PEERS
PracticE Ecosystem for standaRdS

Deliverable 6.3
White Paper on future standardisation needs

23 October 2025

V1.0

Project Information

Project title	PracticE Ecosystem for standaRdS	
Project acronym	PEERS	
Project number	101074040	
Start date/ Duration	1st November, 2022	36 months
Topic	HORIZON-CL3-2021-DRS-01-04. Developing a prioritisation mechanism for research programming in standardisation related to natural hazards and/or CBRN-E sectors	

Work Package title	WP6: Impact and Outreach (Dissemination, Communication, Exploitation)	
Task title	T6.2 Exploitation, Models, Market Uptake and Sustainability	
Deliverable title	D6.3 White Paper on future standardisation needs	
Deliverable type	R - Document, report	
Doc. Version & WP no.	1.0	WP6
Due date	M36 - October 2025	
Lead Beneficiary	FORMIT	
Leading author(s)	Matteo Costola (FORMIT)	
Contributing author(s)	This document has been prepared solely by the author. However, it constitutes the final outcome of a structured stakeholder consultation process. Valuable contributions were gathered through a dedicated survey and in-depth interviews with distinguished experts in the domains of CBRN and standardisation. The author wishes to express his sincere gratitude to all participants for their time, expertise, and insights, which have been instrumental in informing and shaping the content of this deliverable.	
Internal Reviewer(s)	Beatrice Errico (FORMIT), John Sheils (KPMG FA), Jon Hall (RAN), Stefan Krebs (ČAS), Paul van der Werff (FIPRA), Emma Loebler (FIPRA)	
SAB Reviewer(s)	David Crouch	
Release date	23 October 2025	

Classification – This report is:									
Draft		**Final**	X	**Public**	X	**Sensitive**		**Confidential**	

Revision History			
Date	**Version**	**Author**	**Distribution/Substantive changes made**
22-05-2025	v0.1	Matteo Costola (FORMIT)	First draft release.
15-07-2025	v0.2	Matteo Costola (FORMIT)	Second draft release.
01-08-2025	v0.3	Matteo Costola (FORMIT)	Third draft release.

29-08-2025	v0.4	Matteo Costola (FORMIT)	Fourth draft release.
03-09-2025	v0.5	Matteo Costola (FORMIT)	Fifth draft release.
29-09-2025	v0.6	Matteo Costola (FORMIT)	Final draft release.
02-10-2025	v0.7	Beatrice Errico (FORMIT)	Internal review.
17-10-2025	v0.8	Paul van der Werff (FIPRA), Emma Loebler (FIPRA)	Internal review and quality assurance.
17-10-2025	v0.9	David Crouch	Internal review and quality assurance; SAB scrutiny.
23-10-2025	v1.0	Beatrice Errico (FORMIT), Matteo Costola (FORMIT)	Final release.

Acknowledgement

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement No. 101074040.

Disclaimer

Table of Contents

List of Figures

List of acronyms and abbreviations

AI	Artificial Intelligence
CBRNe	Chemical, Biological, Radiological, Nuclear and Explosives
CEN	European Committee for Standardisation
CENELEC	European Committee for Electrotechnical Standardisation
CoE	Centres of Excellence
CTBT	Comprehensive Nuclear-Test-Ban Treaty
CWA	CEN Workshop Agreement
DNA	Deoxyribonucleic Acid
DRS	Disaster Resilient Societies
ETSI	European Telecommunications Standards Institute
EU	European Union
GPS	Global Positioning System
IoT	Internet of Things
NATO	North Atlantic Treaty Organisation
NGO	Non-Governmental Organisation
NPT	Nuclear Non-Proliferation Treaty
NSO	NATO Standardisation Office
PCR	Polymerase Chain Reaction
PEERS	PracticE Ecosystem for standaRdS
RDD	Radiological Dispersal Device
SCADA	Supervisory Control And Data Acquisition
SME	Small and Medium Enterprise
SMR	Small Modular Reactor
STANAG	NATO Standardisation Agreement
UAV	Unmanned Aerial Vehicle

EXECUTIVE SUMMARY

This White Paper, developed in the framework of the PEERS project, is conceived as a foundational document specifically focused on identifying and addressing the future standardisation needs in the field of Chemical, Biological, Radiological, Nuclear, and Explosive (CBRNe) risk management across Europe. Its core objective is to provide institutional policymakers, regulatory authorities, industry leaders, and the broader scientific community with a robust analytical and strategic framework to anticipate and navigate the complex and multifaceted CBRNe threat landscape. By leveraging the knowledge and expertise cultivated throughout the PEERS consortium, this White Paper aims not only to analyse emerging risks and vulnerabilities, but most importantly to promote the creation, adoption, and continuous evolution of harmonised standards. The document therefore seeks to enhance preparedness, interoperability, and resilience of critical infrastructures and societal systems at both the European and international levels, and underscores the vital importance of a collective, coordinated European Union (EU) vision to meet the standardisation challenges posed by emerging CBRNe threats.

The insights and recommendations presented in this deliverable reinforce the centrality of standardisation as a cornerstone for the effective management of CBRNe risks in an era defined by complexity, uncertainty, and interdependence. The work carried out by PEERS demonstrates that, far from being a static or purely technical exercise, standardisation, particularly when conceived as a response to evolving and future needs, is inherently dynamic: it requires ongoing adaptation, continuous stakeholder engagement, and a willingness to incorporate new knowledge, technologies, and ethical considerations into regulatory and operational practice. Harmonised standards, developed through inclusive and evidence-based processes, constitute a critical enabler of interoperability, cross-border cooperation, and the seamless integration of innovative solutions into security and emergency management operations.

Moreover, the strategic foresight approach championed by PEERS demonstrates that future-proof standardisation demands not only vigilant monitoring of current trends and threats, but also a commitment to horizon scanning for weak signals[1], the integration of scenario-based thinking, and systematic preparation for disruptive wild cards[2] that may reshape the risk landscape in unforeseen ways. In particular, this White Paper underscores the need for a European model of standardisation that is open, agile, and resilient, one that can serve as a benchmark globally, while remaining sensitive to the nuances of local implementation and the imperative of ethical governance. Ultimately, it calls upon all actors, public authorities, industry, the scientific and technical community, and civil society, to view standardisation as an ongoing, collaborative, and forward-oriented process, especially in the context of emerging and future needs. By embedding strategic foresight at the core of standardisation efforts, as exemplified by the PEERS project, the EU can position itself at the forefront of global CBRNe risk management. It can thus be prepared not only to address today's threats, but also to shape the security paradigms of tomorrow in an anticipatory, inclusive, and sustainable manner.

[1] i.e., Unclear indicators that warn us about the likelihood of future "game-changing events", and whose weakness is proportionate to the uncertainty associated with their interpretation, importance, and consequences across varying temporal scales, from the short and medium to the long term (iKnow project).
[2] i.e., "*A future development or event with a relatively low probability of occurrence but a likely high impact on the conduct of business*" (Steinmüller, 2003).

1. INTRODUCTION

1.1 INTRODUCTION TO PEERS

Funded by the European Commission's Horizon Europe Framework Programme, PracticE Ecosystem for standaRdS (PEERS) is a 36-month project that addresses the needs of the HORIZON-CL3-2021-DRS-01-04 call. Launched on November 1st, 2022, PEERS aims to advance and reinforce the EU's operational safety and security policies through the development of a practitioner-driven ecosystem focused on pre-normative / standardisation processes and supporting tools. The PEERS ecosystem supports the effective strengthening of preparedness and response in the field of CBRNe through the practitioner-driven Better Practice Guide initiative, gamification and e-Learning support. It primarily targets assisting Europe's CBRNe practitioners, European research policymaking as well as other stakeholders, including the research community and national standardisation bodies. A comprehensive engagement and consultation governance mechanism has been applied for the realisation of the ecosystem. Additionally, the ecosystem includes an integration capability to existing community-building platforms and a gamification strategy, aimed at encouraging solid user engagement, strengthening interactions activities, and furthering user training skills based on situational awareness. PEERS brings together an experienced, multi-disciplinary team of specialists, to work together as a focused delivery team on meeting policymaker and practitioner expectations over the course of the project and deliver transformational change in the European CBRNe environment.

1.2 PURPOSE OF THE DELIVERABLE

The purpose of this deliverable is to provide a forward-looking, evidence-based contribution to the ongoing debate on the future standardisation needs within the CBRNe domain. Developed in the framework of the PEERS project, this White Paper brings together foresight analysis (i.e., a systematic process of anticipating and evaluating possible future trends, risks, and opportunities to support informed decision-making and strategic planning today), stakeholder consultations, and empirical research to identify critical gaps, anticipate emerging challenges, and formulate policy recommendations that can guide both European and national actors in shaping a more coherent and anticipatory approach to CBRNe standardisation. Beyond its analytical dimension, the document is conceived as a conceptual framework for translating strategic foresight into practical governance mechanisms. It seeks to define how standardisation can evolve from a static regulatory exercise into a dynamic and iterative process, capable of integrating new knowledge, technologies, and ethical considerations into operational and policy practice. In doing so, it aims to advance a set of policy recommendations aimed at reinforcing the alignment between research, innovation, and standardisation priorities, promoting an adaptive EU model of CBRNe resilience.

The White Paper therefore positions itself as both a strategic and operational bridge between dialogue and implementation. By fostering continuous interaction amongst policymakers, practitioners, and standardisation bodies such as the European Committee for Standardisation (CEN), the European Committee for Electrotechnical Standardisation (CENELEC) and the European Telecommunications Standards Institute (ETSI), it outlines how the proposed "dynamic dialogue" can translate into tangible implementation steps, including the initiation of coordinated standardisation activities and the integration of PEERS outputs into future European and international frameworks.

1.3 STRUCTURE OF THE DELIVERABLE

This deliverable is structured to guide the reader from context-setting to strategic foresight and actionable recommendations. It begins with an *Executive Summary*, which clarifies the objectives, the methodology, and the key messages, before moving to an *Introduction*, that outlines the objectives of PEERS and the purpose of the document. A *Literature Review* follows, framing the CBRNe landscape and examining the state of the art in CBRNe governance and standardisation at the European level.

Building on this foundation, an overview of the stakeholder consultations carried out within the framework of this White Paper is provided. These perspectives are captured in two parts, according to the methodology applied. First, through an *online questionnaire* designed to collect a wide range of inputs from diverse organisations and stakeholders to identify gaps, impacts, and priorities, and provide a critical assessment of the European framework. Second, through a series of *semi-structured interviews with selected experts*, which offered deeper insights and qualitative reflections on the current state and future directions of CBRNe standardisation that consider emerging risks to strengthen coordination and responsiveness.

A *strategic foresight analysis* is therefore described, identifying six transformative trends, from Artificial Intelligence (AI) and synthetic biology to environmental degradation, disinformation, nuclear instability, and space-based vulnerabilities, and considering their long-term implications for CBRNe security. The final sections set out *policy recommendations and conclusions*, providing concrete guidance for EU and national stakeholders, while the *bibliography* and the a*nnexes* offer supporting tools, information, and references to ensure clarity and rigour.

2. THE STATE OF CBRNE GOVERNANCE AND STANDARDISATION IN EUROPE

The CBRNe landscape in Europe is defined by diversity, complexity, and rapid evolution. It encompasses accidental industrial incidents, the deliberate misuse of hazardous materials, radiological leaks, nuclear accidents, and the spread of infectious diseases, alongside the accelerating influence of disruptive technologies and hybrid threats (Danielewski, 2019; Abaimov & Martellini, 2020). While CBRNe agents are indispensable to legitimate sectors such as medicine, agriculture, energy, and research, their inadequate control or intentional weaponisation poses substantial risks to public health, critical infrastructure, environmental sustainability, and economic resilience. These risks are inherently transnational, transcending national borders and sectors, and therefore demand governance models capable of integrating technical expertise, health security, and international cooperation in a coherent and forward-looking manner (Maurer & Kellenberger, 2019; Rychnovská, 2016).

Over the past decade, the EU has consolidated a broad and multi-layered framework to strengthen preparedness and resilience. The adoption of the CBRN Action Plan in 2009 and its 2017 revision represented milestones in establishing a common strategic direction, with a particular focus on risk assessment, capability development, research integration, and the systematic exchange of knowledge amongst Member States (European Commission, 2009; European Commission, 2017). The Union Civil Protection Mechanism has subsequently embedded CBRNe into the wider EU crisis management architecture, supporting coordination across borders and sectors (European Parliament, 2021). In parallel, the CBRNe Centres of Excellence (CoE), which now involve more than sixty partner countries worldwide, has emerged as a flagship instrument of EU external action. By promoting joint training, voluntary cooperation, and knowledge transfer, it has not only reinforced Europe's own resilience but also extended the EU's role as a reference point for global CBRNe governance (European Commission News, 2025; Sánchez Cobaleda, 2015; European Court of Auditors, 2018).

Standardisation has become a cornerstone of this architecture. Instruments coordinated by CEN, CENELEC and ETSI provide trusted benchmarks that enable credibility and interoperability across Member States, supporting both national preparedness and international cooperation (Goulart et al., 2018). While formal European Standards and Technical Specifications remain essential, their development cycles are often lengthy, which can be difficult to reconcile with the rapid pace of technological innovation and threat evolution (Antoniazzi, 2022; Ruohonen, 2021). To complement them, more flexible instruments such as CEN Workshop Agreements (CWAs) have been introduced, allowing stakeholders to produce consensus-based guidance within shorter timeframes, and thereby ensuring operational relevance in fast-moving domains (European Commission, 2017; Poustourli et al., 2020). Systematic review mechanisms, obliging technical committees to confirm, revise, or withdraw existing deliverables, further contribute to maintaining the relevance and credibility of European standards over time (European Court of Auditors, 2018).

Alongside the European standardisation system, the role of the North Atlantic Treaty Organisation (NATO) and its Standardisation Office (NSO) represents a crucial dimension of the wider European interoperability framework. NATO Standardisation Agreements (STANAGs) provide a well-established set of operational and technical references that have a direct influence on both military and dual-use preparedness frameworks (NATO, 2022; Boulet, 2006). These instruments define common doctrines, terminology, and procedures across Allied nations, ensuring that multinational responses to CBRNe incidents are coherent, efficient, and mutually intelligible. In particular, several STANAGs developed under the auspices of the NSO address areas that are directly relevant to the topics discussed in this White Paper (i.e., detection, identification, and decontamination). By way of example, the Allied Engineering Publications AEP-7 “Allied CBRN Defence Publication – CBRN Decontamination” and AEP-58(B) “CBRN Defence – Decontamination of Aircraft” serve as practical and authoritative references that codify technical requirements, performance parameters, and safety procedures for decontamination operations across NATO Member States (Finabel, 2020; NATO, 2022). These documents illustrate how harmonised military standards can underpin effective cross-border interoperability. However, they also expose a significant asymmetry, as at present there are no equivalent civilian standards at the European level covering comparable aspects of decontamination (Bures, 2017). This absence represents a structural gap that complicates coordination between military and civilian responders in joint or large-scale CBRNe incidents.

Bridging this gap requires greater transparency and structured cooperation between the European standardisation bodies and the NSO. Strengthening the interface between them would help facilitate mutual recognition, reduce duplication, and promote the systematic transfer of best practices from defence to civil protection domains (European Commission: Joint Research Centre, 2025; Trapp, 2017). Enhanced dialogue between the EU and NATO could also accelerate the development of harmonised reference models, fostering convergence in terminology, testing methods, and operational procedures (Gawlik-Kobylińska, 2022). This alignment is not only a matter of efficiency but also of legitimacy: interoperability between civil and military systems must be pursued with full respect for democratic governance, ethical accountability, and public trust (Long, 2021).

At the same time, recent policy developments have highlighted the growing importance of integrating health security into the broader CBRNe agenda. The European Commission’s investments in medical countermeasures, including vaccines, therapeutics, diagnostics, and personal protective equipment, have strengthened both preparedness and rapid response capacity, while also enhancing coordination between health authorities, civil protection, and security actors (Sprenger, 2020; European Parliament, 2021). The COVID-19 pandemic exposed the costs of fragmented approaches and underlined the value of a harmonised European framework in bridging health security and CBRNe resilience (Long, 2021; Sprenger, 2020). In addition, research-driven platforms such as the CBRNe

Knowledge Hub developed by PEERS[3] and complementary initiatives within the Union Civil Protection Mechanism have reinforced the knowledge ecosystem, ensuring that innovations, validated procedures, and best practices are not confined to academic or technical outputs but are systematically embedded into operational use (Civil Protection Knowledge Network, 2025; Goulart et al., 2018).

From a strategic perspective, the EU approach to CBRNe standardisation demonstrates steady and tangible progress toward a coherent, adaptive, and internationally recognised model. By combining formal and flexible instruments, strengthening cross-border cooperation, integrating NATO interoperability frameworks, and embedding health and technological dimensions into its governance structures, the EU has established a multi-layered system that continues to evolve in step with the complexity of contemporary threats (Trump et al., 2021; Novossiolova & Martellini, 2021). This system positions the EU as a credible reference point in the global CBRNe domain, while simultaneously underscoring the need for continued transparency, collaboration, and foresight in the shared pursuit of security and resilience (Gawlik-Kobylińska, 2022; European Commission: Joint Research Centre, 2025).

3. CHALLENGES, LESSONS LEARNED AND FUTURE DIRECTIONS: INSIGHTS FROM A STAKEHOLDER CONSULTATION

In light of the current state of play outlined in the previous chapter, the PEERS project launched a stakeholder consultation combining an online questionnaire with a set of semi-structured interviews with selected CBRNe and standardisation experts. This approach was designed to capture a broad spectrum of perspectives while also allowing for deeper qualitative insights. The findings provide a valuable lens on how CBRNe standardisation is currently perceived and where stakeholders see the most pressing needs for improvement.

These contributions highlight not only the challenges faced by relevant stakeholders today but also the lessons learned from past experiences and the future directions considered most relevant for strengthening preparedness and resilience across the EU.

