COUNTERING THE MISUSE OF CBRN MATERIALS AND KNOWLEDGE – METHODOLOGY FOR NATIONAL CAPACITY ASSESSMENT

Consortium:

Center for the Study of Democracy (CSD), Bulgaria
Hochschule fur den Offentlichen Dienst in Bayern (BayHfoD), Germany
Kentro Meleton Asfaleias (KEMEA), Greece
Ibatech Technologia SL (IBATECH), Spain
Gobierno Vasco – Departamento Seguridad (ERTZ), Spain

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

Table of Contents

Executive summary 1

1. Introduction 3

2. A typology of CBRN threats 5

CBRN threats posed by states 8

CBRN threats posed by non-state actors 16

3. CBRN security capacity assessment 20

Framing CBRN security capacity 23

Methodology for CBRN security capacity assessment 29

4. Conclusion 38

Executive summary

This report outlines a methodology for assessing national capacity for countering the misuse of chemical, biological, radiological, and nuclear (CBRN) materials and related information. This includes the risk that a state or non-state actor may deploy biological, chemical, or nuclear weapons, collectively referred to as weapons of mass destruction (WMD). The proposed methodology is grounded in an all-hazard approach for addressing CBRN risks regardless of their cause and highlights specific aspects of the process of preventing and responding to CBRN threats.

The methodology uses the concept of CBRN security as a general organising principle and a tool for capacity modelling. To unpack this concept, the report provides an indicative typology of CBRN threats posed by state and non-state actors and discusses cross-cutting trends that impact the threat spectrum. CBRN security encompasses two inter-related processes: (1) safeguarding CBRN materials and related information and infrastructure from diversion and/or misuse; and (2) ensuring effective response to deliberate CBRN incidents. Realising these goals requires mainstreaming CBRN security considerations in different areas of action. CBRN security capacity refers to the ability to perform functions of relevance to CBRN security effectively, efficiently, and sustainably.[1] CBRN security capacity can be approached in terms of levels and dimensions. The development of the methodology is underpinned by the following assumptions:

- CBRN security falls within the remit of multiple international regimes.
- CBRN security cuts across different sectors within government and civil society.

[1] Adapted from United Nations Development Programme, *Capacity Assessment and Development: In a Systems and Strategic Management Context*, Technical Advisory Paper No 3, January 1998.

- CBRN security capacity entails a shared commitment among stakeholders to the goals of CBRN security risk management.

The methodology provides a framework for CBRN security capacity assessment at the national level which focuses on the role of stakeholder interaction in the process of preventing and responding to CBRN threats. The framework covers the following aspects:

- Overall national systems context encompassing policy, legal, and regulatory frameworks; and organisational arrangements including distribution of core functions and coordination;
- Delivery and performance of core functions that are relevant to CBRN security;
- Linkages, interdependencies, and communication across sectors and stakeholders.[2]

The methodology underscores that CBRN security capacity is not a fixed state but a process and that capacity assessment is important for ensuring that relevant frameworks, mechanisms, and structures are sustainable and can adequately accommodate and address emerging CBRN security challenges.

[2] Adapted from Food and Agriculture Organisation of the United Nations (UN FAO), *FAO Biosecurity Toolkit*, 2007.

1. Introduction

Chemical, biological, radiological, and nuclear (CBRN) events involving the release of toxic substances can have different causes. For example, accidents can occur following natural disasters, or as a result of technical failure, human error, or negligence. But incidents can also involve the misuse of CBRN agents, materials, or related information with the intention to cause harm to people, infrastructure, or the environment. While the immediate activities that are implemented in response to CBRN events regardless of their cause are likely to share common elements, CBRN attacks could be difficult to predict and many different variables may need to be considered to ensure their effective prevention. Depending on the type of agents or materials involved (i.e. chemical, biological, or radioactive/nuclear) appropriate measures for detection, early warning, incident containment, investigation, and decontamination would be required.

This report focuses on the prevention and countering of deliberate CBRN events. It outlines a methodology for capacity assessment that seeks to facilitate consideration of CBRN security risk mitigation from a cross-sectoral perspective whereby stakeholder interaction is a central attribute of capacity. CBRN security encompasses two inter-related processes: (1) preventing the misuse and diversion of CBRN materials and related information; and (2) ensuring effective response to deliberate CBRN incidents. Realising these goals is grounded in an all-hazard approach for managing CBRN risks which requires mainstreaming CBRN security considerations in different areas of action. The proposed methodology uses the concept of CBRN security as a general organising principle and a tool for capacity modelling. CBRN security capacity is the ability to perform functions of relevance to CBRN security effectively, efficiently, and sustainably.[3] CBRN security capacity can be approached in terms of levels –

[3] Adapted from United Nations Development Programme, *Capacity Assessment and Development: In a Systems and Strategic Management Context*, Technical Advisory Paper No 3, January 1998.

(1) a broad system level; (2) entity level; and (3) individual level – and dimensions. The methodology provides a framework for CBRN security capacity assessment at the national level which focuses on the role of stakeholder interaction in the process of preventing and responding to CBRN threats. It underscores that CBRN security capacity is not a fixed state but a process and that capacity assessment is important for ensuring that relevant frameworks, mechanisms, and structures are sustainable and can adequately accommodate and address emerging CBRN security challenges.

Part 2 of the report outlines an indicative typology of threats involving the misuse of CBRN materials and related information. The typology examines threats posed by state and non-state actors highlighting key trends and factors that underpin the complexity of CBRN protection against deliberate events.

