *BBC News*, 15 July 2018, available at <https://www.bbc.com/news/uk-44839805>; Organisation for the Prohibition of Chemical Weapons, *Salisbury Incident*, 2020, available at <https://www.opcw.org/media-centre/featured-topics/incident-salisbury>; Tanos Franca et al. ‘Novichoks: The Dangerous Fourth Generation of Chemical Weapons’, *International Journal of Molecular Sciences*, vol. 20:5 (2019), available at <https://www.mdpi.com/1422-0067/20/5/1222>.





In August 2020, Mr Alexei Navalny, a prominent Russia opposition leader fell ill during an inland flight.<sup>44</sup> After being first admitted to a local hospital, Mr Navalny was transferred to the Charite hospital in Berlin. On 6 October 2020, the Organisation for the Prohibition of Chemical Weapons (OPCW), issued a report which confirmed that biomarkers of cholinesterase inhibitor, a nerve-acting agent were found in Mr Navalny's samples and that these biomarkers had similar structural characteristics as the toxic chemicals belonging to the so called 'Novichok' family which are prohibited under the Chemical Weapons Convention (CWC).<sup>45</sup> Mr Navalny has openly accused the Russian government of an attempted poisoning.<sup>46</sup>

### Box 6: The Litvinenko case

In 2006, Alexander Litvinenko, a former officer with the Federal Security Service (FSB) in Russia (the successor agency of the KGB) was poisoned with radioactive polonium-210 and died as a result of the symptoms that he developed. Mr Litvinenko was dismissed from duty in 1998 after he made public allegations of illegal activity within the FSB. In 2000, he and his family left Russia to move to the UK where they were initially granted an asylum and later, citizenship. Mr Litvinenko was a journalist and author. He also undertook investigatory work, including preparing due diligence reports on Russian individuals and companies. Mr Litvinenko was taken to hospital in early November after feeling ill but the cause of his condition was only established twenty days later, shortly before his death. Subsequent examination of Mr Litvinenko's body and detailed testing of samples taken from it confirmed that he had died as a result of being poisoned with polonium-210. Two primary suspects were identified for the Mr Litvinenko's murder, Andrey Lugovoy and Dmitrii Kovtun with whom the victim met at a hotel in downtown London earlier on the day that he felt ill. The radioactive material was likely placed in Mr Litvinenko's teapot during the meeting at the hotel bar. The suspects were wanted in the UK for questioning but Russia refused to extradite them on constitutional grounds. According to the report of the public inquiry that was conducted in the UK, the use of polonium-210 could be regarded as a strong indicator of state involvement, since the material had to be made in a nuclear reactor.<sup>47</sup>

---

<sup>44</sup> Whilst this case was not initially included in D 2.1, as that deliverable was completed in April 2020, it has nevertheless been added in the present report given its pertinence to the EU context.

<sup>45</sup> Organisation for the Prohibition of Chemical Weapons, *OPCW Issues Report on Technical Assistance Requested by Germany*, 6 October 2020, available at <https://www.opcw.org/media-centre/news/2020/10/opcw-issues-report-technical-assistance-requested-germany>.

<sup>46</sup> 'Alexei Navalny Blames Vladimir Putin for Poisoning Him', *BBC News*, 1 October 2020, available at <https://www.bbc.com/news/world-europe-54369664>.

<sup>47</sup> Sir Robert Owen (Chairman), *The Litvinenko Inquiry: Report into the Death of Alexander Litvinenko*, 21 January 2016, available at <https://www.gov.uk/government/publications/the-litvinenko-inquiry-report-into-the-death-of-alexander-litvinenko>; 'Alexander Litvinenko: Profile of Murdered Russian Spy', *BBC News*, 21 January





## v. Cybercrime and disinformation

The theme on CBRN cybercrime and disinformation covers cases related to the use of the Internet for obtaining CBRN knowledge and materials, plotting and conducting cyber-attacks, spreading fake news, and mounting hoax attacks (Box 7).<sup>48</sup>

### Box 7: Toxin sale over the ‘DarkNet’

In April 2015, a sixteen-year old boy in the UK was given a 12-month referral order at Manchester Youth Court after he attempted to place an online order for abrin, a toxin 30 times more potent than ricin. The teenager was arrested after he tried to obtain 10mg of abrin on the ‘dark web’, parts of the internet which cannot be found by conventional search engines. The ‘sellers’ in this case were undercover law enforcement officers. In their words, the boy was troubled and vulnerable. In his guilty plea, the perpetrator asserted that he intended to buy the toxin with a view to taking his own life. It is estimated that 0.05mg of abrin is sufficient to kill a person. There is no known antidote for abrin poisoning.<sup>49</sup>

A suicide case involving toxic substance allegedly purchased on the ‘dark web’ was reported in 2014. In that incident, a 28-year old man was found dead in a hotel room after self-poisoning with cyanide illicitly obtained online.<sup>50</sup>

In June 2014, a 34-year-old Danish citizen was sentenced to three years in prison by a court in Randers, Denmark. According to the court, he had attempted to kill an unidentified person in Ukraine, and, for that purpose, he had illegally bought a small amount of the toxin abrin which is very easy to make and very poisonous. A subsequent analysis revealed that the obtained amount of the toxin would have been enough to kill between two and twenty persons. The supplier was a 19-year-old male in Florida, USA, who was selling guns and toxins via ‘Black Market Reloaded’ on the Tor network. The FBI arrested the American

---

2016, available at <https://www.bbc.com/news/uk-19647226>; John Harrison et al. ‘The Polonium-210 Poisoning of Mr Alexander Litvinenko’, *Journal of Radiological Protection*, vol. 37:1 (2017), pp. 266-278, available at <https://iopscience.iop.org/article/10.1088/1361-6498/aa58a7/>; ‘Litvinenko Inquiry: Key Findings’, *BBC News*, 21 January 2016, available at <https://www.bbc.com/news/uk-35371344>.

<sup>48</sup> MASC- CBRN D2.1 Literature Review, p2

<sup>49</sup> ‘Abrin: Boy, 16, Sentenced after Ordering Deadly Toxin Online’, *BBC News*, 20 April 2015, available at <https://www.bbc.com/news/uk-england-manchester-32383135>; for a description of abrin, see Virginia I Roxas-Duncan and Leonard Smith, ‘Of Beans and Beads: Ricin and Abrin in Bioterrorism and Biocrime’, *Journal of Bioterrorism and Biodefence*, S2:002 (2012), available at <https://www.omicsonline.org/of-beans-and-beads-ricin-and-abrin-in-bioterrorism-and-biocrime-2157-2526.S2-002.php?aid=4686%3Faid=4686>.