3.1 CHALLENGES

The stakeholder engagement process highlighted several structural challenges that continue to limit the effectiveness of European CBRNe standardisation. Foremost amongst these is interoperability, which remains a persistent weakness. CBRNe practitioners frequently pointed to incompatibilities in equipment, procedures, and communication systems which, while manageable within national borders, become critical in cross-border operations. The absence of a common operational language undermines coordination, delays response, and erodes trust between agencies.

Fragmentation was another recurring concern. Respondents described a patchwork of standards and frameworks (national, EU, and NATO) that too often coexist without sufficient alignment. This lack of coherence complicates procurement, training, and deployment, leaving the European system vulnerable to inefficiencies and inconsistencies.

Timeliness was also identified as a challenge. While consensus-driven processes are important for legitimacy, their slow pace implies that standards frequently lag behind technological developments and emerging hybrid threats, risking obsolescence by the time of their publication.

[3] See D4.4 – Technical report for the Gamma release of the PEERS platform for further details.

Finally, respondents emphasised issues of accessibility and visibility of standards. Even where robust standards exist, they are not always well communicated, affordable, or adapted for frontline use.

Moreover, ethical and societal dimensions (e.g., transparency, inclusivity, and proportionality) are insufficiently systematically embedded in standard-setting processes, raising concerns about both legitimacy and public trust.

3.2 LESSONS LEARNED

From these challenges, several important lessons emerge. First, interoperability cannot be treated as a technical detail but must be recognised as the operational backbone of effective preparedness and response. Without harmonised procedures, even the most advanced technologies cannot achieve their intended impact.

Second, inclusivity is indispensable. When first responders, small and medium enterprises (SMEs), health agencies, or local public authorities are absent from the standardisation process, standards risk losing their practical relevance. Broad participation is therefore not just desirable but essential for both legitimacy and effectiveness.

Third, stakeholders underlined that standards must be visible, understandable, and embedded in training if they are to influence real-world decision-making under pressure. Documents alone are insufficient: they must be supported by explanatory guidance, exercises, and dissemination strategies that make them accessible and usable for diverse audiences.

Another lesson concerns the nature of risk itself. While high-technology threats such as AI or synthetic biology attract much attention, CBRNe practitioners emphasised that low-tech, low-cost methods can be equally disruptive if neglected. Preparedness requires balancing anticipation of cutting-edge risks with vigilance toward rudimentary but effective attack vectors.

Finally, stakeholders highlighted the central role of legitimacy. Ethical and societal considerations (e.g., privacy, proportionality, and transparency) are not “soft” concerns but operational enablers. Without public trust and societal acceptance, even technically robust standards may fail in practice.

3.3 FUTURE DIRECTIONS

Looking ahead, stakeholders identified several directions for strengthening the European approach to CBRNe standardisation. Foremost is the need to address interoperability and cross-border coordination systematically. This requires harmonised protocols, modular standards that can be updated iteratively, and interoperable data infrastructures to support joint action across Member States.

Second, the standardisation process itself must become more agile and participatory. Institutionalising feedback loops and inclusive governance mechanisms will help ensure that standards remain dynamic and grounded in operational reality. Greater involvement of frontline responders, SMEs, research institutions, and the civil society would enhance both the practical relevance and the legitimacy of standards.

Investment in accessibility and dissemination is equally essential. Open-access repositories, digital platforms, and targeted training resources can ensure that standards extend beyond regulatory bodies and reach practitioners at all levels. At a strategic level, stakeholders emphasised the importance of deeper European integration, supported by sustained funding and common guidance. Institutionalising foresight capacities through structured monitoring of emerging risks, scenario-based

exercises, and anticipatory governance will be critical to bridging the persistent gap between innovation and regulation. Equally important is the integration of ethical considerations from the outset. Structured consultations, impact assessments, and transparent processes can help ensure that standards enjoy durable legitimacy.

Overall, the findings suggest that the future of CBRNe standardisation depends less on producing additional documents and more on cultivating a coherent, flexible, and inclusive ecosystem. Addressing fragmentation, strengthening interoperability, and fostering trust are essential for Europe to anticipate disruption, manage complexity, and enhance societal resilience. This synthesis outlines the overarching trends, while the following sections examine the evidence gathered through the online questionnaire and the expert interviews in greater depth, illustrating how stakeholders across Europe experience these challenges in practice and how their insights can guide a more resilient and forward-looking approach to CBRNe standardisation.

4. INSIGHTS FROM THE STAKEHOLDER CONSULTATION CARRIED OUT THROUGH AN ONLINE QUESTIONNAIRE

To better understand the current landscape of CBRNe standardisation in Europe, in June 2025 the PEERS project launched a targeted online questionnaire amongst practitioners and institutions across multiple sectors. The consultation aimed to capture both the breadth of organisational involvement and the perspectives of those directly engaged in governance, operational response, research, and technological development.

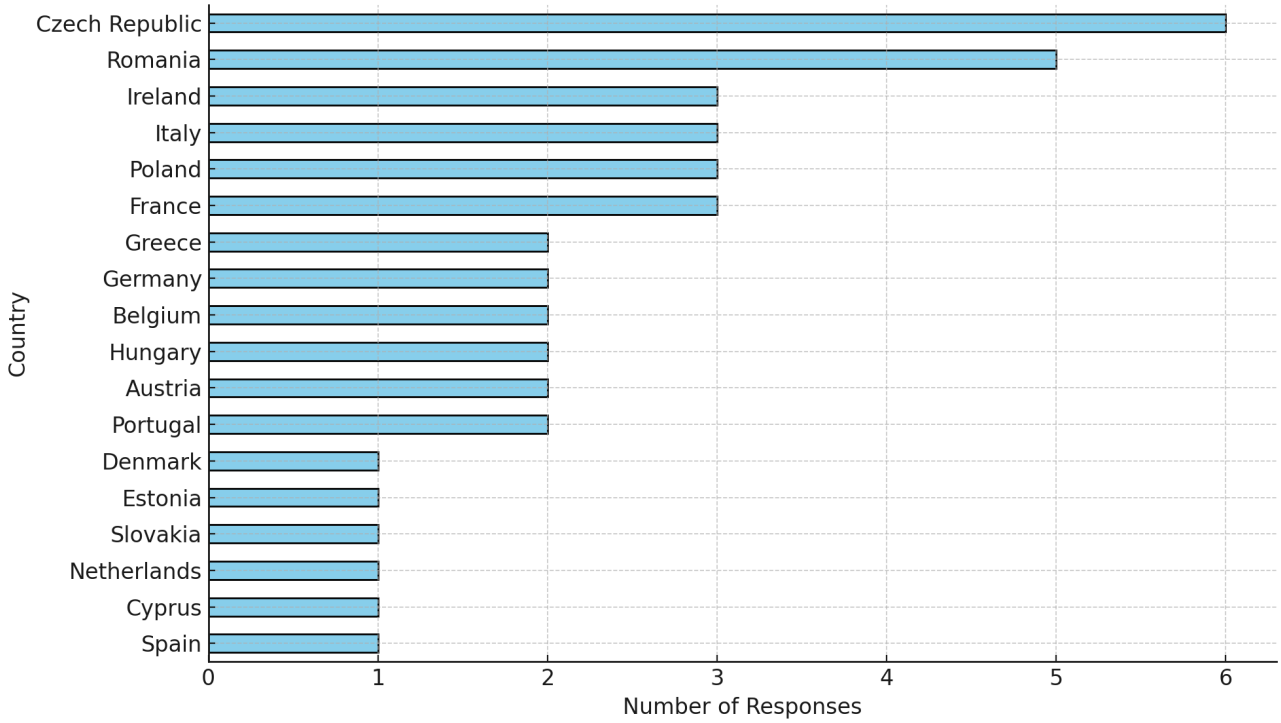

Figure 1 – Number of responses per EU Member State

The responses provide a rich empirical picture, highlighting not only the diversity of stakeholders active in the field but also recurring themes, shared challenges, and common priorities. By systematically analysing these contributions, this chapter identifies patterns and insights that inform

a deeper understanding of the state of European CBRNe standardisation, laying the groundwork for subsequent analyses based on expert interviews and strategic foresight.

The sample encompassed a wide spectrum of organisations, from national authorities and regulatory bodies to law enforcement/defence, academia, industry, and healthcare operators (Figure 2). This variety reflects the inherently multi-sectoral character of CBRNe preparedness, in which governance, operational response, technological innovation, and health protection intersect. Public authorities and regulatory bodies accounted for the largest share of respondents, underlining the central role of government in risk management. However, significant contributions from law enforcement/defence, and research institutions reveal the operational and scientific dimensions of the field, while the participation of industry and private sector actors highlights the growing importance of technological development, equipment provision, and service delivery. Smaller but meaningful inputs from training centres and healthcare operators reinforce the point that CBRNe preparedness is not confined to traditional security sectors but spans an increasingly broad institutional ecosystem.

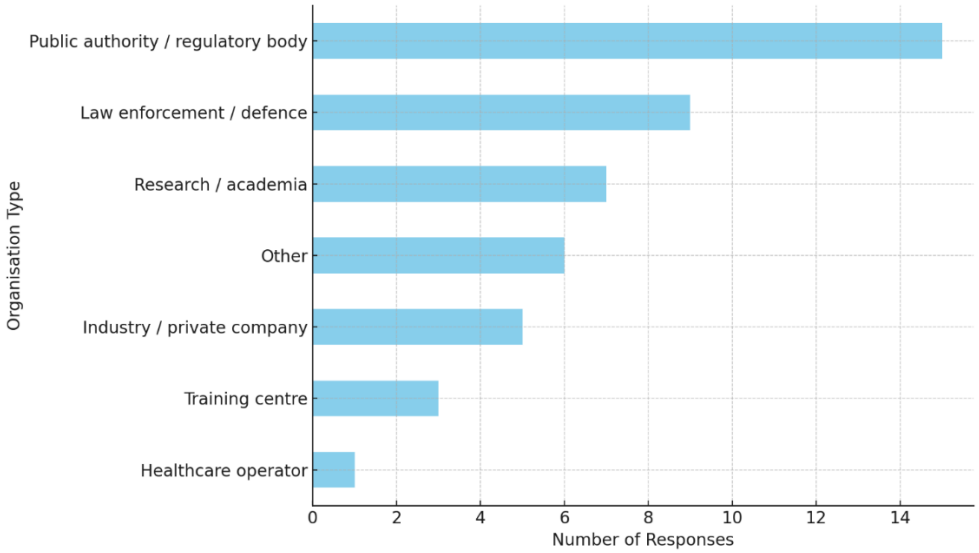

Figure 2 – Number of responses per organisation type

With regard to institutional involvement, most organisations reported either moderate or high engagement in CBRNe activities (Figure 3). This included regular participation in projects and exercises, daily responsibilities in incident management, or central roles in policy and planning. Only a marginal proportion declared low or no involvement, confirming the relevance of the sample to the CBRNe domain.

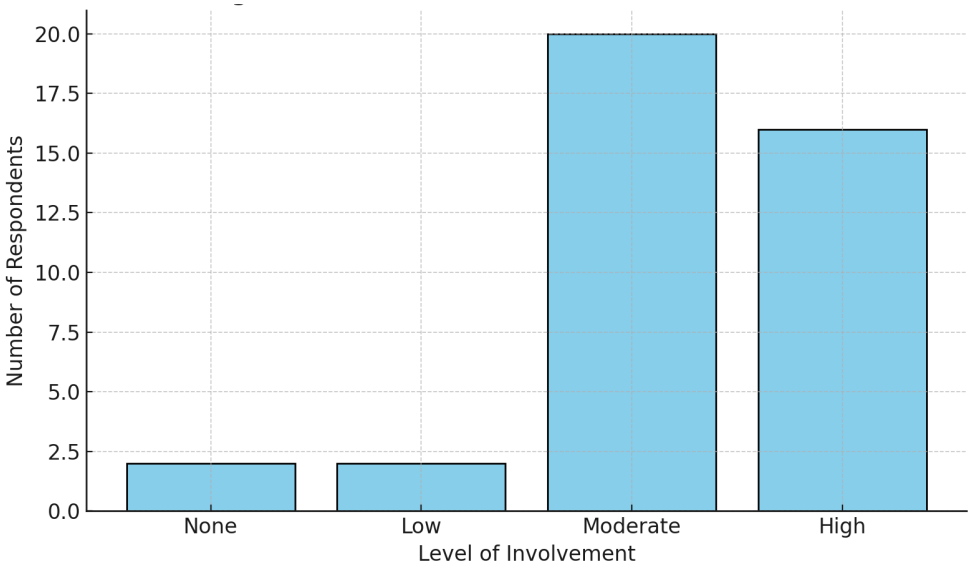

Figure 3 – Organisational involvement in CBRNe activities

When asked about their main areas of focus, respondents prioritised chemical, biological, and radiological threats. Nuclear and explosive risks were cited less frequently, though still present, while many participants also emphasised interdisciplinary and integrated approaches. This is an important finding: it suggests that stakeholders increasingly view CBRNe as an interconnected system of threats requiring cross-cutting governance, rather than discrete technical silos (Figure 4).

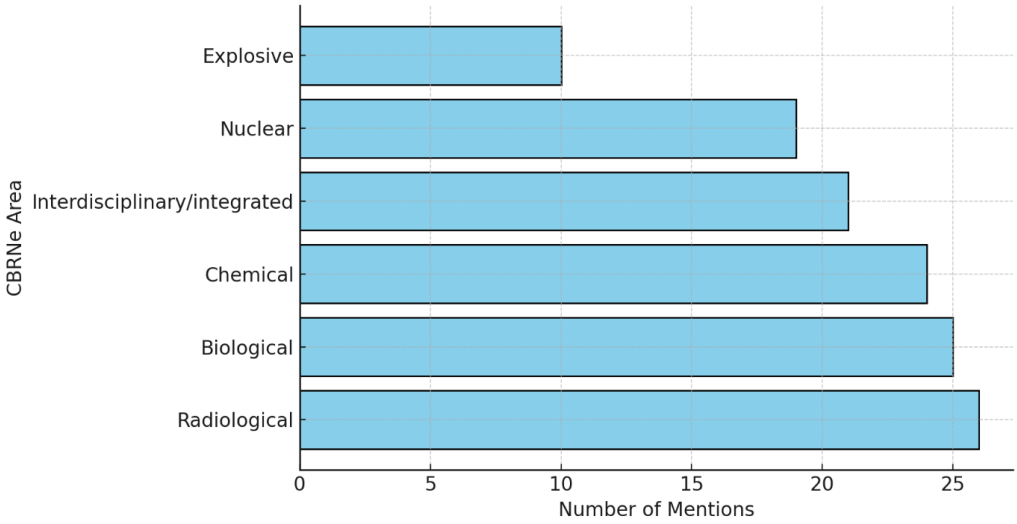

Figure 4 – Most relevant CBRNe areas covered by respondents

The analysis of substantive results reveals a consistent pattern of gaps and challenges in the CBRNe sector (Figure 5). Interoperability clearly emerged as the dominant concern, cutting across technical, procedural, and institutional dimensions. Respondents described persistent incompatibilities in communication systems, equipment interfaces, and decontamination protocols, all of which undermine the efficiency of multinational operations. Fragmentation was also widely reported. National, EU, and NATO standards and frameworks often coexist without adequate alignment, complicating procurement, training, and joint deployments. Another theme that recurred frequently was timeliness: consensus-driven processes, while essential for legitimacy, are often unable to keep

pace with rapid technological change and evolving threats. This raises the risk that by the time new standards are adopted, they may already be outdated or partially obsolete.

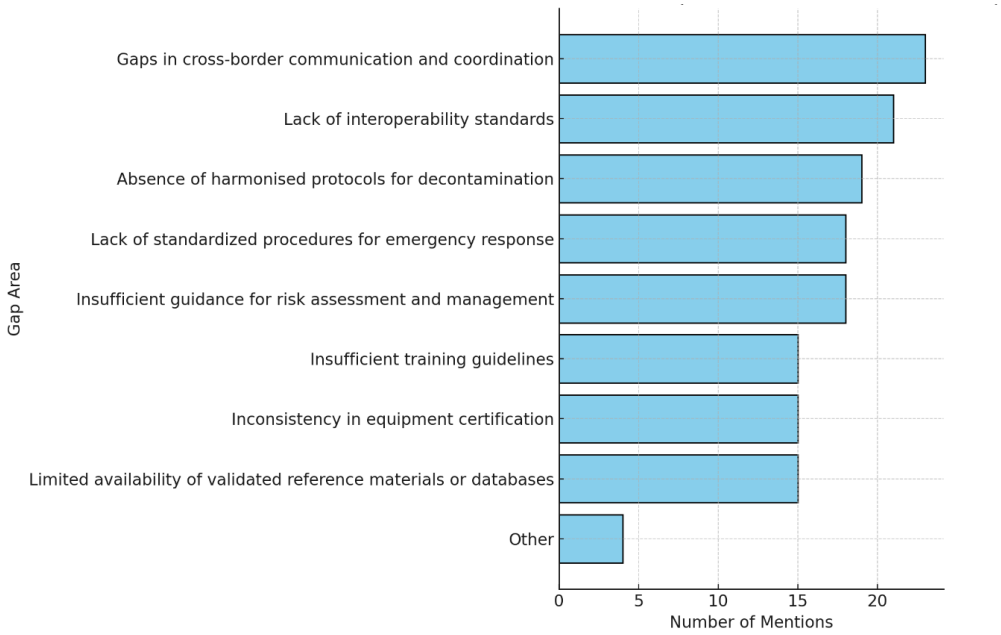

Figure 5 – Main standardisation gaps in the CBRNe sector

These shortcomings are not abstract. They translate into direct operational impacts. Reduced interoperability was the most frequently cited consequence, leading to miscommunication, delays, and inefficiencies during joint operations. Respondents highlighted the risks of confusion in cross-border deployments when protocols, procedures, or equipment are not aligned. They also pointed to safety risks, increased operational costs, and difficulties in procurement, certification, and training recognition across jurisdictions. In short, fragmentation imposes both human and financial costs, while eroding trust and limiting the scalability of multinational cooperation (Figure 6).