Part 3 outlines a methodology for CBRN security capacity assessment. National CBRN security capacity is approached in terms of dimensions and indicative modalities for each dimension are suggested. The methodology provides a comprehensive framework for mapping the policy, regulatory, and organisational setting of CBRN security at the national level and reviewing stakeholder inter-dependencies and interactions. The methodology is supplemented by a Training Guide for First Responders with practical scenario-based exercises that could be used for validating approaches, instruments, and practices for CBRN security risk management.

2. A typology of CBRN threats

This section examines the scope and complexity of CBRN threats. Efforts to prevent and counter the misuse of CBRN agents, materials, or related information reinforce the international regimes that outlaw chemical and biological weapons and prohibit the spread of nuclear weapons (collectively known as weapons of mass destruction, WMD). These efforts cut across multiple domains of activity spanning the entire cycle of use of chemical, biological, radioactive, or nuclear materials and related information which includes development, production, safe handling, storage, transport, transfer, and disposal.

A threat comprises intention and capability, and is informed by the potential consequences and likelihood of success (from the adversary's perspective) of the particular type of a CBRN event.[4] Threats may be identified in terms of 'threats from' (i.e. who the adversary is, which type of material or information the adversary might have or seek access to, and how the adversary might seek to cause harm through that material or information), or 'threats to' (i.e. strategic targets or locations where material or information can be used). Threats can be analysed in terms of adversaries, asset, and tactics.

A potential adversary is characterised by intent, motivation, and capabilities.[5] Intent could include, for example, unauthorised possession of CBRN material, acquisition of sensitive information, or causing harm or damage. Motivation could be financial, political or ideological, or could result from disgruntlement or coercion. The capabilities of an adversary depend on characteristics such as the number of individuals involved, the level of organisation and coordination, prerequisite knowledge and skills, etc. Adversaries may include insiders, that is,

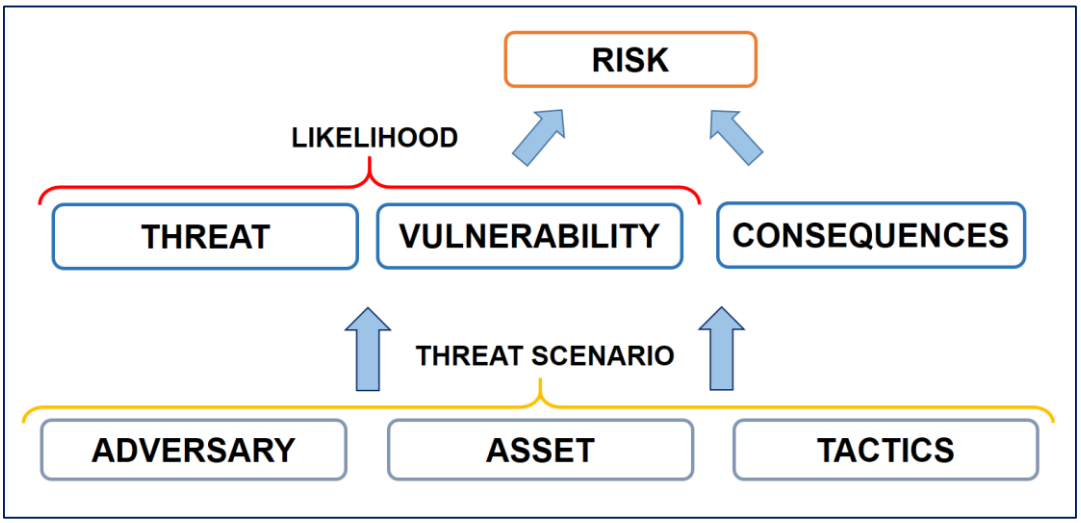
[4] Adapted from International Atomic Energy Agency (IAEA), *Risk Informed Approach for Nuclear Security Measures for Nuclear and Other Radioactive Material out of Regulatory Control*, IAEA Nuclear Security Series No. 24-G, 2015.
[5] International Atomic Energy Agency (IAEA), *National Nuclear Security Threat Assessment, Design Basis Threats and Representative Threat Statements*, IAEA Nuclear Security Series No. 10-G, 2021.

individuals with authorised access to associated facilities or activities or to sensitive information or information assets who could commit or otherwise facilitate criminal or intentional unauthorised acts involving CBRN materials.

An asset is CBRN material or information that an adversary could use to cause harm.[6] Assets cover the type and amount of material or information, the mode of their acquisition, and the locations where they are stored. Tactics refer to the modalities of deliberate CBRN events, that is, how/when/where an adversary may carry out an attack.

Threats and risks are interlinked. A risk is a function of threat, vulnerability and consequences, and may be expressed quantitatively – for example as an expected loss (consequence per year) – or qualitatively using relative rankings (e.g. low, medium and high) (Figure 1).[7]