<sup>50</sup> G. Tournel et al. ‘Dark Web Shopping: A Case Report of a Cyanide Suicide’, *Toxicologie Analytique et Clinique*, vol. 26:2 (2014), pp. S23-24, available at <https://www.sciencedirect.com/science/article/pii/S2352007814700496>; E. Le Garff et al. ‘Cyanide Suicide After Deep Web Shopping: A Case Report’, *The American Journal of Forensic Medicine and Pathology*, vol. 37:3 (2016), pp. 194-197, available at <https://insights.ovid.com/article/00000433-201609000-00014>.





supplier in a sting operation and informed the Danish police, who arrested the Danish buyer in January 2014. The US seller identified as Mr Jesse William Korff was sentenced to 110 months in prison after it was revealed that he advertised the sale of deadly toxins, such as abrin and ricin, and provided his prospective purchasers with information about quantities necessary to kill a person of a given weight, along with instructions on how to secretly administer the toxin so as to avoid suspicion by law enforcement officials. Besides the Danish national, Mr Korff's international customers included individuals from India, Austria, and the UK. The toxins were smuggled from Florida abroad in concealed packages sent through the US Postal Service.<sup>51</sup>

The following sections present CBRN Risk Perceptions, Sources and Factors as identified within WP2.

### 4.1.3 Risk Perceptions

This part presents CBRN Risk Perceptions taking into account the research that has been carried out during WP2.

#### 4.1.3.1 Chemical Risk Perceptions

**Chemical Risks** include all potential risks originating from chemical agents that can cause harm to human life. Attacks using chemicals may aim at killing humans or animals directly (using nerve agents or other lethal substances), causing detrimental and potentially lethal trauma such as chemical burns (corrosive acids) or deformations, and damaging equipment or infrastructure.

Small to medium scale chemical attacks have been the most common CBRN weapon type utilized by terrorist groups.<sup>52</sup> Many toxic chemicals or their precursors are available on the market and while the use of many recognized harmful chemicals and their precursors is strictly regulated internationally, the extent to which existing regulations are effectively implemented and enforced in different parts of the world vary.

The Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction (the Chemical Weapons Convention or CWC) defines chemical weapons as any “toxic chemicals and their precursors, except where intended for purposes not prohibited under this Convention, as long as the types and quantities are

---

<sup>51</sup> Robert Petersen, ‘The Danish Biosecurity System’ in S. Whitby et al. *Preventing Biological Threats: What You Can Do*, University of Bradford 2015, available at <https://www.bradford.ac.uk/bioethics/> ; US Department of Justice, ‘Florida Man Sentenced to 110 Months in Prison for Conspiring to Murder a Foreign National; Sale and Smuggling of Deadly Toxins’, *Press Release*, 18 February 2015, available <https://www.justice.gov/opa/pr/florida-man-sentenced-110-months-prison-conspiring-murder-foreign-national-sale-and-smuggling>

<sup>52</sup> See <https://www.marshallcenter.org/en/publications/occasional-papers/horror-or-hype>.





consistent with such purposes”. Toxic chemicals which have been identified for the application of verification measures under the CWC are listed in Schedules contained in the Annex on Chemicals to the text of the Convention.<sup>53</sup>

Depending on their effects, chemical warfare agents are categorized as nerve, blood, blistering/ nettle and pulmonary agents. Some chemical warfare agents can be stored for great periods of time in airtight containers of appropriately resistant materials. In such containers they might be easier to transfer than bioweapons or radioactive material and possibly difficult to detect. They can be synthesized reliably in considerable quantities through repeat processes; however, most would require stable conditions and high purity yields to be considerably threatening, which are certainly difficult to achieve. Given the size and impact of the global chemical industry (e.g. pharmaceutical, metallurgical, chemical, textile, and petrochemical), the risk of industrial chemical accidents is prioritised alongside with the potential for deliberate attacks, whereby chemical safety and security considerations are addressed together.

#### 4.1.3.2 Biological Risk Perceptions

The **risk of the deliberate misuse of biological knowledge** and materials in Europe exists. The current situation with SARS-CoV2 (COVID-19) and previous disease outbreaks around the globe have demonstrated both the gravity of biological threats and the challenges to addressing such threats in an effective and coordinated manner. Biological risks, regardless of their origins affect humans, animals, and plants. As such, they are regarded as significant concerns in the areas of public health, agriculture, stock breeding, and food production, to name a few. The 1975 Biological and Toxin Weapons Convention (BTWC) prohibits the development, production, stockpiling, acquisition, and retention of “microbial or other biological agents, or toxins whatever their origin or method of production, of types and in quantities that have no justification for prophylactic, protective or other peaceful purposes.”<sup>54</sup> Yet the BTWC does not make specific provisions as regards compliance and verification. After the end of the Cold War, the risk of bioterrorism – the possibility that non-State actors could use disease as a weapon – has received considerable attention, particularly in the light of the rapid progress of the life sciences, wide availability of scientific information, and illicit online trade (e.g. via Dark Net) which reduce the technical barriers to the acquisition of biological weapons. A mass-casualty bioterrorism is generally considered a low-probability-high-impact event which requires a coordinated whole-of-community prevention, preparedness, and response approach. Fostering a reliable nation-wide system for countering deliberate biological risks has important implications for strengthening the prevention of naturally occurring diseases and disease outbreak resulting from laboratory accidents or negligence.

---

<sup>53</sup> See <https://www.opcw.org/chemical-weapons-convention>.

<sup>54</sup> See

[https://www.unog.ch/80256EE600585943/\(httpPages\)/77CF2516DDC5DCF5C1257E520032EF67?OpenDocument](https://www.unog.ch/80256EE600585943/(httpPages)/77CF2516DDC5DCF5C1257E520032EF67?OpenDocument).





#### 4.1.3.3 Radiological/ Nuclear Risk Perceptions

**Radioactive material** can be dispersed in the environment (Radiological Dispersal Device – dirty bomb) or used directly to irradiate people (Radiation Emission Device) resulting in individuals being exposed to radiation.