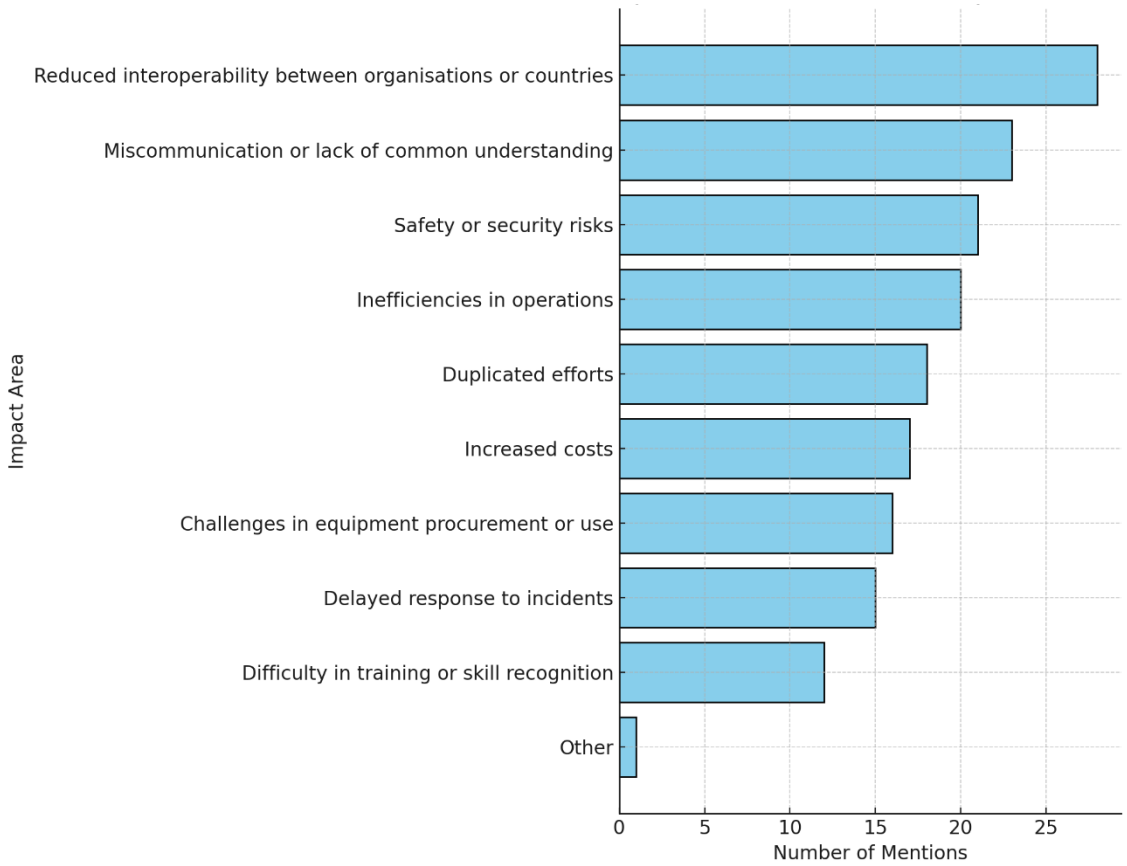

Figure 6 – Perceived impact on standardisation gaps in the CBRNe sector

When asked to prioritise areas for future standardisation, respondents placed interoperability at the top of the agenda. This emphasis was not only conceptual but highly practical, encompassing common communication protocols, compatible equipment standards, and models for seamless cross-border deployment. Training and exercises followed closely, reflecting recognition that technical tools are insufficient without shared practices, curricula, and certification frameworks that ensure mutual recognition of competences across Member States. Data sharing and information management also emerged as critical, pointing to the need for interoperable digital infrastructures that can support situational awareness and coordinated decision-making in real time. By contrast, personal protective equipment and communication systems were generally ranked lower, possibly because respondents considered these domains relatively mature or adequately regulated at the national level (Figures 7 and 8).

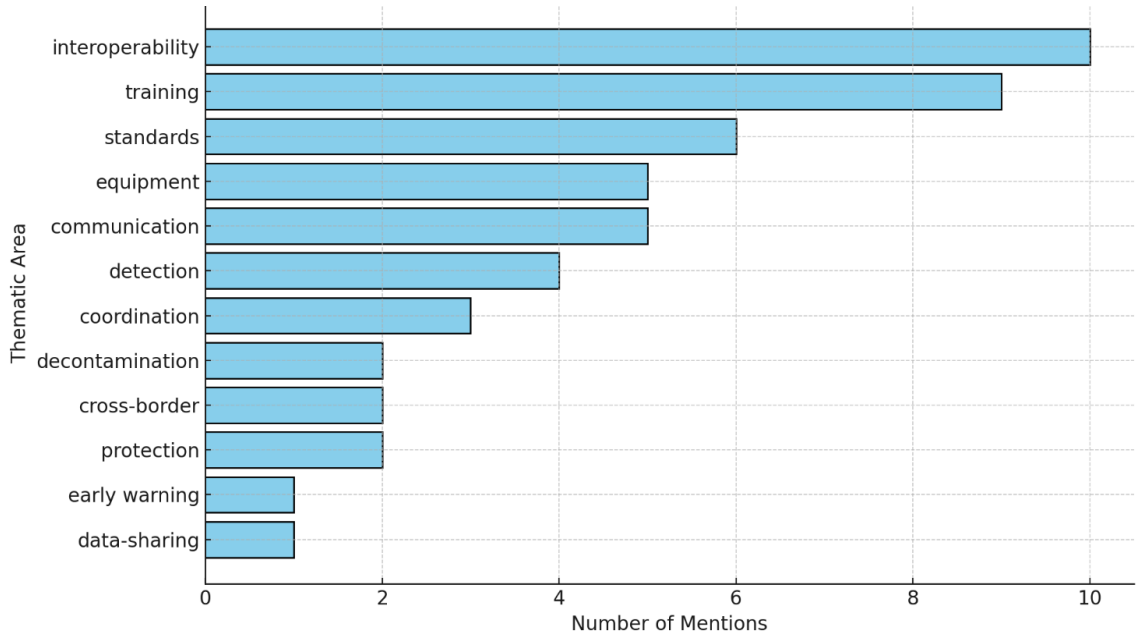

Figure 7 – Suggested areas for new or updated standards in the CBRNe sector

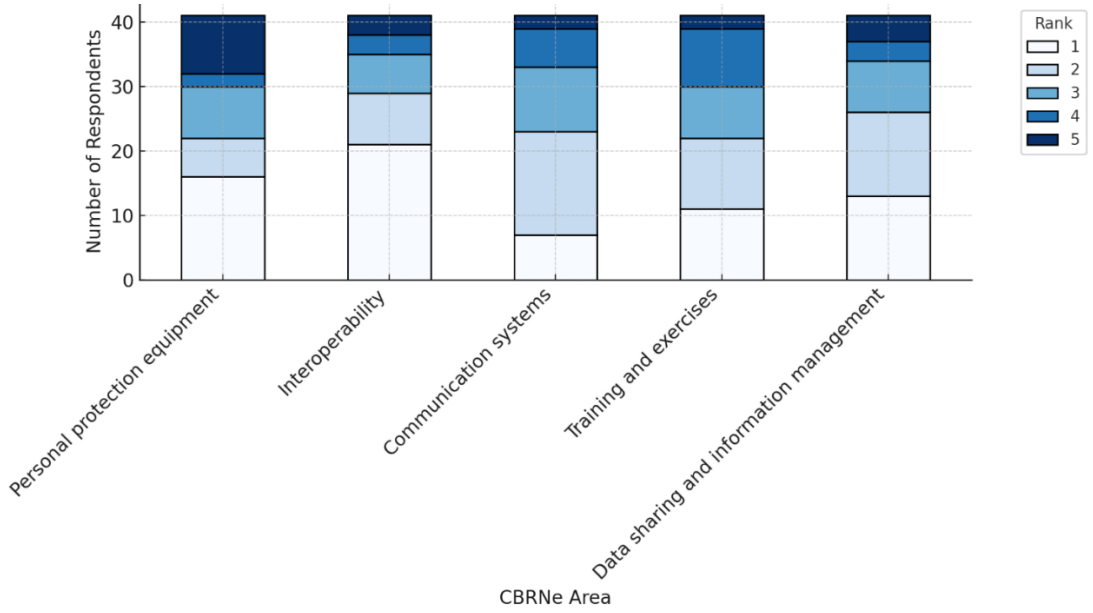

Figure 8 – Distribution of priority rankings for standardisation in the CBRNe sector

Looking beyond current gaps, respondents highlighted to be highly aware about the complexity of emerging risks. Hybrid threats and Artificial Intelligence (AI) were highlighted as transformative drivers of change, demanding new governance frameworks as well as technical responses. Synthetic biology, climate change, and cyber-CBRNe interdependencies were also frequently cited, illustrating the perception that risks are increasingly global, interdependent, and difficult to contain. Respondents warned of regulatory myopia, noting the danger of focusing narrowly on familiar technologies while underestimating disruptive developments that may redefine the threat landscape in the near future (Figure 9).

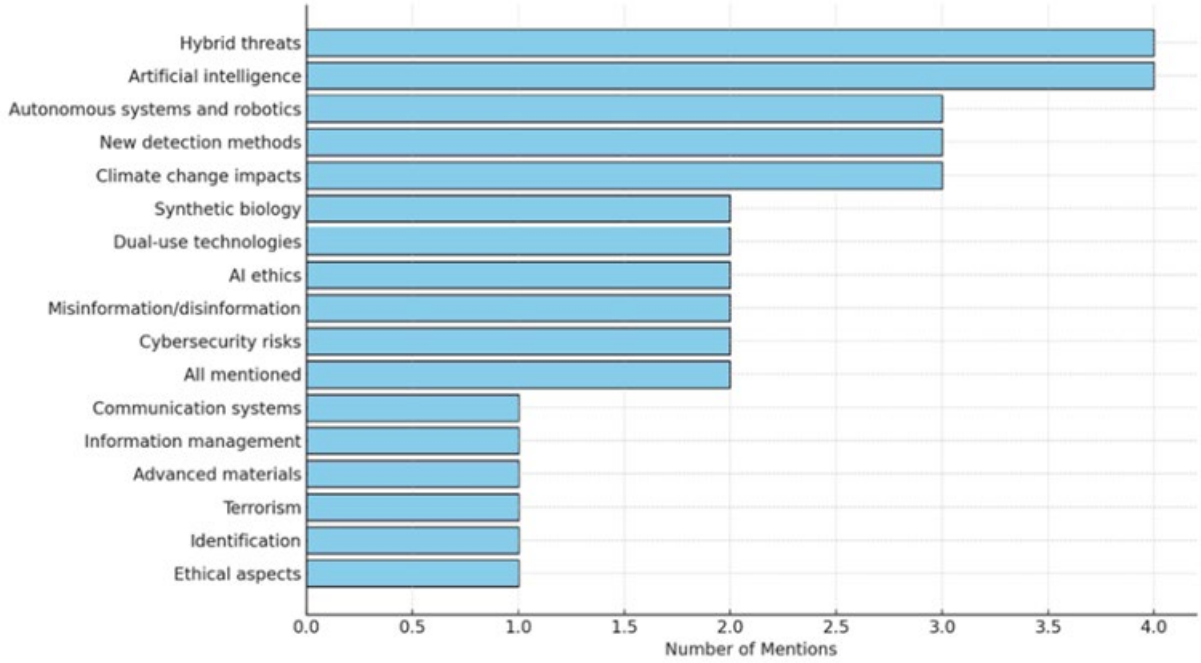

Figure 9 – Emerging challenges for future standards in the CBRNe sector

The scenario-based questions revealed both optimism and concern. On the one hand, increased European integration was widely seen as a likely and desirable trajectory, enabling greater coherence and resilience. On the other hand, fragmentation was also considered plausible, reflecting doubts about whether institutional adaptation can keep pace with technological acceleration. Climate change was repeatedly cited as a disruptive driver, as it is expected to exacerbate vulnerabilities in infrastructure, emergency response, and social stability (Figure 10).

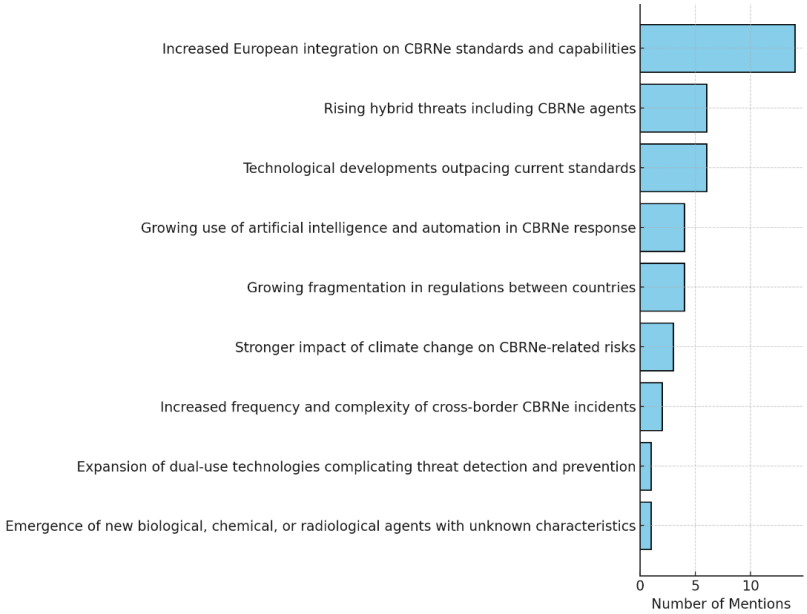

Figure 10 – Most plausible future scenarios for CBRNe standardisation over the next 10-20 years

Most respondents described their institutions as only moderately prepared for highly disruptive scenarios, with very few claiming high levels of readiness. This indicates a structural gap between risk awareness and the capacity to translate foresight analysis into preparedness (Figure 11).

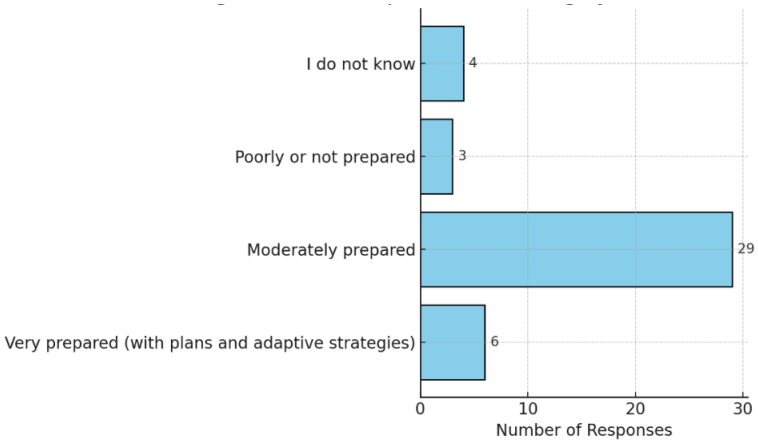

Figure 11 – Respondents' views on their organisations' readiness for highly uncertain or disruptive scenarios

The strategic reflections of respondents reinforce this picture. A majority called for stronger European integration of standards and capabilities, arguing that fragmented national approaches are inadequate in the face of transboundary risks. Funding emerged as the top priority, reflecting recognition that standardisation is resource-intensive and requires sustained investment in research, capability development, and innovation. Common guidelines, digital platforms, and shared databases were also highlighted as essential enablers, providing the doctrinal and infrastructural backbone for interoperability (Figure 12).

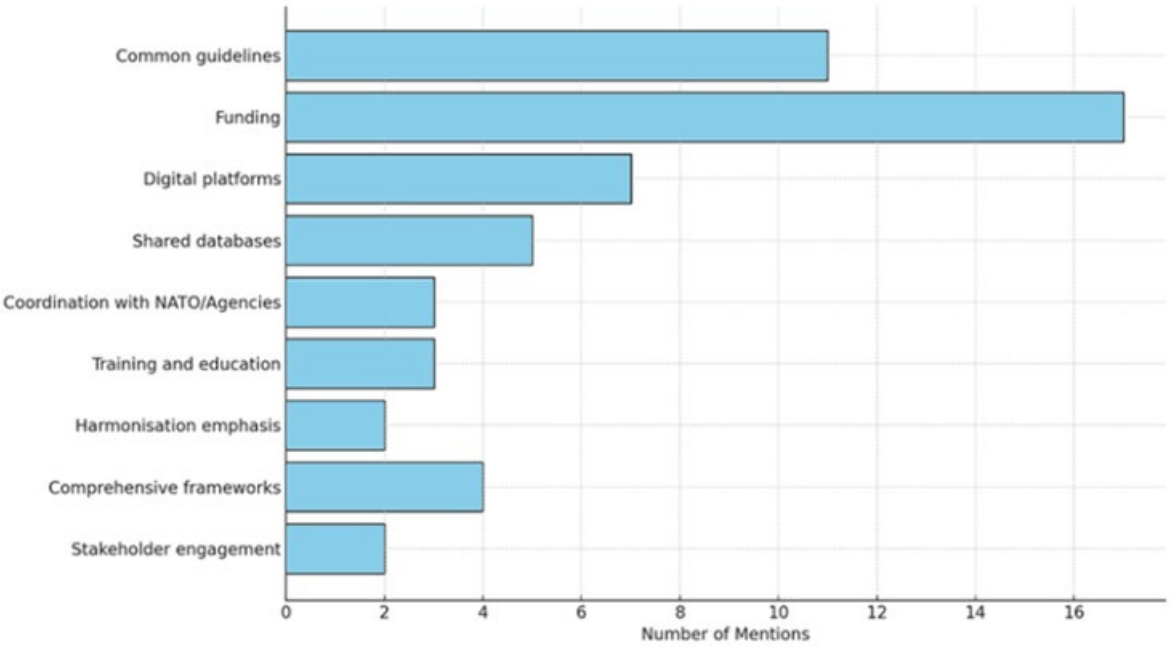

Figure 12 – Respondents' views on EU support measures for CBRNe standardisation

In addition to operational and structural priorities, respondents emphasised the importance of including ethical and societal considerations in future CBRNe standardisation. They widely agreed that standards should not focus solely on technical and procedural aspects, but must also integrate

values such as privacy, proportionality, transparency, and inclusivity. Embedding these principles systematically throughout the standardisation process is seen as essential to ensure legitimacy, public trust, and the broader acceptance of European CBRNe policies and practices (Figure 13).