Figure 1: Relationship between a threat and risk

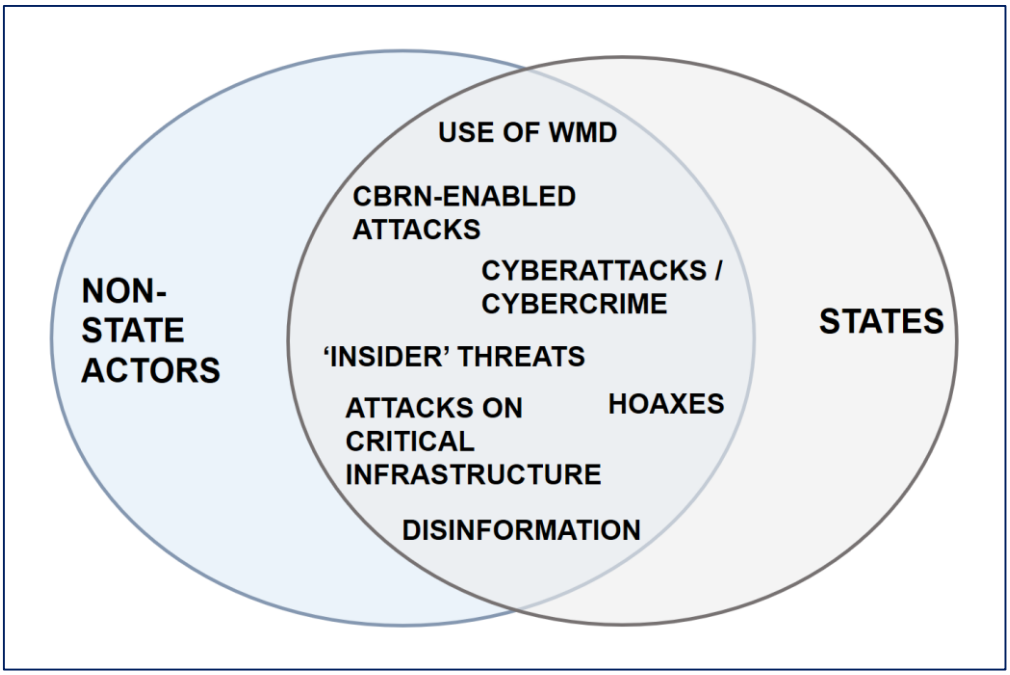


Source: Based on IAEA[8]

[6] Adapted from International Atomic Energy Agency (IAEA), *Risk Informed Approach for Nuclear Security Measures for Nuclear and Other Radioactive Material out of Regulatory Control*, IAEA Nuclear Security Series No. 24-G, 2015.
[7] Adapted from International Atomic Energy Agency (IAEA), *Risk Informed Approach for Nuclear Security Measures for Nuclear and Other Radioactive Material out of Regulatory Control*, IAEA Nuclear Security Series No. 24-G, 2015.
[8] Adapted from International Atomic Energy Agency (IAEA), *Risk Informed Approach for Nuclear Security Measures for Nuclear and Other Radioactive Material out of Regulatory Control*, IAEA Nuclear Security Series No. 24-G, 2015.

The proposed typology of CBRN threats examines two general categories of threats: threats posed by states and threats posed by non-state actors (Figure 2).[9] Many of these threats are not new in nature but the ways in which they may manifest themselves are changing, not least as a result of emerging technologies and increased access to sensitive information and materials.

Figure 2: Indicative typology of CBRN threats



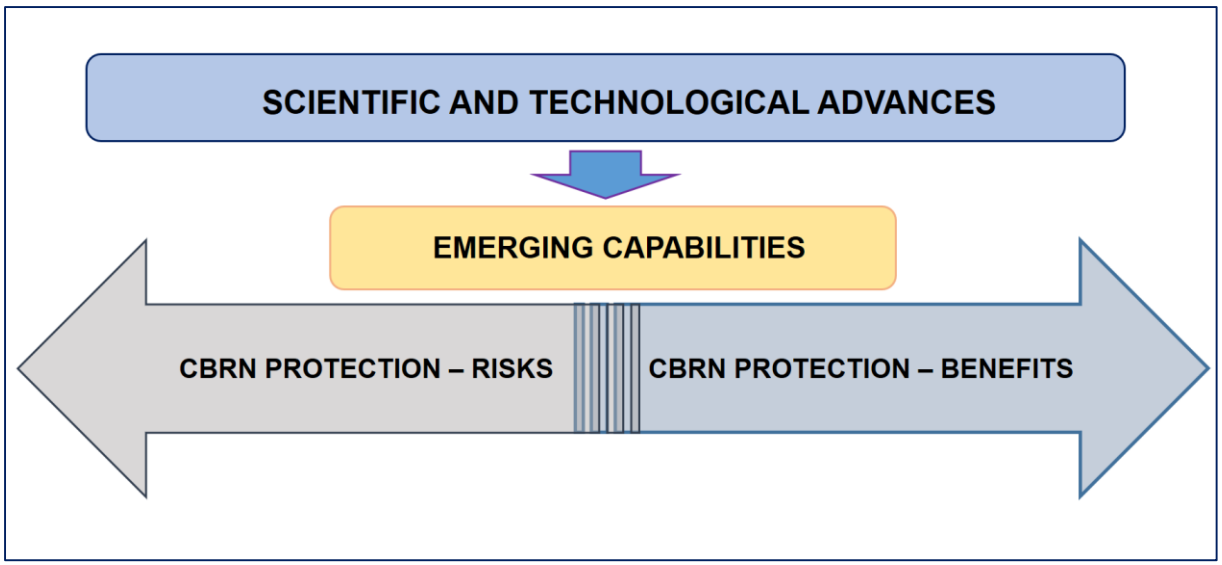
Source: Authors

Scientific and technological innovation is a critical source of solutions in the form of products, techniques, processes, etc. that can contribute to enhancing protection against deliberate CBRN events. These include material identification and detection capabilities; forensic capabilities; systems for physical protection, disinfection, and decontamination; and communication systems for early warning and response coordination, among others. Despite their legitimate applications, enabling capabilities may also be leveraged to plan and carry out CBRN attacks

[9] For a recent analysis of the CBRN threats that the EU faces, see Alexandra Rimpler-Schmid et al. *EU Preparedness and Responses to Chemical, Biological, Radiological and Nuclear (CBRN) Threats*, Study requested by the European Parliament's (EP) Subcommittee on Security and Defence (SEDE), 16 July 2021.

(Figure 3). Security aspects of emerging technologies may not be immediately evident but a multi-faceted impact assessment can facilitate their early identification, as well as the consideration and application of possible mitigation measures.