**Nuclear weapons** are subject to international control and regulation. Under the provisions of the Nuclear Non-Proliferation Treaty, nuclear-weapon States Parties (China, France, Russia, UK, and USA) are obliged not to transfer to any recipient whatsoever nuclear weapons or other nuclear explosive devices or control over such weapons or explosive devices directly, or indirectly; and not in any way to assist, encourage, or induce any non-nuclear-weapon State to manufacture or otherwise acquire nuclear weapons or other nuclear explosive devices, or control over such weapons or explosive devices.<sup>55</sup> Non-nuclear-weapon (NNW) States Parties are obliged not to manufacture or otherwise acquire nuclear weapons or other nuclear explosive devices; and not to seek or receive any assistance in the manufacture of nuclear weapons or other nuclear explosive devices. NNW States Parties are further obliged to accept safeguards for the exclusive purpose of verification with a view to preventing diversion of nuclear energy from peaceful uses to nuclear weapons or other nuclear explosive devices.<sup>56</sup> To date, India, Pakistan, and Israel have neither signed nor ratified the Treaty and North Korea (DPRK) formally withdrew from it in 2003.<sup>57</sup> The risk of accidents on nuclear power plants has been demonstrated by the Three Mile Island accident in 1979 in the USA, the Chernobyl accident in 1986 in the former USSR (present-day Ukraine), and the Fukushima accident in 2011 in Japan. Along with this, there is the risk that terrorists may obtain fissile material or sabotage nuclear facilities with leaks or explosions resulting in a wider contaminated area with longer lasting effects not only on people, but also on the environment.<sup>58</sup>

#### 4.1.4 Risk Sources

This chapter presents CBRN Risk Sources taking into account the work that has been carried out in WP2.

##### 4.1.4.1 Potential Chemical Risk Sources

**Chemical hazards** originate from elements or compounds of chemical nature. Toxic chemicals can be found either in natural or processed state. Exposure to such substances either by inhalation, ingestion or contact with the skin can result in health consequences that vary from illness and injury to death. The range of consequences depends on the type of substance, the amount of substance and the timeframe and duration of the exposure.

Due to their potential magnitude in terms of scale and impact, industrial chemical accidents are considered within the framework of potential CBRN threats. Chemical accidents may arise during the production and/or handling of chemical substances in enterprises in the

---

<sup>55</sup> See <https://www.un.org/disarmament/wmd/nuclear/npt/text>.

<sup>56</sup> See <https://www.un.org/disarmament/wmd/nuclear/npt/text>.

<sup>57</sup> See <https://fas.org/nuke/guide/dprk/nuke/dprk012203.html>.

<sup>58</sup> See <https://www.politico.eu/wp-content/uploads/2017/11/CBRN-Final-Report.pdf>.





pharmaceutical, metallurgical, chemical, textile, and petrochemical sector. Malfunction of technological equipment of chemical infrastructures, damage to gas or oil pipelines or utilisation of explosives present augmented risk. The inappropriate storage of chemical substances may also lead to an incident, as demonstrated in the recent explosion in Beirut whereby some 2,750 tonnes of improperly stored ammonium nitrate resulted in a massive blast which caused significant damage to the Lebanese capital killing 190 people and injuring more than 6,000.<sup>59</sup>

The misuse of chemicals can be the result of oversight failures and procedural safety and security gaps. Toxic chemicals can be released through industrial leaks that pollute the environment and could cause health issues. Furthermore, accidents during the transportation of such materials (e.g. on road, railway, sea, or by air) are considered another potential risk source.

Likewise, deliberately caused incidents, such as terrorist attacks involving the dissemination of toxic chemicals can cause harm both to humans and natural environment. Harassing agents, incapacitating agents, toxic industrial and commercial chemicals and chemical toxins of biological origin (the latter also considered as part of the prohibition of biological and toxin weapons) may be used with the intention to cause harm. A variety of potential delivery methods of toxic chemicals exists. Producing a chemical warfare agent is feasible albeit demanding. As with most other CBRN agents, the type of the selected chemical agent determines the difficulty of production. Structurally simpler chemicals might be easier to produce, whilst more complex ones require intricate physicochemical processes, tailor-made equipment and often closely controlled temperature, pressure, and chemical balance conditions.

#### 4.1.4.2 Biological Potential Risk Sources

A biological hazard, or biohazard, is a biological agent (e.g. bacteria, viruses, fungi) or toxin that poses a threat to the health of humans, animals, or plants. Natural exposure or release (intentional or unintentional) of such microorganisms and toxins can cause illness and death. Biological hazards may result in severe epidemic and pandemic diseases that spread fast and cause a wide spectrum of symptoms. Depending on its incubation period, a disease can spread virtually unnoticed before its symptoms are manifested.

Biological threats include naturally occurring disease outbreaks (e.g. emerging and re-emerging infectious diseases, antibiotic resistant infections), the accidental release of biological agents or toxins (e.g. laboratory accidents, accidental leaks, negligence), and deliberately caused disease outbreaks (e.g. use of biological weapons, bioterrorism).<sup>60</sup> Biological agents and toxins have to be stored in high-containment facilities and subject to extensive physical security restrictions. The ‘insider threat’ – the possibility that an individual with legitimate access to biological agents and toxins within a facility, e.g. laboratory research

---

<sup>59</sup> See <https://www.bbc.com/news/science-environment-54420033>.

<sup>60</sup> MASC- CBRN D2.3 Country report on CBRN risks- Bulgaria, p.9.





staff, technician etc. may steal or deliberately misplace biological agents or toxins – merits specific attention in ensuring the security of biological agents and toxins.

Advances in modern life science may facilitate the development and production of bioweapons. The increased accessibility of equipment and knowledge as well as the emergence of novel techniques, such as next-generation sequencing and gene editing lower the technical barriers to modifying existing biological agents and toxins and synthesising pathogens *de novo*.

Bioterrorism can have significant impact resulting in mass casualties, economic loss (e.g. agricultural damage), environmental degradation, and a long-lasting psychological trauma. This risk needs to be considered against the backdrop of the rapid progress of biotechnology, in order to ensure that advances in the life sciences are used only for peaceful, prophylactic, and protective purposes.

#### **4.1.4.3 Radiological/ Nuclear- Potential Risk Sources**

Radiological and nuclear threats are addressed together, as both entail the threat of radiation and all its harmful consequences to human life and the environment. Radiological threats can be hard to detect, as sources may be present in small amounts and symptoms in victims may not manifest themselves immediately. Radiation poisoning may lead to death, cancers, dizziness, miscarriages, dermal burns and lesions, hair loss and more, all of which depend on the type of radiation source and the intensity and duration of exposure.