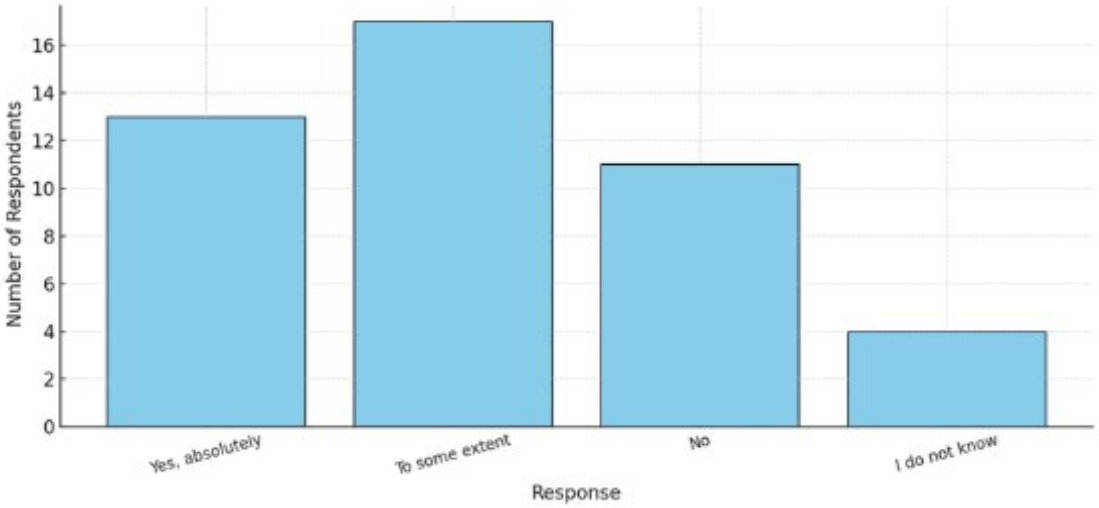

Figure 13 – Respondents' views on whether CBRNe standardisation should include social and ethical considerations

In doing so, respondents further emphasised the need for a multi-stakeholder governance model. While national governments and EU institutions remain central, many respondents recognised the importance of involving research institutions, emergency services, healthcare providers, industry, non-governmental organisations (NGOs), and the civil society. Such inclusivity was described as key to ensure legitimacy and effectiveness, though it raises challenges due to coordination and accountability (Figure 14).

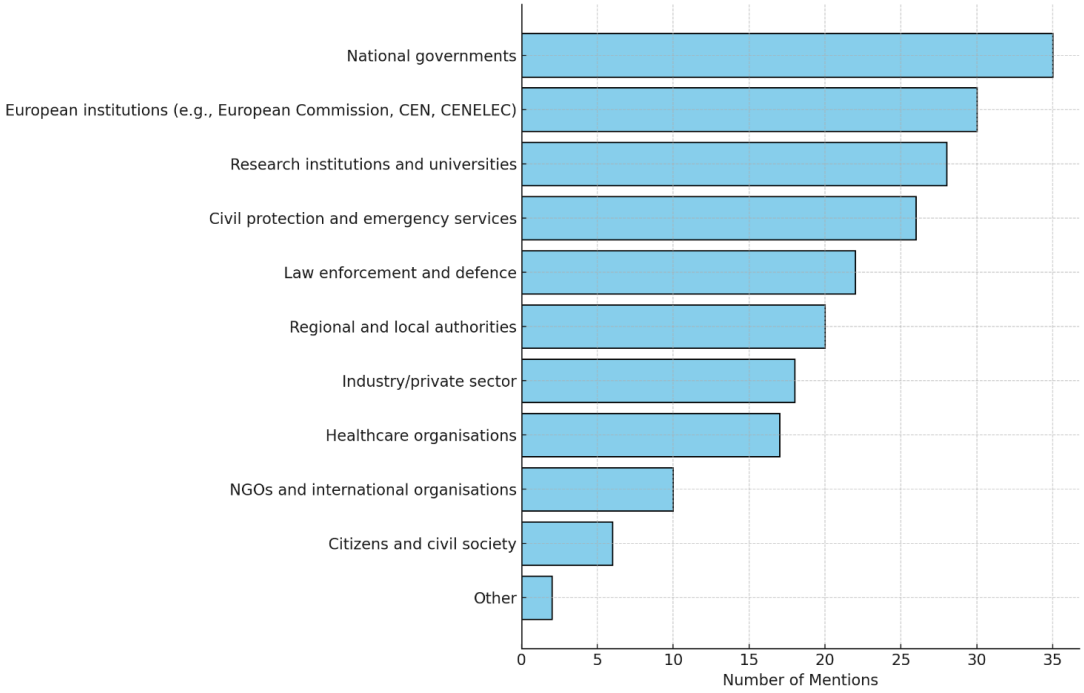

Figure 14 – Key stakeholders to be involved in future CBRNe standard development

The consultation findings collectively highlight three strategic priorities for the future of CBRNe standardisation in Europe. First, the institutionalisation of anticipatory capacities, enabling governance systems to identify, monitor, and adapt to disruptive technologies and emerging risks before they outpace regulation. Second, the consolidation of coherent and adequately resourced European frameworks, designed to overcome fragmentation and ensure sustained interoperability across Member States. Third, the integration of inclusive and ethically robust governance models, embedding transparency, legitimacy, and public trust as core operational prerequisites rather than peripheral considerations.

Respondents therefore did not advocate for a proliferation of technical documents, but for the elevation of standardisation into a strategic instrument of European security governance: anticipatory in outlook, coherent in design, inclusive in process, and resilient in practice.

5. INSIGHTS FROM THE STAKEHOLDER CONSULTATION CARRIED OUT THROUGH SEMI-STRUCTURED INTERVIEWS WITH SELECTED EXPERTS

As part of the broader investigative process surrounding the future standardisation needs in the CBRNe domain, in June and July 2025 a dedicated series of qualitative interviews was conducted with 14 experts drawn from a wide range of operational, institutional, and academic backgrounds. These individuals, spanning civil protection authorities, military and law enforcement bodies, scientific research institutions, public health organisations and field-level practitioners, offered nuanced and often divergent perspectives, which together compose a rich mosaic of experiential knowledge and critical reflection. These interviews were not merely designed to gather opinions. Rather, they aimed to elicit structured insights into the real-world frictions, gaps, and opportunities shaping the current and future landscape of CBRNe standardisation in Europe. The experts were asked to reflect on both their current operational realities and on anticipated developments in CBRNe risks, technologies, and governance frameworks. Through this lens, their responses brought to the fore lived experiences of fragmentation, coordination challenges, regulatory inertia, as well as promising avenues for transformation, innovation, and resilience-building. What emerged from these conversations is not a single, coherent narrative, but a constellation of interrelated concerns and visions, some deeply pragmatic, others more strategic and long-term. Yet, common threads can be traced, *fil rouges* that, despite originating from diverse perspectives and experiences, allow us to better grasp the emerging contours of the CBRNe standardisation landscape.

In the following sections, the expert insights are organised thematically to provide a deeper understanding of the current state of CBRNe standardisation, its foreseeable evolution, the emerging threats that challenge conventional models, and the strategic directions that might help shape a more coherent and future-ready response architecture.

5.1 STATE OF PLAY OF STANDARDISATION AND SUGGESTIONS FOR IMPROVEMENT

The current architecture of CBRNe standardisation across Europe represents an indispensable foundation for ensuring coherence, safety, and interoperability across diverse sectors. From incident response protocols to technical specifications for personal protective equipment, these standards offer a shared language and a set of expectations that help prevent fragmentation, enhance coordination, and build trust across institutional boundaries. Yet, while the system, in its formal design, is clearly robust and institutionally embedded, many of the experts interviewed highlighted the need for a more inclusive and adaptive approach, one that is attuned to the realities of practitioners, researchers, and decision-makers operating in complex and rapidly evolving CBRNe threat environments. A recurrent theme was the importance of expanding participation in the early stages of standard development. Standards are not merely technical artefacts. They are also shaped by the

social, institutional, and disciplinary positions of those who create them. At present, these processes tend to be driven by a relatively narrow set of actors, often excluding key stakeholders working in the CBRNe sector, such as first responders, regional public authorities, civil protection units, healthcare operators, and non-traditional security stakeholders. This can limit both the applicability and the legitimacy of the resulting frameworks. To address this, several interviewees called for a model of engagement that is both vertically and horizontally inclusive, one that involves stakeholders not just as end users but as co-designers. Such a shift would bring in diverse perspectives from across government, academia, civil society, and the private sector, helping to produce standards that are more grounded, flexible, and future-proof.

Equally important is the architecture of participation itself. Current governance mechanisms often follow rigid, linear procedures that can unintentionally constrain the integration of unconventional or emergent insights. Some experts suggested that more agile, adaptive decision-making chains, open to experimentation and heterodox contributions, could generate solutions better aligned with the hybrid and dynamic nature of contemporary CBRNe challenges. This is not a call to dilute technical rigour, but rather to enhance relevance by embedding standardisation within the logic of multidisciplinary collaboration.

Another theme that emerged across multiple conversations concerns the limited visibility and accessibility of existing standards. Even when high-quality and practically relevant, standards are often unknown or underutilised by those who would benefit the most. Their circulation tends to be restricted to formal institutional or regulatory pathways, with insufficient efforts to reach broader communities of practice. To address this gap, several interviewees called for more proactive and decentralised dissemination strategies, such as open-access databases, targeted stakeholder briefings, modular training resources, and digital platforms (notably those envisioned through the co-creation approach promoted by the PEERS project). These tools would not only share technical content but also help translate standards into actionable guidance tailored to real-world operational needs. Closely linked to this is the issue of narrative clarity. In complex fields such as CBRNe, standards are not self-evident. Their uptake depends on interpretability and contextual relevance. Interviewees frequently stressed the importance of supporting materials, training modules, case-based illustrations, and explanatory documents, that make protocols more intelligible and adaptable.

Communication, in this context, is not a supplementary feature. It is key to operational effectiveness. Standards that are explained, discussed, and contextualised are more likely to be embraced and consistently applied. In light of this, several interviewees proposed the creation of standardisation “ambassadors” or *liaison* figures, individuals or small teams tasked with bridging gaps between policy, science, and frontline practice. These mediators could play a vital role not only in disseminating knowledge but also in cultivating trust and alignment amongst stakeholders operating under different institutional logics, terminologies, and time horizons. Their involvement could help ensure that standards are not only technically sound but also socially embedded and legitimate. Furthermore, there was an implicit, though no less important, recognition that standardisation should be understood as a dynamic rather than a static process. In rapidly changing contexts marked by technological innovation, emerging threats, and shifting geopolitical conditions, standards conceived as fixed, one-off solutions may quickly become outdated. This raised important questions amongst the interviewees: How might we institutionalise feedback loops more effectively? What mechanisms are needed to ensure that standards are regularly revisited, revised, and revalidated in light of new evidence or field-based learning? In response of this, some interviewees advocated for lightweight, iterative consultation platforms, potentially hosted at the EU level, where CBRNe practitioners, researchers, and other stakeholders could periodically reassess the adequacy of existing frameworks and co-develop improvements.

In the end, the question may not be whether standardisation is working effectively and how, but rather whether it is functioning in ways that prepare us for the challenges ahead. The insights gathered from the interviews suggest a willingness, even a collective desire, to rethink some of the assumptions that currently shape the system. This openness, if translated into policy and practice, could become one of Europe's greatest assets in strengthening its CBRNe resilience for the years to come.

5.2 FUTURE RISKS IN THE EVOLVING CBRNE LANDSCAPE

What risks lie on the horizon for the CBRNe domain, and how should we begin to conceptualise them? This question, seemingly straightforward, unravels quickly once we begin to disentangle the sheer variety of challenges that the interviewees brought to the surface, challenges that span technology, geopolitics, regulation, society, and the very nature of risk assessment itself. If there is one consensus amongst the experts that were interviewed, it is this: the threats of the next decade will not necessarily resemble those of the past, nor will they conform to traditional categories. Risk is no longer exclusively defined by its magnitude or technical sophistication. It is increasingly defined by its hybridity, its unpredictability, and its capacity to emerge at the interstices of disparate domains, such as science and ideology, legality and criminality, innovation and neglect.

A recurring concern across the interviewees was the accelerated diffusion of technologies (and of AI, in particular) and capabilities once considered the preserve of state or elite actors. The "democratisation" of technological know-how, for all its benefits, is also enabling the development of Do-It-Yourself CBRNe tools that circumvent traditional security filters. Several experts expressed unease at the extent to which digital platforms, forums, and video tutorials now circulate detailed instructions on how to assemble explosive devices, chemical dispersal systems, or weaponised drones with off-the-shelf components. What emerges is a highly decentralised risk environment, where the material and cognitive barriers to CBRNe violence are progressively eroded. One interviewee highlighted, with some urgency, how ongoing conflicts, most notably in Ukraine and in the Middle East, are functioning as real-time testing grounds for low-cost, improvised systems such as Improvised Explosive Devices mounted on commercial drones. The fear is not only that such innovations will be exported to other conflict zones, but that they will become templates for urban, asymmetric attacks against soft targets in Europe. How does one defend against an adversary with no formal logistics chain, no identifiable infrastructure, but access to basic technology and a crowd-sourced archive of tactical knowledge?

The same logic of decentralisation applies to additive manufacturing, particularly 3D printing, which several experts flagged as a disruptive force in the near future. As this technology matures, the ability to produce weaponised components, casings, triggers, dispersal modules, without serial numbers, oversight, or supply chain traceability, could become a defining feature of emergent CBRNe threats. Unlike traditional arms trafficking, these processes bypass customs, intelligence, and international controls entirely. Are we prepared to regulate a future in which harmful devices are not trafficked, but printed, assembled, and deployed within few days?

Yet, the technological frontier is not only defined by threat vectors. It also intersects with global policy goals, particularly energy transition and green innovation, in ways that create unintended CBRNe-adjacent risks. The widespread deployment of lithium-ion batteries in electric vehicles, for instance, presents novel challenges for fire safety, chemical stability, and emergency response. Several interviewees noted that our current frameworks may be ill-equipped to handle large-scale battery incidents, which may combine toxic chemical exposure, prolonged combustion, and hazardous material contamination in ways that elude conventional response doctrines. In light of this, is the future of risk less about malevolent actors than about structural oversights in how we engineer sustainability? Another dimension that drew considerable concern is the radiological domain,

particularly the possibility that non-state actors may seek to weaponise radiological materials, not only through the classic dirty bomb archetype, but also via more insidious, concealed applications. One expert warned of the allure such devices hold: they are relatively easy to assemble, difficult to detect, and psychologically powerful in their capacity to induce fear, panic, and infrastructural paralysis without necessarily inflicting mass casualties. The threshold for creating strategic disruption is lowering, not in scale, but in subtlety. At the same time, several interviewees cautioned against techno-centric tunnel vision. While it is essential to anticipate novel, high-tech risks, it would be a serious mistake to ignore threats that are low-tech, low-cost, and high-impact. One vivid example is the potential use of pipe bombs enhanced with chemical agents, which is a tactic that might seem unsophisticated but can be devastating in enclosed public areas. Similarly, one interviewee referenced the potential weaponisation of ultrasound technology, specifically the use of sonication techniques to disperse chemical agents in liquid form. These are not abstract scenarios, but concrete, technically feasible possibilities grounded in existing science. Alongside this, the rise of emerging risks in the chemical-pharmaceutical nexus appears increasingly central. The threat posed by substances such as fentanyl, which is increasingly accessible, extremely powerful in low doses, and difficult to detect, was repeatedly cited as a major concern. The convergence of pharmaceutical innovation with criminal or terrorist intent represents a particularly challenging frontier, one where CBRNe and public health domains must work more closely than ever before. Here, cross-sector integration is not merely desirable, it is indispensable. Ultimately, experts suggest a need to think beyond dichotomies of high versus low technology. One interviewee warned against the tendency to focus exclusively on “100-click” scenarios, where sophisticated digital tools or cyber-physical systems pose cascading threats, while ignoring the “1-click” threats that remain rooted in physical, chemical, or mechanical simplicity. Both extremes can prove equally destabilising if neglected. Risk, in this sense, is defined less by complexity than by opportunity and intent.

All of these concerns point toward a CBRNe risk landscape that is no longer vertical, contained, or easily mapped. It is horizontal, networked, and interpenetrating. It merges the digital and the material, the accidental and the intentional, the high-concept and the seemingly mundane. And it demands new forms of preparedness, not only in terms of detection, response, or mitigation, but in how we think.

Should we continue to plan for threats as discrete events, or should we begin to model risk as a complex, adaptive system where feedback loops, copycat dynamics, and emergent behaviours become central features? How can foresight be reconfigured not merely to predict, but to perceive, to attune to weak signals, marginal cases, and systemic vulnerabilities that may otherwise escape detection until it is too late?

Crucially, the future of CBRNe risk cannot be understood in isolation from social and political contexts. Technological capacity is only one side of the equation. The willingness to use, the capacity to improvise, the symbolic power of CBRNe agents, all of these are socially constructed, contested, and subject to change. The line between risk and panic, incident and disinformation, preparedness and securitisation, is a thin and shifting one. Thus, while it is tempting to frame future risks as “emerging”, the more accurate descriptor may be "converging": a coalescence of new tools, old resentments, global inequalities and fragmentation, producing a threat environment that defies silos, challenges assumptions, and demands a fundamentally different cognitive posture from all actors involved.

And so, we are left with questions rather than answers. Can governance frameworks evolve fast enough to match the speed of innovation? Can we build institutional memory in domains that are by nature unstable? And, perhaps most importantly, can we cultivate a culture of vigilance that does not slide into paranoia, and of resilience that does not calcify into rigidity?