Figure 3: Impact of relevant scientific and technological advances



Source: Authors

CBRN threats posed by states

CBRN threats posed by states fall into three groups:

- WMD/CBRN threats during an armed conflict.
- WMD/CBRN hybrid threats.
- State-sponsored WMD/CBRN terrorism.

Each group is considered in detail in below.

WMD/CBRN threats during an armed conflict

This group of threats concerns the risk of use of WMD during in an armed conflict and includes threats of attacks or acts of sabotage against chemical, biological, or nuclear facilities.

All three classes of WMD – chemical, biological, and nuclear weapons – have been used in an armed conflict. The development, stockpiling, acquisition, retention, and use of biological, toxin, and chemical weapons is prohibited under international law. The 1975 Biological and Toxin Weapons Convention (BTWC) was the first international treaty outlawing an entire class of weapons of mass destruction. However, several states that had signed (Iraq) or ratified the BTWC (Soviet Union, apartheid South Africa) during the Cold War continued to operate clandestine biological weapon programmes until the early 1990s.[10] Chemical weapons were outlawed in the late 1990s and since then, almost all existing declared stockpiles have been destroyed. Yet the use of chemical weapons during the war in Syria has highlighted the challenges to verifying compliance and establishing accountability for chemical weapon attacks. The international regime that prohibits the proliferation of nuclear weapons distinguishes between nuclear-weapon states and non-nuclear weapon states. Nuclear-weapon states undertake not to transfer nuclear weapons or otherwise assist or encourage non-nuclear-weapon states to manufacture such weapons.[11] Non-nuclear-weapon states undertake to accept safeguards to guarantee that they do not use or divert atomic energy for weapon development. The Nuclear Non-Proliferation Treaty (NPT) does not have a universal membership and verification of compliance with the Treaty provisions can also face challenges.[12]

The shortcomings of the international WMD disarmament and non-proliferation regimes notwithstanding, there is a shared normative expectation against the use of WMD and any such use would attract international criticism and retaliation. The resilience of these norms is intertwined with the integrity of the relevant international and national frameworks,

[10] See, for example, Mark Wheelis et al.(eds.) *Deadly Cultures: Biological Weapons since 1945*, Harvard University Press, 2006.
[11] United Nations Office for Disarmament Affairs, Treaty on the Non-Proliferation of Nuclear Weapons, 1970.
[12] See, for example, International Atomic Energy Agency (IAEA), *Verification and Monitoring in Iran*, 2022.

mechanisms, and institutions that seek to ensure robust preparedness and response capabilities for detecting, countering, protecting against, and investigating possible uses of WMD.

Besides the use of WMD, it is possible to consider a scenario whereby a state engaged in an armed conflict against another state could try to take strategic advantage by targeting local chemical, biological, or nuclear facilities or infrastructure. The effects of such an attack are likely to be commensurate with those of an actual WMD attack. A case in point is the growing concern over the situation at the Zaporizhzya Nuclear Power Plant in Ukraine where the International Atomic Energy Agency (IAEA) has identified serious safety and security breaches during the ongoing hostilities as a result of Russia's invasion in February 2022.[13]

WMD/CBRN hybrid threats

Hybrid threats encompass state-sponsored coercive or subversive activities that remain below the threshold of a formally declared war.[14] Such activities rely on a mixture of conventional and non-conventional methods, e.g. diplomatic, military, economic, technological, and seek to exploit the vulnerabilities of the victim state to influence local decision-making. Hybrid threats prey on ambiguity which can hinder their prevention, detection, and attribution.

WMD/CBRN hybrid threats can take multiple forms. For example, they can involve (1) the deployment of WMD/CBRN agents; (2) acts of sabotage including through the malicious use of cyberspace; and (3) the use of disinformation campaigns to manipulate public opinion, discredit authorities, and influence social behaviour.

[13] See International Atomic Energy Agency (IAEA), *Nuclear Safety and Security in Ukraine*, 2022.
[14] European Commission, *Joint Communication to the European Parliament and the Council: Joint Framework on Countering Hybrid Threats*, JOIN(2016) 18, 6 April 2016; European Centre of Excellence for Countering Hybrid Threats, *Hybrid Threats as a Concept*, 2022.

State-sponsored targeted assassinations using WMD/CBRN agents illustrate the complexity of countering and responding to hybrid threats. These are small-scale incidents that directed at a single individual. As such, even a tiny amount of a potent WMD/CBRN agent would be sufficient to incapacitate or cause death. Depending on the agent used, symptoms may not show immediately, or may be common and not readily linked to the agent activity.[15] Delays in the identification of the agent could prevent the use of appropriate countermeasures and hinder treatment. These would have implications for establishing the exact route of exposure which in turn could impede investigation into the modalities of the attack.

Acts of sabotage including 'insider threats' such as espionage and intrusion that target facilities or infrastructure of national security significance can compromise state's capabilities for WMD/CBRN defence and civil protection. Cyberattacks targeting strategic industrial or scientific facilities can result in the loss of important data through theft or permanent damage, or cause technical failures leading to the release of toxic substances.[16] Cyberattacks can also be used to disrupt vital systems for information sharing and communication, including systems that are critical for emergency preparedness and crisis management.