Most radioactive sources are elements or compounds that are naturally radioactive and occur in nature (or in human activities) through radioactive decay or otherwise spontaneous processes. Nuclear and radiological materials are used in nuclear power plants. In Europe, there are many nuclear power plants with active cores that could pose a risk locally and to neighbouring countries in case of an accident. Radioisotopes are also used in science, industry, and medicine (e.g. x-ray and similar technologies). Although the security requirements in such infrastructures are high, the risk of human error or negligence remains. Loss of radioactive material occurs, even in developed countries with strict protocols which highlights the risk that such material could be obtained by criminals or other actors with malign intent. Transportation of radiological sources require specific equipment to ensure safety and security, and prevent the illicit or unauthorised handling of such material. Radioactive waste and spent nuclear fuel are also subject to strict procedures for proper management.

#### **4.1.5 Risk Factors**

This part examines CBRN Risk Factors taking into account the work carried out within WP2. Factors are categorized per risk category. Potential incentives and enablers for CBRN attacks are also discussed.

##### **4.1.5.1 Factor per category of risk**

###### **4.1.5.1.1 Key factors that impact on the probability of a chemical event**

Chemical threats against critical infrastructures could affect the transport, energy, water, food, and health sectors. Such threats may also be directed at public spaces.





Chemical risks are considered high priority, due to the large amount of hazardous and toxic chemical substances that are available, the large industrial sector in which toxic chemicals find a wide application, and the potential for industrial and transport incidents. Deliberate chemical events may have significant impact in terms of casualties, destruction, and environmental contamination.

#### 4.1.5.1.2 Key factors that impact on the probability of a biological event

The risk of biological events is considered significant due to the high impact that such events could have. Key factors that impact on the level of preparedness of countries for dealing with biological events include the overall state sanitary conditions and measures in place, immunization coverage and vaccination policies, capacity for early diagnosis and disease surveillance, and the availability of infrastructure for health care provision and production and delivery of medicines. The overall impact of a biological events depends on the type, virulence, and transmissibility of the pathogen; the level of immunity of the vulnerable population; the availability of healthcare and treatment; and the early identification of the disease. Additional factors that impact on the risk of a deliberate biological attack include the level of availability and accessibility of pathogens and toxins, including the extent to which biocontainment measures at designated facilities are implemented and enforced and the extent to which relevant scientific and technological advances are monitored and assessed.

#### 4.1.5.1.3 Key factors that impact on the probability of a radiological/nuclear event

A main factor that impacts on the probability of deliberate radiological and nuclear events relates to the extent to which nuclear safety and security policies, regulations, and measures are implemented within designated facilities where nuclear and radiological materials are being handled, stored, and processed. This includes the extent to which relevant laws, regulations, and policies are in place in countries to safeguard radiological and nuclear material and the extent to which all facilities where radiological and nuclear materials are handled implement and enforce relevant rules and procedures for safety and security monitoring, control, and accountability.

#### 4.1.5.2 Incentive and Potential factors

The factors that impact on the probability of an event are diverse. The motivations underpinning terrorist attacks involving CBRN can vary from personal grievances (e.g. in the case of ‘lone wolf’ terror incidents) to perceived socio-economic injustice and political or religious considerations (e.g. far-right extremism, Islamic fundamentalism). Regional instability and protracted conflicts coupled with radical narratives could provide an enabling setting for plotting and organising such attacks, as seen in the case of ISIS in Syria and Iraq.<sup>61</sup>

---

<sup>61</sup> Stephen Hummel, ‘The Islamic State and WMD: Assessing the Future Threat’, *CTC Sentinel*, vol.9:1 (2016), pp. 18-22, available at <https://ctc.usma.edu/the-islamic-state-and-wmd-assessing-the-future-threat/>; Andrew Zammit, ‘External Operations: The 2017 Sydney Plane Plot’, *CTC Sentinel*, vol. 10:9 (2017), pp.13-19, available at <https://ctc.usma.edu/new-developments-in-the-islamic-states-external-operations-the-2017-sydney-plane-plot/>.





The issue of returning foreign fighters is particularly pertinent in this regard in the light of the continued interest of ISIS affiliates in obtaining biological and chemical weapons.

#### 4.1.5.2.1 Socioeconomic factors (Incentive)

In anticipating and preventing a CBRN attack, it is prudent to assess and consider the socioeconomic homogeneity and possible frictions within the population, whether that is on the level of a neighbourhood, a city or a country. Differences can breed friction and friction heats up tensions, which may eventually lead to an actor deciding to resort to violent means to vent desperation or establish their own ideals as superior. Socioeconomic profile is affected by numerous parameters, positively or adversely. Societal forces such as perceived injustice or deprivation may push actors to radicalization.

#### 4.1.5.2.2 Directly related factors (Potential)

This section summarises the main common factors that may facilitate a CBRN attack by a malicious actor. It examines the availability of means, both tangible and intangible which are required for a CBRN attack and of which stakeholders should be aware, in order to reduce the potential for a CBRN attack. The following factors differ significantly from country to country.

##### 4.1.5.2.2.1 Availability of necessary components

A key factor for a CBRN attack is the availability of equipment or means that are necessary for conducting an attack. The availability of a hazardous or toxic material that can be used in a deliberate incident is itself a baseline risk. This principle spans all four categories of CBRN threats, thus, the storage, operation, and circulation of such material (regardless of it being chemicals, biological agent or toxins, or radiological or nuclear material) within the territory of a country poses a risk.

Along with the availability of CBRN materials, the availability of technical expertise and components is equally important. Ready access to experienced personnel able to produce, handle, transport or weaponize a CBRN material, the availability of operational facilities that could allow scaling up production of a CBRN weapon, and technologies that allow the handling or manipulation of the CBRN material can serve as enabling factors for deliberate misuse.

##### 4.1.5.2.2.2 Probability of acquisition

The probability of acquisition – the risk of CBRN materials falling under the control of a malicious actor – is a variable that needs to be assessed.

This variable is essentially moderated by the proper planning, surveillance and control exercised by competent authorities, personnel, and stakeholders that are responsible for preventing the misuse of CBRN knowledge and materials. Biological, chemical, nuclear, and radioactive materials have a wide application in industrial and civilian activities. Reducing the probability of acquisition means that the risk of misuse is minimized at its source.

The probability of acquisition is closely related to availability: CBRN knowledge and materials need to be subject to safety and security policies, regulations, and procedures, in order to ensure that related knowledge and materials are not diverted and exploited for hostile purposes.