These are not rhetorical questions: they are operational imperatives and the future will not wait.

5.3 ENHANCING PREPAREDNESS, COORDINATION, AND RESPONSIVENESS IN THE EVOLVING CBRNE LANDSCAPE: WHAT SHOULD BE DONE?

Faced with an increasingly intricate and evolving threat landscape, one in which traditional lines between civilian and military responsibilities are rapidly blurring, the question of how to reinforce the CBRNe ecosystem, not merely in response to current challenges but in anticipation of those still emerging, has taken on an undeniable sense of urgency. The evidence gathered across the expert interviews underscores the need of a strategic pivot, one grounded in operational realism, institutional learning, and above all, a renewed focus on preparedness and human coordination.

One of the most consistent threads running through these interviews was the urgent need to broaden the scope of CBRNe training and awareness, reaching far beyond those conventionally seen as experts or specialists. While specialised technical expertise remains essential, especially in high-stakes environments involving complex substances or detection technologies, many interviewees stressed the need of embedding basic awareness, recognition skills, and behavioural guidance amongst first responders, broadly defined. This includes not only firefighters, police officers, or civil protection operators, but also educators, school personnel, municipal administrators, and even informed citizens. A culture of preparedness and prevention must be woven into the societal fabric, starting at schools and universities, where critical thinking and basic biosecurity education can help sow the seeds of future resilience. In this regard, preparedness is no longer the exclusive domain of the experts. One of the most insightful reflections captured during the interviews concerned the idea that “those who find themselves closest to the incident are often the first line of defence”. This sentiment challenges the traditional top-down logic of response hierarchies and calls instead for a more distributed model of situational awareness, where trained individuals across all levels of society can recognise, react to, and report anomalies, thus effectively becoming sentinels of public safety.

Parallel to this need for greater decentralisation is a recurrent theme, that is the value of tighter multi-level coordination. The current frameworks at EU level, while generally regarded as sound in structure, are still perceived by some as overly abstract or technocratic in practice. Several interviewees noted that meaningful progress depends on improving the interoperability and continuity between local, national, European, and international actors. NATO-EU coordination, cited multiple times as a functional and promising avenue, represents a model of effective cross-institutional cooperation, one that can and should be scaled both horizontally (across sectors) and vertically (across decision levels).

Within this broader context, the NSO plays a central role in sustaining operational interoperability amongst Allied nations through the continuous development of Standardisation Agreements and Allied Publications that establish shared doctrines, definitions, and procedures. These frameworks are not limited to military applications but also provide a reservoir of tested methodologies, technical specifications, and organisational lessons that can inform civilian preparedness and response systems. Integrating relevant NSO guidance within the EU standardisation ecosystem could therefore serve as a catalyst for greater coherence and mutual reinforcement between defence and civil protection domains.

Such alignment would allow European standardisation bodies, including CEN and CENELEC, to draw upon NATO’s long-standing experience in harmonising procedures for detection, protection, and decontamination, while ensuring that these practices are adapted to the regulatory, ethical, and societal context of the EU. By promoting structured collaboration and reciprocal transparency, the convergence of EU and NATO standardisation approaches could help build a genuinely interoperable preparedness framework, one capable of translating strategic coordination into tangible operational readiness across the entire CBRNe landscape.

Yet, this cannot happen without a more agile and responsive operational doctrine. The ability to quickly deploy modular, mobile, and interoperable units was consistently highlighted as a crucial dimension of future CBRNe preparedness. One particularly memorable observation came from an interviewee who asked, “What happens in the first thirty minutes after a CBRNe incident?”, a question that cuts through layers of policy and reveals the operational core of the issue. In this context, macro-level structures such as stockpiling and high-level contingency planning remain essential, but they must be matched by micro-level capacities: portable decontamination kits, well-equipped ambulances, and on-the-ground response teams capable of immediate action, especially in communication-degraded or contested environments.

The capacity to operate in so-called “dark zones,” where electronic warfare or infrastructural failures disrupt communications, is increasingly viewed as a critical benchmark of CBRNe resilience. In such scenarios, centralised command systems may prove insufficient. Instead, the focus shifts toward trained, semi-autonomous units empowered to act with discretion and realism, supported by scenario-based training that mirrors the chaos and uncertainty of real incidents. However, agility alone does not ensure legitimacy. Many interviewees voiced concern that the imperative to respond rapidly should not override core ethical and democratic principles. Transparency, proportionality, and societal trust emerged as non-negotiable elements of durable CBRNe governance. Standards and protocols, therefore, must be not only technically robust but also socially legitimate, subject to ethical scrutiny and inclusive of diverse, especially vulnerable, populations.

Underpinning all of these concerns is one silent but decisive factor: time. Time is not merely a constraint. It is the medium through which preparedness and response become either effective or insufficient. It is the difference between containment and escalation, between order and breakdown. Several interviewees pointed out that technical capabilities and standardised procedures mean little if they cannot be activated swiftly and cohesively. This highlights the importance of cultivating not just tools and frameworks, but the enabling conditions, clear decision chains, interoperable systems, trusted coordination networks, that make timely action possible. In the CBRNe field, where every second counts, speed is not a secondary consideration. It is the invisible infrastructure that holds all other elements together, the ultimate test of whether systems designed in advance can actually deliver under pressure. In addition, there is a shared recognition that the value of CBRNe preparedness lies not just in having the right assets, but in knowing how to use them, when to use them, and how to communicate effectively across teams and jurisdictions. Several experts advocated for a tiered training framework, one that could adapt to different actor profiles (from strategic planners to frontline operators), and that could be scaled depending on the risk level, the geographic location, and the mission type. Exercises and drills must also become more than bureaucratic formalities. They need to simulate conditions of stress, uncertainty, degraded communications, and conflicting information, which are precisely the conditions under which CBRNe incidents tend to unfold. Embedding these stressors into training was cited as a way to cultivate not just competence, but resilience and adaptive capacity under pressure.

Ultimately, the challenge is not to choose between top-down coordination and bottom-up empowerment, but to find the right balance between structure and flexibility, authority and autonomy, planning and improvisation. Building a more resilient CBRNe ecosystem will depend not on any single reform or innovation, but on a systemic reimagining of how risks are understood, how decisions are made, and how institutions communicate across silos and borders. The pathway is clear. It goes towards a more decentralised, inclusive, agile, and ethically grounded ecosystem, one that acknowledges the limitations of any single actor, and that places collective intelligence at the centre of CBRNe preparedness. Whether the EU can rise to this challenge will depend not only on its political will and technical resources, but also on a shared commitment to vigilance, humility, and the belief that the unthinkable, while never fully preventable, can be anticipated, prepared for, and ultimately mitigated, if we act with coherence and foresight.

5.4 RETHINKING CBRNE RESILIENCE THROUGH MULTI-STAKEHOLDER COOPERATION, TIMING AND SHARED UNDERSTANDING

Reflecting on the breadth of the insights gathered, it becomes increasingly clear that strengthening the CBRNe domain will not be achieved through technological breakthroughs alone, nor through the refinement of existing protocols in isolation. What gradually comes into focus is the importance of complementing existing approaches with broader cultural and structural sensibilities, ones that take into account the interdependent, multi-stakeholder nature of preparedness in today's evolving risk environment. This is not merely about designing better tools or drafting more comprehensive policies, it is about cultivating a new orientation toward complexity, responsibility and collective capability.

To begin with, standardisation cannot remain a technical issue handled by select institutions or top-down processes. What emerges instead is the necessity for a broader ecology of contribution, in which CBRNe stakeholders from across the operational, scientific, policy, and civil landscapes are engaged meaningfully in defining what "standards" should reflect in the real world. It is not simply a question of expanding stakeholder lists, but of fostering an architecture of co-design, where different forms of expertise are not only heard, but structurally incorporated. This means, amongst others, asking ourselves what it would truly entail to design frameworks not merely for frontline actors, but with them. Inclusion, in this light, becomes not just a democratic value, but a functional need.

At the same time, risk awareness must escape the binary between high-tech futures and low-tech negligence. We are indeed entering an era in which emerging technologies, AI, advanced materials, autonomous systems, will reshape both the threat landscape and our defensive capabilities. But within this transformation, there remains a crucial blind spot, that is the enduring simplicity with which harm can be delivered. We cannot afford a future preparedness strategy that is captivated by the elegance of innovation while underestimating the effectiveness of more rudimentary, low-cost, high-impact methods. Planning only for the "100-click" scenarios, while neglecting the "1-click" threats, is a strategic vulnerability that must be actively countered.

This leads us directly to a third, often underestimated dimension: time. Not in the abstract sense of long-term policy planning, but in the very tangible reality of minutes and hours, how quickly information flows, how rapidly protective systems are deployed, how fast local actors can move from confusion to coordination. Resilience is not simply measured by the resources at one's disposal, but by the speed and agility with which those resources can be activated. The most advanced detection device or sophisticated command system means little if it cannot be used in the right place, at the right time, by the right person.

Finally, the most strategic investment of all may well be in a shared cultural understanding of the CBRNe domain. This does not mean asking society to become experts in e.g., toxicology or radiological protocols. Rather, it means cultivating a common language, a baseline of awareness, and a set of civic intuitions about what these threats are, how they manifest, and what forms of collective response they require. From schools to healthcare operators, from first responders to local administrators, diffused knowledge becomes a multiplier of operational capacity. And it is here, arguably, that the line between preparedness and prevention becomes thinnest.

Moving toward a resilient future in the CBRNe field demands that we think less in terms of control, and more in terms of cohesion, less about perfection, and more about connection. The four *fil rouges* that emerged throughout this work (i.e., inclusive standardisation, realistic threat modelling, temporal responsiveness, and widespread awareness), are not parallel concerns to be addressed in silos. They are overlapping conditions that must be met in concert, each reinforcing the others. Only through this integrative lens we can begin to shape a preparedness culture that is capable not only of responding

to crises, but of anticipating, absorbing, and transforming them into catalysts for long-term collective security.

6. FORESIGHT ANALYSIS

In a rapidly evolving security landscape characterised by technological innovation, ecological transformation, and the emergence of increasingly hybrid threats, the capacity to anticipate and adapt has become a fundamental requirement for all actors involved in CBRNe preparedness and response (Trump et al., 2021; Vallerand & Masys, 2023). Rather than discarding established frameworks, the challenge lies in their continuous refinement, ensuring that practices, protocols, and tools remain aligned with evolving operational, technological, and societal dynamics (Antoniazzi, 2022; Maurer & Kellenberger, 2019). This calls for a proactive stance grounded in preparedness, co-development, and harmonisation, where standardisation is no longer seen as a static endpoint, but as a dynamic, enabling process embedded across the entire life cycle of risk governance (European Commission, 2017; Poustourli et al., 2020). At the heart of this vision lies the recognition that robust and future-oriented standardisation frameworks are key to guarantee not only technical interoperability and operational efficiency, but also ethical accountability, transparency, and trust in high-stakes decision-making environments (Gawlik-Kobylińska, 2022; Long, 2021). In particular, the increasing complexity of CBRNe risk scenarios, driven by climate volatility, the integration of AI and autonomous systems, and the convergence of civil and military operational domains, amongst others, requires that standards are flexible, inclusive, and co-created by the very professionals who will apply them in practice (Ajaykumar, 2024; Mokili & Olsson, 2022). This is the approach adopted by the PEERS project, which aims to strengthen the EU's operational security policies through the development of a practitioner-driven ecosystem focused on pre-normative processes, standardisation pathways, and applied supporting tools. PEERS has promoted a collaborative, multi-actor approach to CBRNe preparedness and response, fostering co-creation between experts, end-users, researchers, and policymakers.

The following foresight analysis reflects the strategic orientation of PEERS. It approaches the future of CBRNe standardisation not as a reactive mechanism, but as a proactive infrastructure of resilience. Through the integration of anticipatory analysis, scenario development, and practitioner insights, it seeks to promote a coherent, inclusive, and future-ready approach to risk governance. Its objective is not only to enhance technical capacity, but to contribute to the setup of a harmonised, ethically grounded, and operationally effective framework for CBRNe preparedness across the EU and beyond.

6.1 KEY FINDINGS

The foresight analysis carried out within the PEERS project provides a structured exploration of the systemic transformations that will shape the future of CBRNe preparedness and response in Europe. Rather than treating disruptive forces as external shocks to be absorbed by existing frameworks, the analysis recognises them as drivers of a profound reconfiguration of governance itself (Vallerand & Masys, 2023). The six domains identified (i.e., AI and autonomous systems, synthetic biology, climate volatility, disinformation, nuclear fragility, and critical infrastructural dependencies) together illustrate the scale and scope of the adaptation required.

AI and autonomous systems represent a decisive inflection point. Their integration into detection, classification, and operational decision-making holds the potential to reduce exposure of human responders and accelerate crisis management (NIST, 2024; Mokili & Olsson, 2022). At the same time, the opacity of algorithmic processes and the displacement of responsibility from human operators to machine logics introduce significant ethical, legal, and institutional dilemmas (Azhar, 2021).

Standardisation must therefore move beyond performance metrics to codify principles of transparency, oversight, and contestability, ensuring that AI strengthens resilience rather than introducing systemic vulnerabilities (Trump et al., 2021; Gawlik-Kobylińska, 2022).

Synthetic biology demonstrates the transformation of biological risk from taxonomically defined pathogens to programmable and potentially untraceable constructs (DiEuliis et al., 2024; Jin & Linkov, 2021). Advances in gene editing, AI-assisted design, and decentralised experimentation accelerate innovation while simultaneously eroding the boundaries of oversight (Novossiolova & Martellini, 2021). The foresight analysis highlights that static standards are ill-suited to this domain. Preparedness increasingly depends on adaptive and function-oriented governance architectures capable of recognising programmable behaviours, integrating real-time surveillance, and enforcing traceability across the entire design-to-deployment lifecycle (Abaimov & Martellini, 2020).

Climate volatility emerges as a transversal amplifier of CBRNe risks (Wilbanks, 2017; Asaka & Denham, 2023). Rising temperatures, shifting hydrological patterns, and the destabilisation of ecosystems affect the behaviour of hazardous substances, undermine the integrity of infrastructures, and blur the distinction between natural and technological incidents (Antoniazzi, 2022). In this context, preparedness requires climate-informed standards that integrate environmental intelligence into detection systems, predictive maintenance protocols, and multi-hazard response models (Gupta & Nair, 2011). These standards must also address distributive fairness, ensuring that vulnerable communities are not disproportionately exposed to cascading risks (Cutter et al., 2025).

Disinformation has evolved into a critical dimension of CBRNe risk. Synthetic media, manipulated sensor data, and algorithmic amplification can undermine public trust, distort institutional communication, and paralyse coordinated responses (Giese, 2023). Governance must therefore protect not only the material dimension of risk but also the cognitive environment in which crises unfold (Vallerand & Masys, 2023). Standardisation is required to create infrastructures of credibility, embedding cryptographic provenance, secure communication protocols, and inclusive strategies for transparent and culturally resonant risk communication (European Commission, 2017; Trump et al., 2021).

The nuclear domain reflects the fragility of long-standing governance architectures. The diffusion of small modular reactors, the weakening of verification regimes, and the emergence of cyber threats against nuclear infrastructures create an environment of fragmentation and asymmetry (NATO, 2022; Lentner, 2017). In this context, standards must function as distributed infrastructures of trust, enabling adaptive verification, securing cyber-physical systems, and embedding accountability even where multilateral consensus is fragile or absent (IAEA & Joint Research Centre, 2014).

Finally, the reliance on orbital assets, rare isotopes, and globalised supply chains introduces systemic dependencies that both enable and threaten resilience (Vaseashta, 2018; Szklarski, 2023). Satellite constellations, specialised materials, and AI-mediated logistics form the backbone of modern preparedness, yet they remain vulnerable to disruption, manipulation, or strategic denial (Trump et al., 2021). Standardisation must therefore expand beyond traditional hazard management to include orbital resilience, material traceability, and supply chain integrity, reinforcing the infrastructures that sustain detection, attribution, and coordinated response (Vallerand & Masys, 2023).

6.2 STRATEGIC REFLECTIONS

Viewed as a whole, the foresight analysis underscores a series of structural imperatives that extend beyond the individual trends themselves. What emerges is not merely a catalogue of technological or environmental disruptions, but a coherent signal that European CBRNe governance must evolve into

a dynamic and anticipatory infrastructure (Trump et al., 2021; Novossiolova & Martellini, 2021). The challenges posed by AI, synthetic biology, climate volatility, disinformation, nuclear fragility, and supply chain dependencies cannot be addressed in isolation. They interact, reinforce one another, and generate complex, often unpredictable cascades of risk (Wilbanks, 2017; Sprenger, 2020).

From this perspective, standardisation must be reconceptualised as an enabling system rather than a static regulatory endpoint (Poustourli et al., 2020). It requires mechanisms of continuous validation, adaptive revision, and iterative co-production with CBRNe practitioners and experts (European Commission: Joint Research Centre, 2025; Civil Protection Knowledge Network, 2025). It also demands interoperability not only across Member States, but across technological and operational domains (being them digital, biological, environmental, or cognitive) that increasingly intersect in ways that blur traditional boundaries (Trump et al., 2021; Mokili & Olsson, 2022).

Equally important, legitimacy and ethical accountability are no longer peripheral considerations: they are fundamental preconditions for effective crisis governance, shaping public trust, compliance, and the credibility of cross-border operations (Gawlik-Kobylińska, 2022; Long, 2021). Ultimately, the foresight analysis conveys a strategic imperative: to reposition CBRNe standardisation as a multidimensional governance instrument, anticipatory in outlook, interoperable in practice, and ethically anchored in design (Vallerand & Masys, 2023; Trump et al., 2021). Only by embracing this transformation can the EU develop a framework that is resilient, future-ready, and capable of navigating the accelerating disruptions that will define the coming decades (European Commission, 2017; Novossiolova & Martellini, 2021).

7. POLICY RECOMMENDATIONS AND FINAL REMARKS

As highlighted throughout this White Paper, enhancing Europe's CBRNe preparedness and response capabilities would greatly benefit from a more nuanced and forward-looking approach to standardisation, one that is capable of evolving alongside emerging threats, operational complexities, and technological innovation.