To address emerging cyber threats and prevent the wholesale militarisation of the internet, states have advanced international consensus on the development of norms of responsible behaviour in cyberspace. These norms reflect the expectations of the international community and can help prevent conflict in the ICT (information and communication technology) environment and contribute to its peaceful use.[17] The Group of Governmental Experts (GGE) on Advancing

[15] On this point see, for example, Jonathan Tucker, 'The Body's Own Bioweapons', *Bulletin of Atomic Scientists*, vol. 64:1 (2008), pp. 16-22.
[16] See, for example, North Atlantic Treaty Organisation, *NATO's Chemical, Biological, Radiological and Nuclear (CBRN) Defence Policy*, last updated 5 July 2022.
[17] Note by the UN Secretary-General, *Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*, A/76/135, 14 July 2021.

responsible state behaviour in cyberspace in the context of international security has defined eleven voluntary non-binding norms and offered examples of the kinds of institutional arrangements that states can put into place to enhance cybersecurity and counter malign activities in the digital space (Box 1).[18]

Box 1: Norms of responsible state behaviour in cyberspace

#1 Interstate cooperation to increase stability and security in the use of ICTs and prevent harmful ICT practices

Recommended actions

Put in place or strengthen existing mechanisms, structures and procedures at the national level such as relevant policy, legislation and corresponding review processes; mechanisms for crisis and incident management; whole-of-government cooperative and partnership arrangements; and cooperative and dialogue arrangements with the private sector, academia, civil society and the technical community.

#2 Consideration of all relevant information in case of ICT incidents

Recommended actions

Establish or strengthen relevant national structures, ICT-related policies, processes, legislative frameworks, coordination mechanisms to facilitate the investigation and resolution of ICT incidents involving other states and assess the severity and replicability of an ICT incident.

#3 Preventing the misuse of ICTs within one's own territory

Recommended actions

Take all appropriate and reasonably available and feasible steps to detect, investigate and address the risk of malicious ICT activities emanating from one's own territory, including through the establishment of structures and mechanisms to formulate and respond to requests for international assistance.

#4 Cooperation to tackle the risk of terrorist and criminal use of ICTs

Recommended actions

Have in place national policies, legislation, structures and mechanisms that facilitate cooperation across borders on technical, law enforcement, legal and diplomatic matters relevant to addressing criminal and terrorist use of ICTs; develop appropriate protocols and

[18] See United Nations Office for Disarmament Affairs, Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the context of International Security.

procedures for collecting, handling and storing online evidence relevant to criminal and terrorist use of ICTs and provide assistance in investigations in a timely manner.

#5 Respect for human rights and privacy both online and offline

Recommended actions
Invest in and advance technical and legal measures to guide the development and use of ICTs in a manner that is more inclusive and accessible and does not negatively impact members of individual communities or groups.

#6 Not conducting or knowingly supporting intentional damage on critical infrastructure in another state

Recommended actions
Consider that each state determines which infrastructures or sectors it deems critical within its jurisdiction, in accordance with national priorities and methods of categorisation of critical infrastructure; put in place relevant policy and legislative measures at the national level to ensure that ICT activities conducted or supported by a state and that may impact the critical infrastructure of or the delivery of essential public services in another state are consistent with this norm, used in accordance with their international legal obligations, and subject to comprehensive review and oversight.

#7 Protection of critical infrastructure

Recommended actions
Enhance ICT security measures accorded to critical infrastructure and strengthen existing or develop complementary processes and procedures to detect and mitigate ICT incidents affecting such infrastructure; promote measures to ensure the safety and security of ICT products throughout their lifecycle or to classify ICT incidents in terms of their scale and seriousness.

#8 Responding to request for assistance in case of a malicious ICT activity including acts targeting critical infrastructure

Recommended actions
Promote common and transparent processes and procedures for requesting assistance from another state and for responding to requests for assistance.

#9 Ensuring supply chain integrity

Recommended actions
Put in place comprehensive, transparent, objective and impartial frameworks and mechanisms for supply chain risk management; establish policies and programmes to promote the adoption of good practices by suppliers and vendors of ICT equipment and

systems; put in place measures that encourage ICT vendors to incorporate safety and security in the design, development and throughout the lifecycle of ICT products; promote legislative and other safeguards that enhance the protection of data and privacy.

#10 Responsible reporting of ICT vulnerabilities

Recommended actions
Put in place impartial legal frameworks, policies and programmes to guide decision-making on the handling of ICT vulnerabilities; develop guidance and incentives on the responsible reporting and management of vulnerabilities and the respective roles and responsibilities of different stakeholders in reporting processes.

#11 Not conducting or knowingly supporting activity to harm the information systems of the authorised emergency response teams in other states

Recommended actions
Declare or put in place measures affirming that they will not use authorised emergency response teams to engage in malicious international activity and acknowledge and respect the domains of operation and ethical principles that guide the work of authorised emergency response teams; put in place other measures such as a national ICT-security incident management framework with designated roles and responsibilities.

Source: *Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*, Note by the Secretary-General, A/76/135, 14 July 2021.

Disinformation refers to the deliberate spread of inaccurate, incomplete, or false information. It is similar to propaganda but whereas the latter typically seeks to encourage a political or social action, disinformation can be used solely with the goal of discrediting an entity, trend, or phenomenon and instilling a sense of helplessness, anxiety, apathy, cynicism within the target community.[19] Disinformation can serve as a domestic and foreign policy tool for advancing one's agenda through manipulation and deceit. Recent and ongoing state-sponsored disinformation campaigns in the WMD/CBRN domain are a case in point.[20] Whilst not entirely

[19] Dean Jackson, *Issue Brief: Distinguishing Disinformation from Propaganda, Misinformation, and "Fake News"*, 17 October 2017; see also Council of Europe, *Dealing with Propaganda, Misinformation, and Fake News*, 2022;
[20] See, for example, Gordon Ramsay and Sam Robertshaw, *Weaponising News: RT, Sputnik, and targeted disinformation*, King's College London, 2019; Linda Qiu, 'Theory About U.S.-Funded Bioweapons Labs in Ukraine Is Unfounded', *New York Times*, 11 March 2022. On the impact of bioweapon-related disinformation

a new phenomenon in international political affairs, contemporary disinformation campaigns benefit from the wide availability of information and communication technologies; the ubiquity of online media platforms, including social media; and the sheer volume of data being transmitted at a rapid pace on a global scale that can hinder immediately distilling fact from fiction. Moreover, disinformation campaigns specifically aim to exploit existing social tendencies to elicit emotional reaction and polarise communities. Disinformation campaigns can destabilise societies and exacerbate their vulnerability to crisis situations. For example, studies suggest that disinformation campaigns in the context of the COVID-19 pandemic have played a role in undermining public trust in the response measures adopted for disease control and prevention.[21]

State-sponsored WMD/CBRN terrorism

International law prohibits states from providing any type of support to non-state actors that are involved or may otherwise facilitate the planning or carrying out of acts of terrorism, including terrorism using WMD or CBRN materials or agents.