The probability of acquisition is also connected with motive. Individuals with relevant technical knowledge and expertise may be recruited by criminal or terrorist organisations and subsequently contribute to the ‘training’ of affiliates of extremist organisations motivated to carry out a CBRN attack. The probability of acquisition is considered higher in conflict zones and in countries with prevalence of corruption and crime where governments may not be in a position to exercise effective oversight on relevant facilities and existing stockpiles.

#### *4.1.5.2.2.3 Probability of production*

Producing CBRN material is not a trivial task; however, as the 1995 sarin attack in Tokyo has demonstrated, the possibility that a terrorist organisation may develop viable WMD exists. Nowadays, the Internet may be extensively exploited by actors with malign intent both to incite CBRN attacks and to facilitate the organisation of such attacks (e.g. via Darknet).

Regular monitoring of suspicious online activities, data and intelligence sharing, and international cooperation among relevant security and intelligence services and designated authorities can contribute to countering the multifaceted effects of online radicalisation, including the plotting and organisation of deliberate CBRN incidents in a timely and effective manner.

#### *4.1.5.2.2.4 Potential Impact*

By definition, CBRN events are considered high-impact events. The impact of a CBRN attack can be short- or long-lasting depending on the target and the type of the attack (e.g. the material or weapon that has been deployed). Possible immediate consequences may include loss of lives, economic paralysis, and environmental degradation. Long-term effects are more difficult to predict, as they depend on the scale of the attack and the level of resilience of the target. Assessing the impact of a CBRN attack plays an important part in the preparedness and response planning of relevant agencies and first responders.

## **4.2 CBRN Risk Trajectories**

### **4.2.1 Scientific and technological landscape**

The CBRN risk spectrum is conditioned by the rapidly evolving scientific and technological landscape. As part of WP2, the state of the scientific and technological landscape with relevance to CBRN has been examined, in order to identify key trends and drivers in S&T innovation that impact on the accessibility and proliferation of CBRN-related capabilities. To this end, relevant publicly available data sources were compiled and systematically categorised, to develop an indicative snapshot of the main drivers, enablers, and trends in scientific and technological innovation with relevance to CBRN fields.

The progress of modern technologies has expanded the range of potential CBRN risks. The growth of dual-use research whereby the outcomes of benignly intended science activities can be misused for malicious ends is a case in point.





As stated in MASC-CBRN D2.2 Mapping on Scientific and Technological Trends<sup>62</sup>, science and technology (S&T) play a pivotal role in modern-day society. In the context of chemical, biological, radiological, and nuclear (CBRN) risks and threats, S&T underpin both the assessment of potential hazards and the development of effective response mechanisms for dealing with their manifestations.

Two types of dynamics that have an impact on S&T innovation have been identified: intrinsic and extrinsic.<sup>63</sup>

Intrinsic dynamics comprise the trends and drivers that are characteristic of CBRN-related research and development (R&D) processes in the twenty-first century. The manifestation of these dynamics is indicative of both the benefits and risks arising from modern science and technology. These include:

- Convergence.
- De-skilling, pace, and mechanisation of R&D processes.
- Availability of CBRN-related information online.
- Globalisation of R&D processes.<sup>64</sup>

Extrinsic dynamics comprise the trends and drivers that shape CBRN-related R&D processes in the twenty-first century. Implicit in the manifestation of these dynamics is the value that is attached to science and technology as key vehicles for achieving socio-economic progress and gaining political and military power. These include:

- The role of S&T in socio-economic development.
- The role of S&T in civil protection and emergency preparedness
- The role of S&T in security and defence.<sup>65</sup>

To capitalise on the expected benefits in these domains, it is important that the potential security, ethical, social, and legal concerns arising from advances in science and technology in relevant fields are effectively managed.

### **Intrinsic dynamics**

**Convergence** broadly refers to the increasing interaction between different scientific disciplines that seeks to develop new approaches and tools for resolving scientific and technological problems. It is manifested in the emergence of novel interdisciplinary fields of epistemological enquiry as a result of the incremental progress made in disparate disciplines, including through the availability of high-precision investigative instruments that allow the manipulation of matter at a previously unprecedented scale and advancing computer and data science.

**De-skilling and mechanisation/automation of R&D processes** refers to the changing nature of innovation as technology evolves. Technological convergence is lowering the barriers to the practice of science, thus allowing the emergence of civilian science and DIY science. Equally,

<sup>62</sup> MASC- CBRN D2.2 Mapping on scientific and technological trends, p.1.

<sup>63</sup> MASC- CBRN D2.2 Mapping on scientific and technological trends, p.1.

<sup>64</sup> MASC- CBRN D2.2 Mapping on scientific and technological trends, p.1.

<sup>65</sup> MASC- CBRN D2.2 Mapping on scientific and technological trends, p.1.





enabling technologies are impacting on professional science practice by generating novel capabilities that hold a significant potential for reshaping existing research norms and modes of behaviour.

**Wide availability of S&T information and materials** refers to the large amount of open-source experimental data and products that can be accessed, including in real time. The Internet plays a crucial role in this regard by enabling online academic publishing, online teaching, training, and learning, the online exchange of information through live platforms and teleconferences, and online trade in laboratory materials and equipment.

**The globalisation of R&D processes** refers to the growth of international scientific collaboration through foreign exchange programmes; the availability of teaching, learning, and research career opportunities in foreign countries; and the opportunities for resource and technology sharing.<sup>66</sup>

## Extrinsic Dynamics

### The Role of S&T in Socio-Economic Development

Science, technology, and innovation are regarded as critical prerequisites for sustainable social and economic development. High-quality, knowledge-intensive jobs and innovative enterprises that lead to discovery and new technology are vital ingredients for burgeoning economy and social prosperity.

### The Role of S&T in Civil Protection and Emergency Preparedness

The Sendai Framework for Disaster Risk Reduction 2015-2030<sup>67</sup> that was adopted by the Third UN World Conference on Disaster Risk Reduction underscores the need for a multi-hazard approach and inclusive risk-informed science-based decision-making process for disaster risk reduction. Innovation, technology development, and technology transfer are key aspects of the prevention and detection of, and the response to disaster risks, regardless of their origins. The value of a multi-hazard approach to disaster risk management that seeks to tackle both environmental and man-made disaster risks has also been recognised at EU level.<sup>68</sup> The spectrum of potential hazards includes CBRN events.