In a context that is increasingly shaped by the complexity of transboundary threats, the accelerating pace of dual-use technological developments, and the evolving fragmentation of regulatory landscapes, there is a growing need to reconsider the role of standardisation, not merely as a technical endpoint, but as a potential enabler of more strategic, anticipatory, and adaptive forms of governance. In this sense, effective standardisation must operate at two interdependent levels: at the macro level, it must enable long-term, strategic coordination across jurisdictions, infrastructures, and policy domains, and at the micro level, it must provide actionable, reliable, and intuitive tools for practitioners who operate under pressure, often with limited time and incomplete information. Thinking "100 clicks ahead" is indispensable for strategic foresight and systemic resilience, but this must be matched with the ability to support "1 click at a time" operational realities, particularly in training, decision support, and real-time response environments.

The following policy recommendations are proposed as a contribution to an evolving discussion on how to align future standardisation efforts with the operational realities, strategic priorities, and anticipatory needs emerging within the CBRNe domain. They reflect a synthesis of foresight analysis, stakeholder input, and empirical evidence gathered throughout the PEERS project, and are intended to support both immediate enhancements and longer-term policy development across the EU standardisation landscape.

I. **Encouraging the development and institutionalisation of more flexible, adaptive, and accelerated standardisation pathways, that can respond to the pace of technological innovation and the unpredictability of emerging risks.** These pathways refer to the processes and governance mechanisms through which standards are conceived, tested, and validated. They encompass pre-normative activities, experimental frameworks, and fast-track procedures designed to shorten the distance between research and regulation. Establishing such agile pathways would ensure that new knowledge and operational insights are rapidly converted into structured guidance, enabling European standardisation to anticipate disruption rather than react to it.

II. **Supporting the development of modular, interoperable, and context-sensitive standards as the concrete outcomes of the aforementioned pathways, as described in Recommendation I above**. While the aforementioned pathways describe how standards are produced, standards themselves define what is produced: the shared technical, procedural, and ethical reference points that anchor interoperability and mutual recognition across Member States. These standards should be designed in a flexible manner, to adapt to diverse national operational scenarios while maintaining coherence at the European level. Strengthened coordination between European and international standardisation bodies, including NATO and its Standardisation Office, would facilitate the integration of these standards into a single, complementary framework that bridges regulatory, technical, and practitioner-driven dimensions.

III. **Ensuring that ethical, legal, and societal considerations are not treated as external or secondary to the standardisation process, but rather systematically embedded within its conceptual design, procedural development, and implementation mechanisms.** This is particularly critical in domains such as algorithmic decision-making, biometric surveillance, data governance, and dual-use research, where the implications of standardisation choices extend well beyond technical performance, affecting fundamental rights, public accountability, and democratic legitimacy. Standard-setting bodies, regulatory authorities, and research institutions should therefore adopt inclusive, interdisciplinary approaches that incorporate the expertise of ethical experts, legal scholars, social scientists, and civil society actors alongside technical experts. By doing so, it becomes possible to identify context-specific risks, anticipate unintended consequences, and develop safeguards that reinforce public trust.

IV. **Developing a coherent and integrated training and dissemination ecosystem that ensures standards are not merely produced and published, but actively understood, operationalised, and stress-tested across relevant user communities.** This entails the creation of multilingual digital platforms, practitioner-oriented e-learning modules, and scenario-based simulations capable of replicating complex, real-world conditions. Particular emphasis should be placed on ensuring that training content is modular, updatable, and responsive to technological and procedural evolution, enabling both foundational capacity building and advanced specialist training. At the same time, access to critical CBRNe-related standards and associated guidance materials should be made open or publicly subsidised, especially for emergency responders, municipal actors, and small-scale operators, recognising that preparedness-related knowledge constitutes a public good. However, this openness must be carefully calibrated against the need to manage sensitive or security-relevant information, especially in domains such as medical countermeasures, synthetic biology, and biosecurity, where premature disclosure or uncontrolled dissemination could lead to misuse. Therefore, dissemination frameworks must be accompanied by robust access controls, risk-based classification protocols, and clear governance procedures to ensure that transparency and accessibility are balanced with responsibility, confidentiality, and public safety. Furthermore, future standardisation efforts should incorporate continuous feedback loops and evaluation

mechanisms to assess their real-world effectiveness over time. This includes the systematic collection of implementation data, operational feedback from end-users, and periodic reviews to update or review standards in light of evolving conditions and lessons learned.

V. **Encouraging sustained cross-sectoral dialogue and structured co-creation processes between standardisation bodies, research communities, operational end-users, and relevant regulatory actors, ensuring that real-world expertise, constraints, and insights are embedded into normative frameworks from the earliest stages of development.** This collaborative approach is essential to avoid the disconnect that often arises between technical standards and operational applicability, particularly in high-risk, time-sensitive environments such as CBRNe preparedness and response. The factor of time must be explicitly addressed, not only in terms of the urgency and responsiveness required during crises, but also with regard to the life cycle of standards themselves, which must be developed, validated, updated, and disseminated at a pace commensurate with the rapid evolution of technologies, threat vectors, and institutional needs. Effective co-creation is therefore not a one-off consultation exercise, but an ongoing, iterative process that aligns normative development with the temporal realities of field operations, strategic planning, and technological deployment.

Taken together, these recommendations underscore the need for a more agile, inclusive, and forward-looking standardisation paradigm, one that can translate strategic foresight into operational readiness. By embedding adaptability, collaboration, and accountability at the core of standard-setting processes, Europe can reinforce its leadership in CBRNe resilience and build a more secure, interoperable, and anticipatory response framework for the challenges ahead.

8. BIBLIOGRAPHY

- Abaimov, S., Martellini, M. 2020. *21st Century Prometheus: Managing CBRN Risks in the Era of Artificial Intelligence.* Cham: Springer.
- Ajaykumar, S. 2024. *Emerging Technologies in the Development and Delivery of CBRN Threats*. Observer Research Foundation. https://www.orfonline.org.
- Antoniazzi, L. 2022. *Climate Risks and Regulatory Disruption*. Oxford: Oxford University Press.
- Asaka, J., Denham, M. 2023. "Climate-Driven Instabilities and Emergency Governance". Environmental Policy and Governance 33 (2): 121-35.
- Azhar, A. 2021. *The Exponential Age: How Accelerating Technology Is Transforming Business, Politics, and Society*. New York: Diversion Books.
- Boulet, C. A. 2006. "Development of a Science and Technology Response for CBRN Terrorism: The Canadian CBRN Research and Technology Initiative". Science and Technology Policies for the Anti-Terrorism Era, edited by Jean-Pierre Vigier, 113-29. Dordrecht: Springer.
- Bures, O. 2017. "The EU's Fight Against Terrorism: A New Strategy, but the Same Old Problems?". Terrorism and Political Violence 29 (4): 629-45.
- Civil Protection Knowledge Network. 2025. *Role of Uncrewed Vehicles in CBRN Defence*.
- Cutter, S. L., Ash, K., Emrich, C. T. 2025. *Hazards, Vulnerability, and Environmental Justice: The Next Generation*. New York: Springer.
- Danielewski, J. 2019. "CBRN Defence in the European Union: Current State and Future Challenges". European Security 28 (4): 461-80.
- DiEuliis, D., Imperiale, M. J., Berger, K. M. 2024. "Biosecurity Assessments for Emerging Transdisciplinary Biotechnologies: Revisiting Biodefense in an Age of Synthetic Biology". Applied Biosafety 29 (1): 4-12.
- European Commission. 2009. *Council Decision: Action Plan on Enhancing CBRN Preparedness and Response*. Brussels: DG HOME.
- European Commission. 2017. *EU CBRN Action Plan. SWD(2017) 124 Final*. Brussels.
- European Commission: Joint Research Centre, Plaza Jimenez, P., Garrone, B., Sabatelli, M. R., Iatan, A., Micucci, S., Busch, J., Usmanova, N., Wittermans, H., Radoini, A., Abdou Abdelhamid Mariey, H., Hamilton, R. A., Toleubayev, T., Lursmanashvili, M., Hemimou, Y., Rahmoun, J. A., Gitari, P., Povoden, G., Clevestig, P., Cheong, S., Metopishvili, E., Zavkibek, T. 2025. *15 years of international cooperation through the EU CBRN Risk Mitigation Centres of Excellence Initiative*. Bottone, S., De Bruijn, M., and Goulart, M. (eds.). Luxembourg: Publications Office of the European Union.
- European Commission News. 2025. *EU CBRN CoE Marks 15-Year Anniversary with Forward-Looking Conference*. Accessed October 23, 2025. https://cbrn-risk-mitigation.network.europa.eu/news-1/eu-cbrn-coe-marks-15-years-forward-looking-anniversary-conference-brussels-2025-05-21_en.
- European Court of Auditors. 2018. *Special Report No. 14/2018: The EU Chemical, Biological, Radiological and Nuclear Centres of Excellence – More Progress Needed*. Luxembourg: Publications Office of the European Union.
- European Parliament. 2021. *EU Preparedness and Responses to Chemical, Biological and Pandemic Threats.* EXPO_STU(2021)653645. Brussels.
- Finabel. 2020. *Civil-Military Preparedness Against CBRN Threats in Europe*. Brussels.
- Gawlik-Kobylińska, M. 2022. "Public Participation in Nuclear Safety Standardisation: Toward Inclusive Resilience". International Journal of Critical Infrastructures 18 (2): 133-50.
- Giese, R. 2023. "Navigating the Dual-Use Dilemma: AI, Biotechnology, and International Security". International Affairs 99 (1): 221-39.

- Goulart, M., Gonçalves, M., Oceano, I., Abousahl, S. 2018. “EU CBRN Centres of Excellence: Effective Solutions to Reduce CBRNE Risks”. Enhancing CBRNE Safety & Security: Proceedings of the SICC 2017 Conference, 309-16. Cham: Springer.
- Gupta, S., Nair, R. 2011. *Climate Change and Environmental Contaminants*. New Delhi: TERI Press.
- IAEA and Joint Research Centre. 2014. *Nuclear Forensics Activities Supported by the EU CBRN Action Plan*. Vienna: International Atomic Energy Agency.
- Jin, A., Linkov, I. 2021. “Synthetic Biology Brings New Challenges to Managing Biosecurity and Biosafety”. Resilience and Risk, edited by B.D. Trump, M.V. Florin, E. Perkins, and I. Linkov. OAPEN Library.
- Lentner, H. H. 2017. “Radiological Hazards and Civil Protection”. Journal of Risk Research 20 (9): 1204-25.
- Long, C. 2021. *The Molecularisation of Security: Medical Countermeasures, Stockpiling and the Governance of Biological Threats*. London: Routledge/Taylor & Francis.
- Maurer, A., Kellenberger, A. 2019. “Governing Security in the EU: The Role of Agencies in Addressing New Threats”. *Journal of European Integration* 41 (7): 967-82.
- Mokili, D., Olsson, N. 2022. “Artificial Intelligence and Biosecurity: Risks and Opportunities for Global Health Security”. Health Security 20 (6): 506-15.
- NATO. 2022. *Chemical, Biological, Radiological and Nuclear Defence Policy*. Brussels: NATO.
- NIST. 2024. *AI Risk Management Framework 1.0*. Gaithersburg, MD: U.S. Department of Commerce.
- Novossiolova, T., Martellini, M. 2021. *Effective and Comprehensive CBRN Security Risk Management in the 21st Century*. Brussels: European Non-Proliferation Consortium.
- Poustourli, A., Emmanoloudis, D., Chalaris, M. 2020. *Security Research and EU Preparedness for CBRNE Threats*. Strasbourg: CERIS.
- Ruohonen, J. 2021. “A Review of Product Safety Regulations in the European Union”. arXiv preprint, February 6. https://arxiv.org/abs/2102.02841.
- Rychnovská, D. 2016. *The Politics of Bio(in)security: Science, Experts and the Dilemma of Dual Use*. Prague: Charles University.
- Sánchez Cobaleda, A. 2015. “The CBRN Risk Mitigation Centres of Excellence of the EU: The Case of Morocco”. Paix et Sécurité Internationales 3: 159-74.
- Sprenger, A. 2020. “The COVID-19 Pandemic as a Stress Test for European Health Security”. Journal of European Integration 42 (8): 1085-99.
- Steinmüller, K. 2003. *The future as Wild Card. A Short Introduction to a New Concept*, Z_punkt GmbH, Buro fur Zukunftsgestaltung Essen and Berlin, Berlin.
- Szklarski, Ł. 2023. “CBRN Threats – Advancing National Security Through Interdisciplinary Innovations”. Zeszyty Naukowe SGSP 1 (88): 93-118. Warsaw: Szkoła Główna Służby Pożarniczej.
- Trapp, R. 2017. *The EU’s CBRN Centres of Excellence Initiative after Six Years*. Stockholm: SIPRI.
- Trump, B. D., Florin, M., Perkins, E., Linkov, I. 2021. *Resilience and Risk: Methods and Application in Environment, Cyber and Social Domains*. Cham: Springer.
- Vallerand, A. L., Masys, A. J. 2023. “Science Technology and Innovation: Transforming the Complex Safety and Security Multi-Level Landscape.” Safety and Security Science and Technology Policies, edited by A. J. Masys, 21-44. Cham: Springer.
- Vaseashta, A. 2018. “Roadmapping the Future in Defense and Security: Innovations in Technology Using Multidisciplinary Convergence.” Detection and Defence against CBRN Agents. Cham: Springer.
- Wilbanks, T. J. 2017. *Global Climate Risk, Attribution, and Conflict*. Cambridge: Cambridge University Press.

9. ANNEXES

ANNEX 1 – THE ONLINE QUESTIONNAIRE

Introduction to the online questionnaire
This survey is primarily targeted at organisations and professionals engaged at different levels of Chemical, Biological, Radiological, Nuclear, and explosive (CBRNe) activities, ranging from those with a core mandate in CBRNe response, research, or management, to those with moderate or occasional involvement, as well as institutions with limited or indirect engagement. Stakeholders may include national authorities, European institutions, emergency services, law enforcement, defence actors, healthcare organisations, research institutions, industry representatives, NGOs, and civil society actors with a role or interest in CBRNe preparedness. The aim of the questionnaire is to gather insights on organisational involvement, identify gaps in European CBRNe standardisation, assess the effectiveness of current frameworks, and explore emerging needs, innovations, and future scenarios.

By collecting diverse perspectives, this questionnaire seeks to inform and strengthen European-level coordination, foster innovation, and ensure that future CBRNe standards are effective, inclusive, and responsive to evolving threats and challenges.

This questionnaire is structured into seven sections and is available online in English.

The outcomes of this questionnaire will serve to enrich the White Paper on "*Future standardisation needs in the CBRNe domain*", which is part of the ongoing work of the Horizon Europe funded project PEERS (PracticE Ecosystem for standaRdS, Grant Agreement No.101074040). Answers to this questionnaire will be analysed in an aggregated manner.

Individual contributions provided through the open questions of the questionnaire may be eventually used in the study but in an anonymised form.

Section 1: General information
*(Questions marked with * are mandatory)*

* Full name:

* Organisation:

* Organisation type:
- Public authority / regulatory body
- Law enforcement / defence
- Healthcare operator
- Industry / private company
- Research / academia
- NGO / International organisation
- Training centre
- Other (please specify)

* Role/position:

* Sector of work:
- Healthcare

- Energy
- Critical infrastructure
- Environmental protection
- Emergency response
- Public administration
- Education
- Research and development
- Manufacturing
- Information technology
- Other (please specify)

* E-mail:

* Country:

Section 2: Involvement in the CBRNe domain
*(Questions marked with * are mandatory)*

***** To what extent is your organisation involved in CBRNe activities?

- High: CBRNe activities are a core part of my organisation's mandate or daily operations (e.g., direct response, planning, or management of CBRNe events; regular handling of CBRNe materials; frequent training or research in the field).
- Moderate: CBRNe activities are a significant but not central part of my organisation's work (e.g., occasional projects, response, or research; participation in CBRNe-related exercises or collaborations).
- Low: CBRNe activities are peripheral or infrequent in my organisation (e.g., rare involvement in CBRNe incidents, occasional training or awareness).
- None: My organisation does not engage in any CBRNe activities.

* Which CBRNe areas are the most relevant to you? Select all that apply.

- Chemical
- Biological
- Radiological
- Nuclear
- Explosive
- Interdisciplinary/integrated

Section 3: Standardisation needs
*(Questions marked with * are mandatory)*

* In your opinion, what are the main current gaps in standardisation in the CBRNe sector at the European level? Select all that apply.

- Lack of interoperability standards
- Absence of harmonised protocols for decontamination
- Insufficient training guidelines
- Inconsistency in equipment certification
- Gaps in cross-border communication and coordination
- Lack of standardized procedures for emergency response
- Limited availability of validated reference materials or databases
- Insufficient guidance for risk assessment and management

- Other (please specify)

* What has been the impact of these standardisation gaps? Select all that apply.
  - Inefficiencies in operations
  - Safety or security risks
  - Duplicated efforts
  - Delayed response to incidents
  - Increased costs
  - Miscommunication or lack of common understanding
  - Reduced interoperability between organisations or countries
  - Challenges in equipment procurement or use
  - Difficulty in training or skill recognition
  - Other (please specify)

* Are there any specific areas (e.g., personal protection, interoperability, communication, training) that you believe need new standards and/or updates?
  - Yes
  - No
  - I do not know

* Based on your experience and expertise, please rank the following areas in order of priority for standardisation within the CBRNe field, with 1 being the most important to you and 5 being the least important.

	1	2	3	4	5
Personal protection equipment					
Interoperability					
Communication systems					
Training and exercises					
Data sharing and information management					
Other (please specify)					

* How effective do you find the current European regulatory framework in the CBRNe field?
  - Very effective: The regulatory framework fully supports and facilitates CBRNe preparedness and response. Very few, if any, improvements are needed.
  - Fairly effective: The regulatory framework is generally supportive, but some areas require improvement or updating.
  - Slightly effective: The regulatory framework addresses a few important issues, but significant gaps or shortcomings remain.
  - Ineffective: The regulatory framework does not adequately address CBRNe challenges or provide meaningful support.
  - I do not know enough to assess: I am not sufficiently familiar with the European regulatory framework to provide an informed answer.