United Nations Security Council Resolution 1373 (2001) obliges all states, *inter alia*, to (1) refrain from providing any form of support, active or passive, to entities or persons involved in terrorist acts, including by suppressing recruitment of members of terrorist groups and eliminating the supply of weapons to terrorists; (2) deny safe haven to those who finance, plan, support, or commit terrorist acts, or provide safe havens; and (3) prevent those who finance,

campaigns, see Milton Leitenberg, 'False Allegations of Biological-Weapons Use from Putin's Russia', *Non-proliferation Review*, vol.27:4-6 (2020).

[21] See, for example, Julie Posetti and Kalina Bontcheva, *Disinfodemic: Deciphering COVID-19 Disinformation*, UNESCO, 2020; Christian Johnson and William Marcellino, *Bad Actors in News Reporting: tracking news manipulation by state actors*, RAND, 2021. On the broader effects of disinformation in the context of disease prevention, see Rose Bernard et al. 'Disinformation and Epidemics: Anticipating the Next Phase of Biowarfare', *Health Security* vol. 19:1 (2018), pp.3-12.

plan, facilitate or commit terrorist acts from using their respective territories for those purposes against other States or their citizens.[22]

United Nations Security Council Resolution 1540 (2004) obliges all states to refrain from providing any form of support to non-state actors that attempt to develop, acquire, manufacture, possess, transport, transfer or use nuclear, chemical or biological weapons and their means of delivery.[23]

One area of concern in this regard is the advent of state-sponsored cybercrime, whereby state-affiliated or state-backed groups engage in malign cyber activities, including website hacking (e.g. service denial), data theft, and cyber-espionage.[24] Such activities could be difficult to track and attribute which raises critical issues about holding those responsible to account and highlights the risk of continued impunity.

CBRN threats posed by non-state actors

CBRN threats posed by non-state actors fall into three categories:

- WMD/CBRN terrorism.
- Cyber-enabled CBRN incidents.
- Hoax CBRN incidents.

Each group is considered in detail below.

[22] United Nations Security Council, Resolution 1373 (2001), S/RES/1373 (2001), 28 September 2001.
[23] United Nations Security Council, Resolution 1540 (2004), S/RES/1540 (2004), 28 April 2004.
[24] Patryk Pawlak and Gergana Petkova, *State-Sponsored Hackers: Hybrid Armies?*, European Union Institute for Security Studies, 30 January 2015.

WMD/CBRN terrorism

Non-state actors trying to develop or procure viable WMD and their means of delivery are likely to encounter certain barriers.[25] These include, *inter alia*, access to specialised equipment, technical knowledge, and production material such as biological or chemical agents, or fissile material. Yet the type of barriers that may hinder the acquisition of chemical, biological, or nuclear materials differ considerably. Whilst nuclear or radioactive material may be difficult to procure, biological agents such as bacteria, viruses, and fungi exist in nature and can be used to harm humans, animals, or plants even without weaponising them first. Toxic chemicals and substances are common in manufacturing and agriculture and some have similar properties to chemical warfare agents. Against this backdrop, the fact that chemical, biological, or nuclear weapons require time, expertise, and substantial resources to develop does not automatically preclude the possibility of non-state actors using chemical, biological, radiological, or nuclear material to harm people or damage the environment or infrastructure.

There is no universally accepted definition of terrorism but, in general, it is understood as the use of politically motivated violence, or the threat thereof against civilians or infrastructure.[26] Terrorists may be ideologically, or religiously inspired; equally, they could seek to advance a specific cause.[27] A WMD/CBRN terror attack could result in a mass-casualty event, and even when the scope of such an attack is limited, it could still have far-reaching cumulative effects and lead to large-scale contamination. Chemical, biological, or radioactive materials could also be deployed by individuals seeking solely financial or other form of personal gain. Whereas

[25] See MASC-CBRN, *Integrated Directory on the CBRN Risk Spectrum*, December 2020.
[26] Directive (EU) 2017/541 on combating terrorism of 15 March 2017 establishes a common understanding of the phenomenon of terrorism within the EU.
[27] See Europol, European Union Terrorism Situation and Trend Report 2022, 13 July 2022.

terror attacks tend to be indiscriminate, CBRN-enabled crimes are likely to target specific individuals or entities.

Acts of sabotage against critical infrastructure such as nuclear power plants, and water or food supply systems could have far-reaching consequences and deprive communities of essential services for a prolonged period of time. Non-state actors could use different tactics to procure toxic materials such as infiltrating facilities where such materials are stored or handled, or fostering close ties with individuals working at relevant facilities.

Increasing attention is given to addressing the risk that non-state actors may develop, acquire, or use WMD or CBRN materials and enhancing chemical, biological, and nuclear safety and security globally.[28] Lines of effort that seek to complement crime prevention and counter-terrorism include protecting sensitive materials, equipment, and information against theft, loss, misplacement, or diversion, including during shipment, transport, or transfer; enhancing the protection of critical infrastructure; and ensuring appropriate incident response planning in case of attacks.