### The Role of S&T in Security and Defence

The advancement of science and technology has had a considerable impact on security planning, defence, and weapon development. Novel military technology can change the face of conflict and the ways in which armed operations are carried out. The history of the development of weapons of mass destruction (WMD) – chemical, biological, and nuclear weapons – is instructive in this regard. In particular, it shows how the increasing scientific

<sup>66</sup> MASC- CBRN D2.2 Mapping on scientific and technological trends, p.13.

<sup>67</sup> UN General Assembly, *Sendai Framework for Disaster Risk Reduction 2015-2030*, United Nations Office for Disaster Risk Reduction, 2015, available at <https://www.undrr.org/publication/sendai-framework-disaster-risk-reduction-2015-2030>.

<sup>68</sup> European Commission, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Overview of natural and man-made disaster risks in the EU*, SWD/2014/0134, 8 April 2014, available at <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52014SC0134>.





understanding in fields such as chemistry, biology, and physics coupled with opportunities for scaled up production can pave the way for the establishment of weapon programmes.<sup>69</sup>

## 4.2.2 Risk Trajectory

This part examines CBRN risk trajectories taking into account the work carried out under WP2. The section highlights the importance of a comprehensive ‘cradle-to-grave’ approach to the prevention of the deliberate misuse of CBRN materials and knowledge covering all stages of a potential CBRN deliberate incident: Inception, Access to materials and Information, Illicit trafficking of Materials, Plotting and Conducting an attack, Threat risk preparedness and response.

### 4.2.2.1 Inception

The inception of a CBRN attack is a crucial yet elusive stage. This stage involves the initial decision of conducting such an act. This decision is influenced by a multitude of factors and can take unlimited potential forms depending on the malicious actors (lone wolves, terrorist organization or radicalized crime groups, other), their motives and goals, previous acts, as well as, selected targets.

The inception of a CBRN attack concerns CBRN security stakeholders, that is relevant state authorities. Preventing an attack at this stage is arguably the most effective strategy, but also the most challenging one, as reliable intelligence and irrefutable evidence is required to justify pre-emptive action.

### 4.2.2.2 Access to CBRN Materials and Information

This stage involves obtaining the knowledge and materials necessary to conduct a CBRN attack.

Material acquisition includes obtaining all the necessary resources for carrying out a CBRN attack, including weaponization, transportation and deployment devices as well as facilities and equipment, should the perpetrators decide to produce the CBRN material themselves. Information about potential targets would also be collected at this stage.

Producing CBRN material requires expertise and essential ingredients and equipment. Such an undertaking would further require extensive financial and material resources. Acquiring readily available CBRN material might thus be preferred as an option by would-be perpetrators. Ensuring the physical safety and security of CBRN materials in all facilities where such materials are used is of vital importance in reducing the risk of theft, misplacement, loss, or misappropriation. Equally, attention needs to be given to ensuring that relevant personnel are aware of the risk of CBRN misuse and trained to address this risk effectively. Key points related to the technical, behavioural, and procedural aspects with regard to preventing the illicit acquisition of CBRN materials and information are listed in Tables 1, 2, and 3.

---

<sup>69</sup> MASC- CBRN D2.2 Mapping on scientific and technological trends.



**Table 1: Technical Aspects**

- CBRN materials should be stored in sealed and secure locations. The locations should be under lock.
- The access to CBRN materials and information should be secured.
- Reliable cybersecurity and information exchange systems should be in place.
- Systems for access control and real-time monitoring (e.g. video monitoring, electronic access systems) should be in place.
- The access to storage spaces of CBRN materials should be personalised and relevant credentials should not be commonly shared.
- Access to the storage locations should be monitored and records of accessing personnel should be kept.
- Doors to premises and storage spaces should be clearly marked with appropriate signage indicating the existence of CBRN materials.
- Information concerning CBRN materials and other materials of dual use should be encrypted on a secure network.
- Location-based registration of the infrastructure areas or departments where activities involving CBRN materials are taking place should be established.

**Table 2: Behavioural Aspects**

- Personnel reliability should be enhanced in view of the need to minimise the ‘insider threat’.
- Strict criteria for obtaining and handling CBRN related information within and outside the facility should be established.
- Employees should demonstrate awareness of CBRN risks, including the risk of deliberate misuse. All designated personnel and supporting staff should be aware that CBRN materials are handled on the premises.
- Personnel should demonstrate an understanding of the need for reporting both incidents and near-incidents (e.g. lapses that have been effectively addressed).

**Table 3: Procedural Aspects**

- A clear protocol on the access to CBRN-related information should be established.
- The transport and transfer of CBRN materials should be tracked and end-locations and all transit zone should be registered.
- Regular audit and accountability procedures, including regular reporting and incident alert should be in place to ensure that CBRN materials in storage are kept safe and not misplaced.
- The amounts of CBRN materials stored on facility premises should be not exceed necessary quantities. Oversupply of the materials kept in stock should be avoided.
- Awareness-raising programme about CBRN risks, including the risk of deliberate misuse for all personnel should be established.





- Internal (institutional) CBRN safety and security policies should cover both physical and information security and feature regular risk assessment and contingency planning in case of an incident.
- Safety and security measures should be subject to regular monitoring and evaluation.
- Mechanisms for verifying compliance with the established safety and security procedures and for reporting instances of non-compliance should be in place.
- Mandatory inspections of spaces with enhanced security (e.g. laboratories, storage rooms) should be performed.
- The proper use of the existing technical systems for physical security should be guaranteed.

#### 4.2.2.3 Illicit trafficking of CBRN Materials

If perpetrators are not able to acquire CBRN materials from within the country, they could attempt to smuggle them from abroad. Reducing the risk of such activities requires a comprehensive system of policies, regulations, and measures for strengthening border controls, in order to ensure timely detection of illicit actions. Indicative key points related to the technical, behavioural, and procedural aspects of preventing the illicit trafficking of CBRN materials are listed in Tables 4, 5, and 6.

##### Table 4: Technical Aspects

- Mechanisms for detecting CBRN materials at borders, points of entry, and checkpoints (e.g. sensors, container scanning technology) should be in place.
- Technical equipment for tracking the movement of CBRN materials inside facilities should be in place.
- Electronic tracking and tracing system should be in place to monitor the shipment, transfer, and transport of CBRN materials.

##### Table 5: Behavioural Aspects

- Sensitive and classified information should be handled in line with appropriate procedures.
- Personnel should demonstrate understanding of the fact that CBRN materials can be dual use and that the risk of deliberate misuse should be properly addressed.
- Personnel should be familiar with the laws and regulations on the transferring of CBRN materials both within and between countries and should follow them.