Section 4: Foresight and innovation
*(Questions marked with * are mandatory)*

* Does your organisation actively monitor future trends in the CBRNe domain?
  - Yes, in a structured way (e.g., dedicated unit, foresight tools)
  - Yes, but informally

- No
- I do not know

* What emerging changes do you consider the most relevant for the future of CBRNe standardisation (e.g., dual-use technologies, hybrid threats, AI ethics, synthetic biology, advanced materials, autonomous systems and robotics, new detection methods, misinformation/disinformation during emergencies, climate change impacts, cybersecurity risks in critical infrastructure, etc.)?

_____

* Do you think CBRNe standardisation should include social and ethical considerations (e.g., privacy, equity, responsible innovation)?

- Yes, absolutely
- To some extent
- No
- I do not know

Section 5: Future vision and scenarios
*(Questions marked with * are mandatory)*

* What new technologies or emerging threats do you think should be addressed through standardisation in the next 5-10 years? Select all that apply.

- Artificial intelligence and machine learning for detection, response, or risk assessment
- Autonomous systems and robotics for CBRNe operations
- Synthetic biology and genetic engineering with potential CBRNe applications
- Advanced materials and nanotechnology for protection, detection, or decontamination
- Dual-use technologies relevant to CBRNe threats
- Drone and unmanned systems for surveillance or response in CBRNe incidents
- Quantum technologies for secure communication or threat detection
- Cybersecurity threats to CBRNe-related infrastructure and systems
- Hybrid threats (combining CBRNe risks with conventional or cyber-attacks)
- Chemical and biological weapon advancements
- Threats linked to climate change impacting CBRNe preparedness (e.g., extreme weather, infrastructure resilience)
- Disinformation/misinformation affecting CBRNe emergency management
- Other (please specify)

* Which of the following future scenarios do you consider most plausible for the next 10-20 years? Select up to 2 options.

- Increased European integration on CBRNe standards and capabilities
- Growing fragmentation in regulations between countries
- Rising hybrid threats including CBRNe agents
- Stronger impact of climate change on CBRNe-related risks
- Technological developments outpacing current standards
- Expansion of dual-use technologies complicating threat detection and prevention
- Greater involvement of private sector and non-state actors in CBRNe preparedness
- Growing use of artificial intelligence and automation in CBRNe response
- Increased frequency and complexity of cross-border CBRNe incidents
- Wider adoption of digital tools for monitoring, detection, and coordination
- Greater emphasis on social and ethical aspects in CBRNe policy and standardisation

- Emergence of new biological, chemical, or radiological agents with unknown characteristics
- Other (please specify)

* How prepared is your organisation to respond to highly uncertain or disruptive future scenarios (i.e., wild cards)?
- Very prepared (with plans and adaptive strategies)
- Moderately prepared
- Poorly or not prepared
- I do not know

* What do you think is the ideal role of European institutions and standardisation stakeholders (e.g., CEN, CENELEC, European Commission) in future CBRNe standardisation? Select all that apply.
- Coordinating and harmonising CBRNe standards across Europe
- Facilitating knowledge and best practice sharing amongst Member States
- Providing funding and support for research and innovation in CBRNe standardisation
- Ensuring the inclusion of social and ethical considerations in standards
- Promoting stakeholder engagement and cross-sector collaboration
- Monitoring and evaluating the implementation of standards
- Supporting training and capacity building
- Responding rapidly to new threats and emerging technologies
- Other (please specify)

Please elaborate or suggest additional roles you consider important:

_____

* Would your organisation be interested in participating in future working groups or consultations on CBRNe standardisation?
- Yes
- No
- I do not know

Section 6: Institutional support and cooperation
*(Questions marked with * are mandatory)*

* In your view, how should the EU better support CBRNe standardisation in the coming years (e.g., funding, common guidelines, digital platforms, shared databases, etc.)?

_____

* Which actors should be more involved in defining future CBRNe standards? Select all that apply.
- National governments
- Regional and local authorities
- European institutions (e.g., European Commission, CEN, CENELEC)
- Industry/private sector
- Research institutions and universities
- Healthcare organisations
- Civil protection and emergency services
- Law enforcement and defence
- NGOs and international organisations

- Citizens and civil society
- Other (please specify)

Please elaborate or suggest additional stakeholders you consider important.

Section 7: Final remarks

Do you have any further suggestions, recommendations or comments on the topic?

ANNEX 2 – SCRIPT OF THE INTERVIEWS CARRIED OUT WITH SELECTED EXPERTS

This interview will take place in the context of the White Paper on "*Future standardisation needs in the CBRNe domain*", which is part of the ongoing work of the Horizon Europe funded project PEERS (PracticE Ecosystem for standaRdS, Grant Agreement No.101074040). The discussion aims to capture expert perspectives on the evolving challenges, opportunities, and priorities in CBRNe standardisation. Through an open dialogue, the interview will explore how standards are currently understood and applied, how they might need to adapt to emerging risks and uncertainties, and what role different actors (e.g., from policymakers and practitioners to civil society) should play in shaping them. Key areas of focus will include rethinking the purpose and impact of standards, anticipating future technological and societal dynamics, examining governance and institutional roles, and articulating a long-term strategic vision for a more inclusive, resilient, and forward-looking European standardisation ecosystem. Insights gathered will directly inform the White Paper's recommendations, ensuring they are grounded in diverse expertise and oriented toward practical and future-relevant solutions.

Areas of discussion
The following are the areas of discussion that will be covered during the interview and the possible questions that will be raised.

1. *Opening remarks*

- Can you briefly introduce your current role and how your expertise connects to the CBRNe domain?
- In your view, what is a key challenge or blind spot in current CBRNe thinking that deserves greater attention?

2. *Rethinking standardisation*

- What, in your view, should a "standard" represent in today's complex risk environment? Is it a technical tool, a governance instrument, a shared narrative?
- What tensions do you observe between the need for robust standards and the imperative for adaptability and innovation?
- Have you witnessed situations (positive or problematic) where a standard had a major impact on cooperation, trust, or operational effectiveness?
- Are there any areas where standardisation may unintentionally hinder progress or reinforce outdated practices?

3. *Future dynamics and strategic foresight*

- Looking ahead 10 to 15 years, what emerging developments (technological, environmental, societal, or geopolitical) do you believe will most profoundly affect the CBRNe domain?
- Are there any “non-traditional” threats or disruptions that, in your view, are not yet adequately addressed in strategic or normative planning (e.g., misinformation, dual-use innovation, climate-triggered infrastructure failures, synthetic biology, AI-driven systems, etc.)?
- How can standardisation processes be designed to better anticipate and accommodate unknowns or disruptive change?
- Do you see a need to embed ethical, societal, or human rights considerations more explicitly within future CBRNe standards? If so, how might this be operationalised?
- What role should public trust, risk perception, or societal values play in shaping what is standardised, and what is not?

4. *Governance, ecosystems and institutional roles*

- According to your opinion, who currently has too much, or too little, influence in defining CBRNe-related standards?
- How should the relationship between scientific knowledge, policy decisions, and operational practice be balanced in the development of future standards?
- Is there a role for civil society or non-traditional stakeholders in standardisation processes, or should this remain primarily a technical matter?
- Should the EU institutions take a more proactive, innovation-oriented role in shaping the future of CBRNe standards, or should they focus strictly on harmonisation and coordination?
- How do you view the relationship between civil and military standardisation in the CBRNe context, particularly in relation to NATO or in response to hybrid or high-intensity scenarios? Should we aim for greater interoperability, or is it more appropriate to maintain distinct approaches?

5. *Strategic vision*

- Imagine a new European mechanism or ecosystem designed to foster forward-looking, inclusive and adaptive standardisation in the CBRNe domain. What features would it need to have to be effective?
- Are there any lessons to be drawn from other sectors (e.g., AI governance, public health, environmental policy) that could inspire more agile or participatory approaches in CBRNe standardisation?
- If you could pose one “strategic question” that standard-setters and policymakers should seriously consider over the next five years, what would it be?

6. *Closing remarks*

Before we conclude: is there any key message, a cautionary insight, or a provocative idea you would like to share with those developing the White Paper?

ANNEX 3 – DETAILED FORESIGHT ANALYSIS

TREND 1 Beyond the human loop. AI, autonomy and the future of CBRNe response	
Phase	**Description**
Phase 1: Analytical framework	The landscape of CBRNe response is undergoing a structural shift driven by the convergence of AI, autonomous robotics, edge computing, and unmanned systems. What is emerging is not a simple technological upgrade, but a reconfiguration of how threats are detected, interpreted, and acted upon. Traditionally, CBRNe response has relied on human-centred command chains, where experts operate sensors, interpret signals, and take responsibility for decisive action. Today, however, the sheer speed, complexity, and scale of modern threats are exceeding human cognitive capacity. Autonomous unmanned aerial vehicles (UAVs) and ground robots equipped with advanced sensors can now operate in environments too hazardous for human responders, performing real-time detection, mapping, and classification. Edge computing enables immediate analysis at the source, compressing the time between observation and action. As a result, decision authority is gradually migrating away from humans and toward algorithmic agents, often operating at the edge of supervision. This transition raises pressing questions: • How do we validate AI-driven classifications under unpredictable field conditions? • Who is accountable when autonomous systems make errors that affect public safety? • How can interoperability be ensured when multiple agencies and jurisdictions deploy heterogeneous platforms? The trend, therefore, is not merely about automation or efficiency. It signals the rise of AI-enabled decision-making architectures that increasingly shape emergency responses. While this shift promises faster, safer, and more scalable operations, it simultaneously exposes regulatory lag, ethical ambiguity, and risks of over-dependence on systems whose internal logics may be opaque. In this emerging paradigm, the critical challenge is not whether machines can perform CBRNe tasks, but how governance, standards, and accountability will adapt as autonomy becomes embedded in life-and-death scenarios. **1. Standardisation needs** • Asymmetry of pace: rapid technical innovation vs. slow legal adaptation. • Benchmarks missing: no universal standards for AI performance outside controlled labs. • Interoperability failures: heterogeneous data logics hinder joint operations.

	• Dual-use risks: detection drones can be repurposed for surveillance or hostile use. Standardisation must evolve into anticipatory governance, embedding encryption, transparency, continuous validation, and accountability into system design. **2. Weak signals** • Autonomous UAVs perform reconnaissance, mapping, and preliminary classification without direct oversight. • Swarm robotics demonstrate distributed awareness and task-sharing with minimal human input. • Decision dashboards replace raw data, making operators dependent on algorithmic interpretation. Human agency is shifting from direct control to post-hoc oversight, raising risks of automation bias, opacity, and accountability erosion. **3. Social and ethical dimensions** • Delegation of authority: AI decisions (e.g., evacuations, quarantines) directly affect rights and freedoms. • Opacity and accountability gaps: unclear responsibility for failures across developers, operators, and regulators. • Inequalities: advanced systems concentrated in high-tech States risk widening preparedness gaps. • Civil liberties: pervasive UAV-based monitoring blurs lines between security and surveillance. Standardisation must be seen as a moral and institutional infrastructure, embedding fairness, contestability, and transparency, aligned with the EU AI Act.
Phase 2: Scenario planning (2025-2050)	*Scenario 1 – Automation by accumulation* Autonomy emerges gradually through procedural shortcuts. By the 2040s, UAVs routinely classify threats without human review. Trust builds, until a major misclassification exposes the silent drift of authority. *Scenario 2 – Response at machine speed* AI systems coordinate across agencies, but divergent training and taxonomies lead to conflicting classifications. Autonomy enables machine-speed response but creates oversight gaps and institutional fragmentation. *Scenario 3 – Constraint by design* After failures and public backlash, new architectures reintroduce structural safeguards: AI detects and recommends, but high-impact actions require human validation, transparency modules, and oversight councils.

Phase 3: Megatrends & wild cards	**Megatrends** • Accelerating innovation & hyperconnectivity: AI becomes a distributed cognitive infrastructure but introduces systemic fragility. • Shifting security paradigms: non-state actors with dual-use technologies blur boundaries of risk. **Wild cards** • Adversarial interference: poisoned training data undermining classification. • Political backlash: false alarms triggering suspension of autonomy. • Misinformation loops: autonomous systems reinforcing spoofed data into self-sustaining errors.
Strategic reflections	The governance of AI-enabled CBRNe systems requires a paradigm shift in standardisation, from static compliance to dynamic stewardship. Key imperatives are the following: 1. Continuous validation & lifecycle monitoring under real-world conditions. 2. Codified human-AI protocols: thresholds, overrides, clear responsibilities. 3. Cross-sector interoperability: shared semantics, taxonomies, and heuristics. 4. Ethical resilience: transparency, bias mitigation, participatory oversight. 5. Dual-use prevention: safeguards against misuse, audit trails, access controls. 6. Polycentric governance: standards co-designed with agencies, communities, and international actors. The future of CBRNe response will not be defined only by algorithms, but by the legitimacy and adaptability of the norms that rule them. Standards must evolve into instruments of structured flexibility, balancing innovation with accountability in life-critical domains.

TREND 2 **Programmable organisms, unpredictable threats. The strategic risks of synthetic biology and bioengineering**	
Phase	**Description**
Phase 1: Analytical framework	Synthetic biology is redefining what is a biological threat. Unlike classical pathogens, which are taxonomically stable and phenotypically recognisable, synthetic constructs are modular, programmable, and potentially untraceable. This shift moves biosecurity from taxonomy toward functionality and emergence. Detection frameworks built on static reference libraries are increasingly

	inadequate in the face of programmable organisms that can mimic benign agents, activate conditionally, or evolve in unpredictable ways. At its core, this trend represents an epistemic shift: from identifying known biological agents to governing systems of latent, adaptive behaviour. Standards can no longer be reactive checklists. They must evolve into anticipatory governance architectures, capable of adapting to volatility and ambiguity. **1. Standardisation needs** • Functional risk profiling: moving beyond phenotype to evaluate programmable behaviours, toxicity triggers, and latent logic. • Adaptive detection protocols: certification of machine-learning platforms trained on synthetic datasets. • Traceability: enforcing digital watermarking, blockchain registries, and chain-of-custody tracking across the design-to-deployment lifecycle. • Dual-use boundaries: open-source gene editors and AI design tools blur innovation and misuse. • Dynamic standards: continuous updating, real-time surveillance, and anomaly detection must feed into regulation. **2. Weak signals** • DNA printers and cloud-based editing platforms lowering barriers to entry; synthetic biology diffuses beyond high-containment labs. • Do-It-Yourself biohacking communities, operating outside formal oversight, expand experimental capacity. • AI-assisted organism design accelerates innovation beyond the predictive capacity of classical review boards. • Diagnostic blind spots: modified agents evade PCR or standard assays, activating only under specific conditions. Threat perception is shifting from visible epidemics to latent, programmable risks. **3. Social and ethical dimensions** • Democratisation of design: accessibility of tools multiplies risks and undermines classical gatekeeping. • Attribution crisis: synthetic agents may originate from fragmented, decentralised processes, diffusing responsibility. • Public trust: stealth pathogens could trigger fear, misinformation, and backlash far exceeding technical risk. • Intergenerational justice: synthetic organisms may alter ecosystems permanently, creating biological legacies.

Phase 2: Scenario planning (2025-2050)	*Scenario 1 – Conditional pathogenicity* Programmable microbes activate only under specific triggers (e.g., chemicals, humidity, host metabolites), evading detection and complicating attribution. Surveillance systems collapse under static models. *Scenario 2 – Synthetic ecological cascades* Thousands of engineered organisms interact across borders, producing emergent hybrids with unforeseen properties. No single actor can explain or govern the outcomes. *Scenario 3 – Corporate-controlled bioplatforms* Private firms dominate bio-design and deployment, encrypting genomes with proprietary codes. Public agencies lose visibility and response capacity, turning biosecurity into a sovereignty issue.
Phase 3: Megatrends & wild cards	**Megatrends** • Tech convergence & hyperconnectivity: AI, cloud, and distributed biofabrication expand capabilities while outpacing regulation. • Ecological pressure & resource scarcity: crisis-driven deployment of synthetic organisms risks “deploy-first, regulate-later” ethos. **Wild cards** • Persistence in the wild: engineered organisms mutate, recombine, and escape detection, forcing emergency governance responses. • Stealth pathogens: latent constructs designed to evade standard surveillance until activated by triggers. • Opaque AI-designed organisms: constructs with functional logics beyond human interpretability challenge explainability and oversight**.**
Strategic reflections	Synthetic biology transforms risk governance from pathogen identification to functional system management. Standards must shift from static compliance toward modular, adaptive, and ethically grounded frameworks. Key imperatives are the following: 1. Function-centric classifications: stress-test constructs under variable conditions. 2. Real-time, adaptive diagnostics: anomaly detection beyond molecular fingerprints. 3. Iterative certification: continuous validation, not one-off approvals. 4. Traceability mandates: watermarking, blockchain, and forensic readiness. 5. Dual-use foresight: structured reviews, access controls, use-case bounding. 6. Plural oversight: interdisciplinary panels combining technical, legal, and civil expertise.

	7. Ecological resilience: reversibility clauses and intergenerational accountability. 8. Global interoperability: standards must cross jurisdictions, as programmable biology is inherently transnational. Synthetic biology requires standardisation as a living infrastructure, which is anticipatory, resilient, and accountable. Governing programmable organisms means governing the biological futures we are actively creating.