Cyber-enabled CBRN incidents

Non-state actors could misuse cyber technologies to target facilities and infrastructure that produce, handle, or process chemical, biological, or nuclear materials, or related information. Service disruption at such facilities could cause data loss, breaches of privacy, or technical failures, or lead to the release of toxic substances. Cyberattacks could also target the information

[28] See, for example, Organisation for the Prohibition of Chemical Weapons (OPCW), Dealing with the threat of terrorism, 2022; International Atomic Energy Agency (IAEA), Security of nuclear and other radioactive material, 2022; World Health Organisation, *WHO guidance on implementing regulatory requirements for biosafety and biosecurity in biomedical laboratories: a stepwise approach*, 2020; World Organisation for Animal Health (WOAH), Biological threat reduction, 2022.

and communication systems that connect emergency services and thus delay immediate incident response.

Illicit online marketplaces such as those available on the Darknet could be used to facilitate the plotting of CBRN attacks. Such marketplaces make it possible to purchase biological or chemical agents and toxins, as well as instructions and manuals for their handling, storage, and application for nefarious purposes. Non-state actors could also take advantage of legitimate online trade to procure technology and equipment, for example, to set up production infrastructure, or to deploy as dispersal devices.

Hoax CBRN incidents

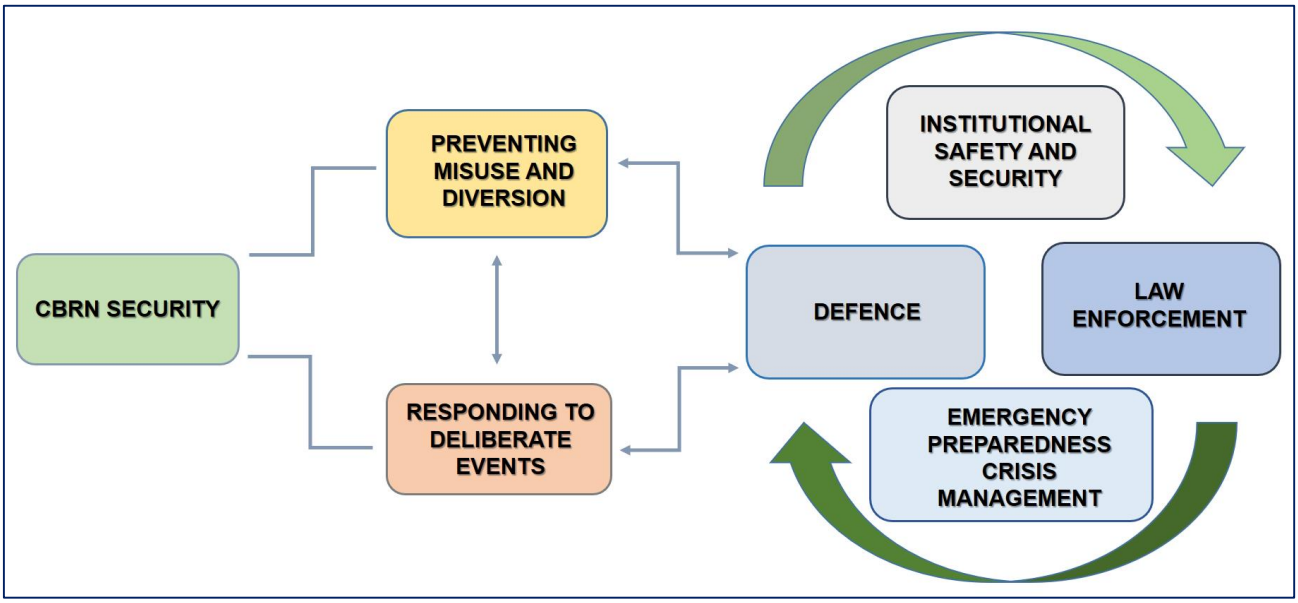
Whereas CBRN incident hoaxes do not seek to cause direct material or environmental damage or loss of life, they could disrupt the provision of essential services and lead to mass panic. Hoaxes prey on public fears and can be used to exploit social vulnerabilities to erode trust in the existing institutions. Responses to CBRN incident hoaxes can incur significant costs resulting in key resources being diverted from areas where they really are needed.

3. CBRN security capacity assessment

CBRN security encompasses governance frameworks, processes, structures, mechanisms, and practices that aim to ensure and promote the prevention and countering of the misuse of CBRN materials and information. It focuses on two complementary goals: to safeguard CBRN materials and related information and infrastructure from misuse and diversion; and to ensure effective response to deliberate CBRN incidents (Figure 4).[29] The process of realising these goals is grounded in an all-hazard approach for managing CBRN risks which requires mainstreaming CBRN security considerations in different areas of action. These include institutional safety and security at facilities where chemical, biological, or radioactive materials and related information are used or stored; counter-terrorism and law enforcement (e.g. detection and investigation of crimes involving CBRN material or related information); crisis management and emergency preparedness (e.g. medical assistance, decontamination); and defence (e.g. intelligence-gathering, WMD counter-proliferation, CBRN protection).

[29] This understanding of CBRN security is consistent with the core objectives of the EU Action Plan on CBRN security risks, see European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee, and the Committee of the Regions, *Action Plan to Enhance Preparedness against Chemical, Biological, Radiological and Nuclear Security Risks*, COM(2017) 610, 18 October 2017.