##### Table 6: Procedural Aspects

- Licensing procedures for the transfer of CBRN materials should be in place.
- Procedures for ensuring compliance with the existing dual-use export controls should be in place.
- Procedures for the audit of CBRN material upon delivery should be in place.





- Employees should be aware of how to deal with sensitive CBRN-related information and trained to handle sensitive information, and to act accordingly.

#### 4.2.2.4 Unravelling CBRN attack plots

Intelligence gathering and data sharing among relevant security services play a key role in uncovering plans for potential illicit activities, including CBRN attack plots by non-State actors. It is equally essential that all relevant stakeholders that work with or handle CBRN materials have a basic level of situational awareness of the risk of CBRN deliberate misuse and can identify signs of suspicious behaviour. Community intelligence constitutes an important line of prevention and contribute to detecting would-be perpetrators before the latter have managed to carry out an attack. Key technical, behavioural, and procedural aspects related to the development of effective mechanisms for uncovering CBRN plots are listed in Tables 7, 8, and 9.

##### Table 7: Technical Aspects

- Cybersecurity systems should be in place in facilities where CBRN materials are handled.
- Systems for reliable real-time data exchange between law enforcement and intelligence services should be in place.

##### Table 8: Behavioural Aspects

- Personnel in facilities handling CBRN materials should be trained to identify and report signs of suspicious behaviour.
- Channels of communication between facilities handling CBRN materials and relevant competent authorities, including law enforcement services should be established.

##### Table 9: Procedural Aspects

- Facilities handling CBRN materials should have in place procedures for reporting and dealing with suspicious behaviour.
- Procedures for reliable real-time data exchange between competent security authorities at national and EU level should be in place.

#### 4.2.2.5 CBRN risk preparedness and response

Adequate preparedness and response capacities for dealing with CBRN events are essential for mitigating the negative impact of deliberate CBRN incidents. Depending on the type of the attack, different authorities would need to step in. To ensure the safety of first responders (e.g. fire services, police, special security units, army forces, medical staff), the incident scene would need to be carefully evaluated. In case explosives have been used, the structural integrity of





buildings needs to be assessed, including for any signs of open fires, or dispersed toxic substances. The required protective equipment and gear of first responders would be selected accordingly. Scents, colours, pools of liquids or damages to infrastructure can also serve as indicators that CBRN materials have been used. Autonomous aerial systems (e.g. drones) with CBRN sensors could be deployed for collecting data from the incident scene immediately after the attack to help identify the type of material that has been used. Medical emergency teams would be dispatched and if necessary mobile laboratory units could be deployed for diagnostics. Key points related to the technical, behavioural, and procedural aspects of CBRN preparedness and response are listed in Tables 10, 11, and 12.

**Table 10: Technical Aspects**

- Portable equipment and systems for incident scene screening and forensics, diagnostics, testing, and decontamination that can be deployed for crisis management, including CBRN events should be available.
- CBRN personal protective equipment should be available to first responders arriving at the incident scene.
- An integrated national alert system that disseminates information to relevant emergency and security services in case of an incident should be in place.
- Mobile medical units, including field hospitals should be available.
- Protective gear and therapeutics should be made available to the general public throughout the duration of crisis response and decontamination operations to mitigate CBRN incident impact.

**Table 11: Behavioural Aspects**

- Emergency services should have operational capacity for coordinated action on CBRN crisis management.
- First responders should be properly trained to deal with CBRN incidents.
- The general public should have basic awareness of the required steps to be taken in case of a CBRN incident.

**Table 12: Procedural Aspects**

- CBRN crisis management plans should be in place at national, regional, local, and institutional level.
- Regular field exercises for CBRN crisis management should be conducted at national regional, local, and institutional level.
- Procedures for the timely reporting of CBRN incidents should be in place, especially at facilities where CBRN materials are handled.
- CBRN personal protective equipment should be regularly tested and upgraded. Procedures should be in place to ensure that designated personnel are aware of the level and types of equipment that need to be used.





- Information about emergency evacuation procedures at public spaces (e.g. shopping centres, office buildings, event centres, art and music halls, public transport etc.) should be clearly displayed.
- Nation-wide CBRN incident risk assessment should be conducted on a regular basis.
- Procedures for crisis communication and data sharing should be in place.
- Victim support services should be provided.





## 5 Conclusions and key points

### 5.1 Conclusions

The report acknowledges that the CBRN risk spectrum is wide, covering different risk perceptions, sources, factors and trajectories that are relevant to the EU context.

*“Whether released accidentally or deliberately, chemical agents, pandemic and epizootic biological diseases, and radiological and nuclear substances can pose significant threats to global health, the environment and the economy.”<sup>70</sup>*

There is an extensive body of relevant EU legislation and strategic guidance on terrorism which underscores the important role that the European Union can play in crisis management through proactive partnership between its institutions and the Member States.

The work carried out as part of WP2 includes analysis of CBRN risks that was informed by research on the EU context, a literature review, a review of scientific and technological trends relevant to CBRN, and national surveys. As part of the national surveys, the countries participating in this project prepared scenarios of possible deliberate CBRN events. The scenarios covered different instances of malicious acts involving chemical, biological, and radiological/nuclear sources. For reasons of confidentiality and security this document will not reference the scenarios.

It is worth noting that all national survey reports recognise that CBRN challenges are diverse and multifaceted and that they can vary from a country to country. CBRN risk trajectories are in constant change and evolve as a result of local, national, and international events and dynamics, including relevant scientific and technological advances.

Chemical risks are considered high priority, due to the large amount of hazardous and toxic chemical substances that are available, the large industrial sector in which toxic chemicals find a wide application, and the potential for industrial and transport incidents. It has been recognised at EU level that the misuse of chemical substances poses a particular threat.<sup>71</sup>

The potential misuse of biological agents and toxins is an important risk and when examining biological risks attention should be given to the difficulty in distinguishing between naturally occurring and deliberately caused outbreaks.

The misuse of radioactive substances within medical infrastructures and of radiological waste is considered, particularly as regards the potential health and psychological impact that such attacks could have on communities, as well as the environmental contamination likely to result.

<sup>70</sup> See [https://www.eca.europa.eu/Lists/ECADocuments/SR18\\_14/SR\\_CBRN\\_EN.pdf](https://www.eca.europa.eu/Lists/ECADocuments/SR18_14/SR_CBRN_EN.pdf) , p.8.