TREND 3 **From weather to weapon. Environmental collapse and CBRNe futures**	
Phase 1: Analytical framework	Climate change is no longer a backdrop to CBRNe risks. It is becoming a direct amplifier, trigger, and obfuscator of chemical, biological, and radiological hazards. Rising temperatures, volatile hydrology, and ecosystem collapse are eroding the stable baselines on which detection, containment, and response frameworks were built. • Traditional models assume constants of air pressure, humidity, or hydrological flow. These assumptions now fail. Chemicals volatilise faster, radionuclides migrate unpredictably, and pathogens adapt within destabilised ecosystems. Legacy infrastructures (e.g., chemical depots, radiological storage, biological labs) were designed for 20th-century climate conditions and increasingly prove inadequate. • This shift is systemic: climate does not only increase hazard frequency, it reshapes exposure, attribution, and governance. It fuses natural and technological risks into compound crises, where attribution blurs between accident, negligence, and deliberate act. Future standards must therefore become adaptive infrastructures, integrating climate intelligence, real-time environmental overlays, and predictive maintenance as core functions of preparedness. **1. Standardisation gaps** • Climate-informed calibration: embedding shifting temperature, humidity, and hydrology into sensor thresholds and risk models. • Cross-domain interoperability: integrating climate data, biosurveillance, and emergency response platforms. • Infrastructure resilience: digital twins and predictive maintenance for facilities stressed by floods, heat, or permafrost thaw. • Forensic adaptation: standards that incorporate environmental variables into attribution and incident classification. **2. Weak signals** • Legacy hazards reactivated: thawing permafrost exposes buried munitions and biowaste. • Multi-hazard cascades: extreme weather triggers simultaneous chemical, radiological, and biological releases.

	• Natural-technological (Natech) fusion: wildfires, floods, or heatwaves catalyse industrial or lab failures. • Attribution ambiguity: climate-driven accidents resemble sabotage, complicating legal and political response. These signals point to non-linear crisis pathways beyond siloed detection and response. **3. Socio-ethical dimensions** • Unequal exposure: vulnerable communities near ageing sites or in fragile states face disproportionate risk. • Algorithmic governance: opaque AI forecasting may undermine trust in evacuation or containment decisions. • Risk of securitisation: climate-CBRNe fusion may justify exceptional surveillance or militarised response. • Standards must embed climate justice, transparency, and safeguards for civil liberties.
Phase 2: Scenario planning (2025-2050)	*Scenario 1 – Reawakened permafrost* Thawing Arctic soils release decades-old chemical munitions, radiological waste, and synthetic-biological remnants. Lack of jurisdiction and archival gaps paralyse response until new registries and adaptive containment standards emerge. *Scenario 2 – Heat cascade* An urban megacity collapses under a record heatwave. Failures across energy, radiological storage, chemical depots, and biotech labs cascade into systemic disaster. Standards shift toward multi-hazard integration and urban resilience by convergence. *Scenario 3 – Pathogen drift* Ecological fragmentation accelerates recombination between synthetic agricultural microbes and natural pathogens. A hybrid virus spreads across borders, evading diagnostics and jurisdictional categories. Standards introduce the notion of “functional hybrid agents” and mandate global traceability of synthetic deployments.
Phase 3: Megatrends & wild cards	**Megatrends** • Climate change as amplifier: environmental volatility reshapes hazard geography, frequency, and complexity. • Fragmented security landscape: attribution blurred across accidents, sabotage, and systemic failure. • Resource scarcity & urbanisation: fragile governance and dense cities intensify cascading risks. • Hyperconnectivity: IoT-based detection offers new capacity but increases systemic vulnerability to cyber disruption and misinformation.

	Wild cards • Zoonotic spillover: thawed pathogens or recombined microbes bypass detection frameworks. • Climate-triggered facility collapse: extreme events unleash multi-domain toxic blends across borders. • Masked attacks: adversaries exploit natural disasters to disguise CBRNe releases, complicating attribution.
Strategic reflections	Governing the climate-CBRNe nexus requires standards that are not static codices but living infrastructures for resilience under uncertainty. Key imperatives are the following: 1. Multi-hazard convergence: integrated detection fusing climate, chemical, biological, and radiological data. 2. Climate-resilient infrastructures: predictive maintenance, modular fail-safes, and adaptive sealing. 3. Attribution frameworks: environmental signature tracking and probabilistic forensic models. 4. Function-based diagnostics: behavioural modelling for climate-activated or hybrid agents. 5. Distributive fairness: prioritising vulnerable communities with inclusive communication and early warning. 6. Explainable AI forecasting: transparency and contestability in climate-driven predictive tools. 7. Interoperable command grammars: shared procedures across agencies and borders for compound crises. 8. Permanent stress-testing: living scenario libraries that expose institutional fragilities and blind spots. As climate volatility fuses with CBRNe risk, standardisation must move beyond technical compliance and become a form of institutional foresight: a climate-smart governance framework able to anticipate compound hazards, integrate environmental intelligence, and ensure equitable protection. In this age of systemic disruption, resilience will depend not only on adaptive sensing and infrastructure robustness, but also on the preservation of trust, legitimacy, and accountability under unprecedented strain.

<table>
<tr><th colspan="2">TREND 4
Cognitive contagion. Disinformation as a CBRNe weapon</th></tr>
<tr><td>Phase 1: Analytical framework</td><td>
Disinformation is no longer a peripheral irritant in CBRNe preparedness. It is becoming a weaponised risk vector capable of amplifying hazards, undermining institutional credibility, and fragmenting public trust. As crises unfold in environments saturated with synthetic media and algorithmic influence, the challenge is not only to detect chemical, biological, or radiological agents, but also to preserve the cognitive integrity of emergency communication.

In this emerging landscape, CBRNe governance must integrate physical hazard management with cognitive resilience. Sensor data, alerts, and public advisories circulate in contested information ecosystems where the line between verified signal and synthetic fabrication is increasingly blurred. The ability to authenticate information flows and maintain narrative coherence may prove as decisive as technical detection itself.

1. Standardisation gaps
• Signal integrity: cryptographic provenance and verifiable data chains for sensor telemetry and institutional alerts.
• Semantic resilience: metadata and integrity markers to detect subtle manipulations in language, imagery, or format.
• Crisis communication: codified templates, multilingual accessibility, and culturally resonant alerts.
• Institutional interoperability: shared semantics and escalation protocols to prevent divergent narratives across agencies.

Standards must evolve into infrastructures of credibility, protecting not only data but the conditions of public trust.

2. Weak signals
• Synthetic incidents: deepfakes and fake sensor feeds simulating CBRNe events.
• Algorithmic amplification of fear: botnets and coordinated campaigns linking routine exercises to false threats.
• Crisis fusion: climate-linked disasters reframed as deliberate contamination, fuelling panic.

Disinformation must be treated as a potential initiator of cascading CBRNe crises.

3. Socio-ethical dimensions
• Inequality of exposure: digitally marginalised populations are disproportionately vulnerable to manipulation.
</td></tr>
</table>

	• AI governance dilemmas: disinformation detection raises risks of surveillance, bias, and censorship. • Narrative warfare: institutions must balance timely disclosure with the risk of fuelling distrust. Standardisation becomes a tool of knowledge governance, embedding transparency, contestability, and safeguards for human rights.
Phase 2: Scenario planning (2025-2050)	*Scenario 1 – Synthetic incident spiral* Generative AI enables full-spectrum simulations of CBRNe crises. Public scepticism inverts: real alerts are doubted while fabrications proliferate. Preparedness depends on signal authentication and credibility metrics. *Scenario 2 – Fragmented cognition* Information ecosystems fracture into incompatible epistemic blocs. A single event yields divergent interpretations across borders. Without shared narrative ground, international coordination collapses. *Scenario 3 – Resilient cognition by design* Societies invest in cognitive resilience as critical infrastructure: community validation hubs, participatory dashboards, and media literacy as civil defence. Preparedness becomes democratically co-produced.
Phase 3: Megatrends & wild cards	**Megatrends** • Synthetic media proliferation: deepfakes and AI content destabilise perception of threats. • Hybrid threat paradigms: physical, digital, and psychological domains converge. • Knowledge polarisation: algorithmic silos fracture shared factual baselines. • Inequity of access: marginalised groups remain most exposed to cognitive manipulation. **Wild cards** • Synthetic knowledge collapse: coordinated disinformation simulates a mass incident, causing real-world chaos. • Institutional disinformation: state actors weaponise false alerts to justify militarisation. • AI-induced suppression: compromised CBRNe platforms silently distort or withhold critical data.
Strategic reflections	In a world where belief becomes as critical as detection, CBRNe governance faces a dual imperative: managing material risk while safeguarding the cognitive architectures of trust, coordination, and legitimacy.

	Key imperatives are the following: 1. Cryptographic provenance: verifiable chains of custody for crisis data. 2. Narrative-aware communication: context-sensitive, multilingual, and participatory alert protocols. 3. AI governance safeguards: auditability, transparency, and human oversight for automated systems. 4. Cognitive resilience: media literacy, verification hubs, and rehearsals that integrate narrative stress-testing. 5. Equity and rights: standards that protect vulnerable communities from both manipulation and overreach. The next systemic CBRNe failure may not stem from a missed detection, but from a failure to agree whether the threat exists at all. Standardisation must therefore govern both physical conditions and cognitive environments, treating perception as critical infrastructure. In this sense, it becomes not only an operational discipline, but a cornerstone of democratic resilience in the age of synthetic disruption.

TREND 5 **The fragile atom. Asymmetric conflict and the collapse of global nuclear norms**	
Phase 1: Analytical framework	The nuclear risk landscape is shifting from superpower deterrence to an ecosystem defined by asymmetric proliferation, technological diffusion, and geopolitical fragmentation. The erosion of arms control treaties, combined with crises in Ukraine and the Middle East, exposes foundational weaknesses in verification regimes. Traditional architectures, reliant on political consensus and centralised mechanisms of the International Atomic Energy Agency are no longer sufficient. Emerging risks include: • Small Modular Reactors (SMRs) deployed in unstable zones, attractive but vulnerable to diversion and sabotage. • Dual-use diffusion through commercial channels and simulation platforms. • Cyber-mercenary threats targeting Supervisory Control And Data Acquisition (SCADA) systems in nuclear facilities. Standards must therefore evolve from compliance instruments to distributed infrastructures of trust: embedding AI-assisted verification, blockchain-based fuel telemetry, interoperable safety protocols, and climate-adaptive resilience.

	1. Standardisation gaps • Adaptive verification: autonomous anomaly detection and cryptographically secure data chains. • SMR safeguards: end-to-end traceability, cyber-physical access control, and deployment criteria for fragile States. • Decentralised oversight: modular standards that function even without treaty consensus. • Cognitive security: protocols to counter narrative manipulation and disinformation in nuclear discourse. **2. Weak signals** • Proliferation of centrifuge components via commercial supply chains. • Cyber mercenary access to reactor SCADA systems. • SMR deployments in grey zones, escaping multilateral regulation. • Strategic opacity in Iran and North Korea's programmes. • Open-source simulation tools lowering barriers to nuclear know-how. Collectively, these signals reveal a governance ecosystem marked by diffusion, fragmentation, and asymmetry, where traditional controls are outpaced. **3. Socio-ethical dimensions** • Risk inequity: energy-poor nations may adopt SMRs without safety cultures, creating radiological precarity. • Non-state proliferation: terror networks and cyber groups outside treaty frameworks. • Public narratives: disinformation and propaganda erode institutional credibility. • Normative imbalance: Global North dominance risks perceptions of exclusion or bias. Standards must be multilateral, context-aware, and culturally sensitive, embedding both technical safeguards and cognitive legitimacy.
Phase 2: Scenario planning (2025-2050)	*Scenario 1 – Fragmented deterrence* Regional powers expand ambiguous nuclear programmes under civilian cover. SMRs spread via bilateral deals in unstable zones. Deterrence becomes transactional, based on unverifiable claims and opaque postures. *Scenario 2 – Non-state radiological attacks* A Radiological Dispersal Device (RDD) detonated using medical isotopes causes panic, economic disruption, and attribution deadlock. Weak traceability

	and fragmented registries erode public trust, forcing *ad hoc* coalitions to patch governance gaps. *Scenario 3 – Autonomous reactor failure* An AI-controlled SMR in a volatile region fails during a cyber conflict. Proprietary, opaque control systems prevent human override. Misinterpretation of data triggers regional escalation, exposing the risks of unverifiable autonomy.
Phase 3: Megatrends & wild cards	**Megatrends** • Multipolar fragmentation: treaties weaken, verification collapses. • Tech acceleration: AI, blockchain, and cyber systems both enable and undermine control. • Hybrid actors: non-state proliferators and cyber-mercenaries emerge as credible threats. • Civil society empowerment: contested legitimacy of nuclear standards and SMR deployments. • Climate stress: facilities are vulnerable to floods, heat, and drought-induced failures. **Wild cards** • AI-enabled nuclear design lowers barriers to weaponisation. • Collapse of the Nuclear Non-Proliferation Treaty (NPT) and the Comprehensive Nuclear-Test-Ban Treaty (CTBT) triggers cascades of proliferation. • RDD in a megacity blurs line between terrorism and nuclear conflict. • Climate-induced reactor collapse spreads radiological fallout across borders.
Strategic reflections	The nuclear order is entering an era of asymmetric fragility, where proliferation, cyber risk, and environmental volatility converge. Technical containment alone is insufficient. Three imperatives emerge: 1. Vigilant adaptation: standards must anticipate grey-zone conditions (e.g., SMR oversight, AI auditability, climate-sensitive resilience). 2. Cognitive security: governance must treat perception and communication as critical infrastructures, embedding credibility protocols and multilingual alert frameworks. 3. Polycentric norms: frameworks must be modular, inclusive, and interoperable, ensuring legitimacy across fractured geopolitical and cultural contexts. At the intersection of proliferation, technological acceleration, and climate fragility, the future of nuclear governance will depend on adaptive standards that

	safeguard not only reactors and isotopes, but also the architectures of trust, meaning, and collective action. This requires a transition from static compliance toward anticipatory governance, capable of functioning amid geopolitical rivalry, cyber interference, and ecological volatility. Standards must evolve into living infrastructures, embedding continuous verification, climate-integrated resilience thresholds, and safeguards against both material diversion and informational manipulation. Crucially, nuclear preparedness in the 21st century cannot be reduced to containment technologies alone. It must also preserve public legitimacy, equitable security, and cognitive stability, ensuring that societies can interpret, communicate, and act coherently under conditions of nuclear ambiguity. In a multipolar and digitally saturated world, where escalation may emerge as much from perception as from material events, the integrity of governance frameworks becomes as critical as the safety of facilities themselves. Without such foresight, today's fractures risk becoming tomorrow's irreparable ruptures, not only in reactors or treaties, but in the very credibility of the global nuclear order.

TREND 6 **Orbital dependencies and terrestrial exposure. CBRNe risks to space-based infrastructure and strategic resources**	
Phase 1: Analytical framework	CBRNe preparedness is becoming structurally dependent on fragile infrastructures once considered peripheral: • Satellite constellations now underpin biosurveillance, radiological plume mapping, and encrypted coordination. • Rare isotopes, high-purity polymers, and rare earths are indispensable for detection and protection systems. • AI-mediated logistics chains increasingly determine the availability of critical components. These enabling layers are also points of systemic vulnerability, susceptible to spoofing, jamming, cyber infiltration, coercive embargoes, counterfeit insertions, or adversarial AI manipulation. Future standards must therefore govern not only agents and protocols, but also the infrastructures of resilience themselves. **1. Standardisation gaps** • Space systems: criteria for shielding, signal integrity, and cross-constellation failover. • Material governance: blockchain-led traceability, ethical sourcing, and redundancy in isotope supply. • Supply chain security: component authentication, anomaly detection in logistics metadata, and deep-tier audits.

	• Semantic authority: safeguards to preserve credibility against spoofed signals or counterfeit components. **2. Weak signals** • GPS spoofing near radiological facilities. • Ransomware disrupting isotope transport. • Black-market trade in dual-use microelectronics. • Coordinated delays in biosensor supply chains. • Satellite downlink interference during CBRNe drills. They are indicators of a systemic fragility, where preparedness rests on infrastructures beyond state control. **3. Socio-ethical dimensions** • Equity gaps: States without satellites, isotope production, or resilient logistics face structural disadvantage. • Legitimacy risks: opaque sourcing or external control undermine trust. • Governance dilemmas: in crises, who owns orbital access or material flows? Standards must embed procedural transparency, distributive fairness, and cognitive resilience.
Phase 2: Scenario planning (2025-2050)	*Scenario 1 – Orbital denial* A CBRNe emergency coincides with satellite interference. Plume tracking collapses, forecasts diverge, and disinformation fills the void. Without failover standards, command chains stall. *Scenario 2 – Resource nationalism* Export controls on rare isotopes paralyse detection networks. Preparedness becomes hostage to supply leverage, turning materials into geopolitical deterrents. *Scenario 3 – Synthetic supply chain compromise* Adversarial AI inputs poison logistics routing. Counterfeit biosensors circulate undetected. Trust collapses, mutual aid breaks down, and response architectures fragment.
Phase 3: Megatrends & wild cards	**Megatrends** • Technological hyperconnectivity: more capability, more exposure. • Multipolar contestation: resource weaponisation and infrastructure denial. • Scarcity: isotopes and rare earths as critical chokepoints. • Non-state actors: manipulating opaque supply networks.

	Wild cards • Orbital degradation (e.g., debris cascades, anti-satellite weapons strikes). • Strategic isotope embargoes. • Synthetic component infiltration of sensors/drones. • AI-driven logistics sabotage during compound crises.
Strategic reflections	CBRNe resilience now depends on infrastructures that are transnational, commercially governed, and geopolitically contested. Standards must shift from technical compliance to anticipatory governance of systems-of-systems. Key imperatives are the following: 1. Orbital resilience: codify shielding, telemetry continuity, and inter-constellation failover. 2. Material security: institutionalise traceability, ethical provenance, and redundancy in critical inputs. 3. Supply chain protection: expand oversight beyond first-tier vendors, embedding AI anomaly detection and tamper-proof certification. 4. Cross-domain interoperability: align orbital, logistics, and material standards across jurisdictions. 5. Stress-tested norms: evaluate standards under wild card disruptions, such as satellite denial or synthetic infiltration. The future of CBRNe governance will hinge not only on countering agents, but on securing the infrastructures of trust, flow, and attribution that sustain detection and response. Without anticipatory standards, today's enabling systems risk becoming tomorrow's systemic failures.