<sup>71</sup> See <https://op.europa.eu/webpub/eca/special-reports/cbrn-14-2018/en/>.





Nuclear risks related to the misuse of technology are considered low probability. Nevertheless, the need for continued strengthening of the implementation of nuclear safety and security is acknowledged.

Each of the CBRN categories i.e. chemical, biological, radiological/ nuclear could pose a risk for the EU on a different level based on multiple factors. It needs to be kept in mind that terrorist acts using CBRN materials could be, as any other terrorist acts, unpredicted and not expected, could use either new technologies or old technologies in a new way and could be very creative.

*“As CBRN threats know no borders the EU cannot confine its actions to the EU area. Indeed, the European Council, the Council of the European Union and the European Parliament have repeatedly stressed the importance of linking the EU’s internal and external security policies, which cover CBRN matters.”<sup>72</sup>*

The prioritization of risk assessment performed with appropriate tools is necessary for strengthening the regional, national, and international preparedness and in delegating appropriate roles when facing CBRN risks of any type. Effective response to the CBRN risk spectrum requires proactive thinking, synergies, and strategies, as well as resources and training are important. Multi-level contingency planning at all stages of the CBRN risk prevention and management cycle and inter-agency coordination are of particular value in this regard. By increasing accountability and awareness among relevant stakeholders and fostering partnerships, the CBRN risk spectrum can be addressed in a way that takes into account different countries’ local circumstances. Constructive dialogue and synergies within and outside the EU are needed to enhance the prevention of security risks, including deliberate CBRN incidents.

## 5.2 Key Points

Key challenges when dealing with a CBRN incident, including deliberate CBRN attacks may include:

- Lack of decontamination capabilities and capacities;
- Limited stock of decontamination solutions;
- Limited specialised medical capabilities and capacities;
- Lack of waste management capabilities and capacities (including disposal of contaminated water);
- Limited crisis response and counter measure capabilities and capacities.<sup>73</sup>

---

<sup>72</sup> See [https://www.eca.europa.eu/Lists/ECADocuments/SR18\\_14/SR\\_CBRN\\_EN.pdf](https://www.eca.europa.eu/Lists/ECADocuments/SR18_14/SR_CBRN_EN.pdf), p.9.

<sup>73</sup> Atlantic Treaty Association, *Final Report Chemical, Biological, Radiological, and Nuclear Threats*, September 2017, <https://g8fip1kplyr33r3krz5b97d1-wpengine.netdna-ssl.com/wp-content/uploads/2017/11/CBRN-Final-Report.pdf>.





A basic CBRN risk management cycle addresses at least the following phases:

- **Prevention and mitigation:** Actions are taken before the incident to prevent or minimise consequences through assessments of hazards and vulnerabilities.
- **Preparedness:** Assessments from the first phase lead to the development of the plan to manage the CBRN incident, including the acquisition of capabilities and training programmes. The plan should clearly integrate medical capabilities at the local, regional, and national levels. This may require the establishment of coordination agreements between different services and agencies so they can be integrated smoothly into the command and control system. Management plans should be as simple as possible and be clearly expressed, as complex plans may be difficult to implement.
- **Response:** The emergency plan is put into practice in a real-time event. The response phase will depend on the preparedness phase.
- **Recovery:** Finally, actions are taken to return to the pre-event situation. Such actions might include disposal of hazardous materials and remediation of the incident site, as well as further assistance to victims.<sup>74</sup>

Based on the four domains listed above, key points of relevance to CBRN risk management and resilience as regards infrastructure, governance, preparedness, and cooperation (Boxes 8, 9, 10, and 11) are considered.

#### **Box 8: KEY POINT GROUP A – Infrastructure**

- Conducting vulnerability assessment.
- Development of measures and procedures to enhance the resilience of all elements of critical infrastructures.
- Development of maintenance and oversight procedures for ensuring the infrastructure performance infrastructure (including its supply chain).
- Development of a contingency plan that will enable the infrastructure to function with minimal resources at minimal level.
- Development of monitoring systems and early warning mechanisms in case of an emergency.
- Development of public or private funding mechanisms for increasing resilience.
- Development of accountability and penal procedures for enhancing compliance with institutional and national regulatory requirements.

---

<sup>74</sup> OPCW, *Practical Guide for Medical Management of Chemical Warfare Casualties*, 2019, [https://www.opcw.org/sites/default/files/documents/2019/05/Full%20version%202019\\_Medical%20Guide\\_WEB.pdf](https://www.opcw.org/sites/default/files/documents/2019/05/Full%20version%202019_Medical%20Guide_WEB.pdf)



**Box 9: KEY POINT GROUP B – Governance**

- Creation of CBRN management coordination groups at local, regional, and national level.
- Development of standards on resilience methods, procedures, and tools.
- Conducting threat and risk assessment.
- Development of a resilience plan with short- and long-term perspective to prevent, mitigate, respond to, and recover from CBRN events.
- Development of contingency plans at national and regional level.
- Development of a regulatory framework with clearly defined duties and responsibilities for different stakeholders.
- Development of resilience measures and procedures for the protection of public spaces.
- Integration of local, regional, national, and international plans CBRN risk management plans and strategies.
- Development of a strategy for a cross-country coordination approach for CBRN risk management.

**Box 10: KEY POINT GROUP C – Preparedness**

- Development of a communication platform that allows for regular information sharing during the crisis.
- Enhancing public awareness of CBRN risk management.
- Fostering public-private partnerships for the development of tools, practices, technologies and methodologies for CBRN crisis management.
- Conducting capacity assessment.
- Development of education and training mechanisms for response teams, local authorities, emergency services, and critical infrastructure stakeholders.
- Integrating lessons learned and good practices from previous crisis management operation into CBRN training and capacity building programmes.

**Box 11: KEY POINT GROUP D – Cooperation**

- Enhancing participation in local, regional, national, and international networks for promoting knowledge, exchanging experiences, and increasing capacities and capabilities.
- Assigning specific responsibilities and duties and allocating resources to all stakeholders involved in the prevention, preparedness, response, and recovery phases of a CBRN event.
- Development of practices and procedures for cross-sectorial coordination and cooperation and establish collaborative networks.
- Development of a culture of resilience among citizens.
- Development of technical training and field exercises for different sectors.





- Organising public consultations to ensure communities' participation and cooperation in case of a CBRN event.
- Development of training sessions and workshops for citizens and organisations based on their specific needs.