Figure 4: CBRN security – goals and areas of action



Source: Authors

Activities such as biomedical research, pharmaceutical development, medicine, agriculture, manufacturing, and energy production involve the use of chemical, biological, radioactive, or nuclear materials and related information. To ensure that the legitimate application of CBRN materials and information is not compromised by individuals or entities seeking to cause harm, stakeholders across relevant sectors are implementing appropriate measures, initiatives, and practices for safety and security.[30] Integrating safety and security frameworks and procedures is key, as safety shortcomings or acts of negligence can create vulnerabilities that malevolent actors could exploit.

Responding to deliberate CBRN events requires planning and preparedness for effective coordination during incident management. The cause of the event may not be immediately

[30] See, for example, World Institute for Nuclear Security, WINS Academy, 2022; European Chemical Industry Council (Cefic), *The European Responsible Care Security Code*, 2010; Inter-Academy Partnership, *IAP Statement on Biosecurity*, 2005 (IAP has also endorsed the *Tianjin Biosecurity Guidelines for Codes of Conduct for Scientists*, 2021); International Gene Synthesis Consortium, *Harmonised Screening Protocol: gene sequence and customer screening to promote biosecurity*, 19 November 2017.

apparent and deliberate events could at first resemble accidents or natural phenomena (e.g. natural disease outbreaks). Established protocols and mechanisms for dealing with CBRN incidents such as systems for disaster and accident management could support the implementation of adequate response measures and facilitate incident investigation.

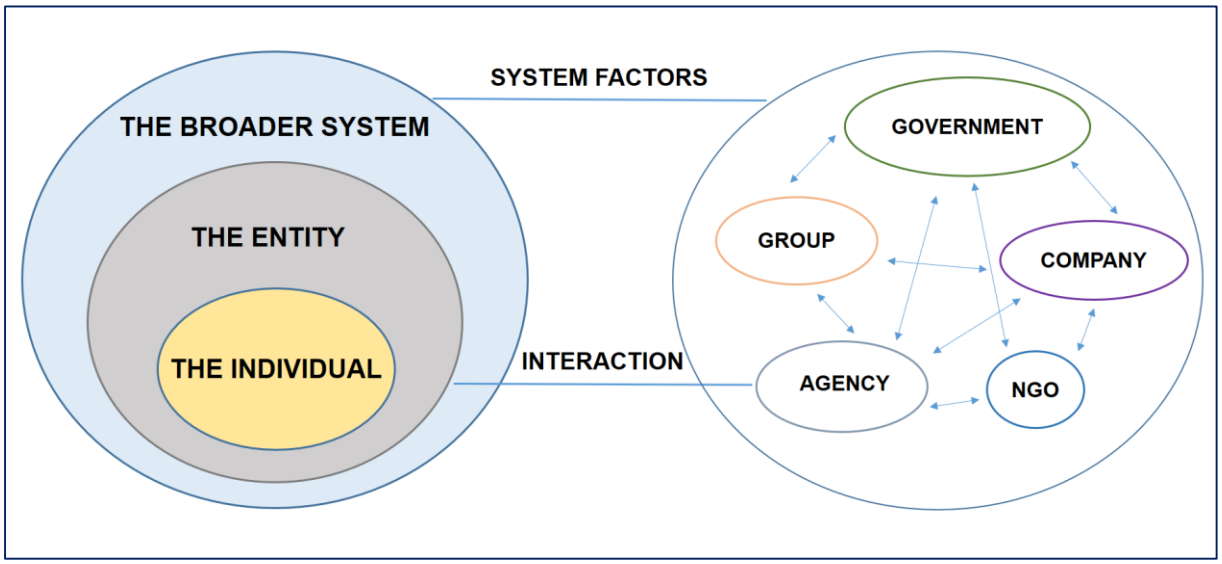
To remain relevant in the face of emerging threats, it is important that the governance mechanisms dealing with CBRN security can address and accommodate the evolving range of risks concerning the misuse of CBRN materials and related information. In other words, these mechanisms need to be flexible enough to ensure a greater adaptive capacity. The process of adaptation requires that systems, entities, and individuals recognise the changes that occur in their milieu and respond to these changes in ways that enable them to continue to operate and function sustainably. Sustainability is key to effective adaptation; yet neither adaptation nor sustainability is easy to measure in quantitative terms.

Risk analysis is at the heart of adaptation. Risk analysis allows identifying and prioritising potential threats and provides for mapping possible approaches, steps, and initiatives that can be leveraged to tackle local vulnerabilities and ultimately contribute to sustainable risk management outcomes. The proposed methodology rests on the assumption that maintaining CBRN security capacity is essential for effective CBRN security risk management and the performance of core relevant functions. The methodology is intended as a tool for facilitating consideration on CBRN security risk mitigation from a cross-sectoral perspective whereby stakeholder interaction is a key attribute of capacity. It maps cross-cutting areas of action that are common to all three domains – chemical, biological, and radiological/nuclear – but it could also be used to monitor capacity in any of these security domains separately.

Framing CBRN security capacity

Capacity is the power of a system, an organisation, a person, etc. to perform or to produce; it is not a passive state but part of a continuing process.[31] Human resources and the overall context within which organisations undertake their functions are central to capacity development and maintenance. Capacity assessment is a structured and analytical process whereby the various dimensions of capacity are assessed within the broader systems context, as well as evaluated for specific entities and individuals within the system. Capacity can be analysed at three levels (Figure 5).

Figure 5: Modelling capacity



Source: Based on UNDP[32]

The highest level is the broader system or enabling environment level. It includes both formal and informal organisational entities, as well as their relationships and interactions, and the

[31] Adapted from United Nations Development Programme, *Capacity Assessment and Development: In a Systems and Strategic Management Context*, Technical Advisory Paper No 3, January 1998.
[32] United Nations Development Programme, *Capacity Assessment and Development: In a Systems and Strategic Management Context*, Technical Advisory Paper No 3, January 1998.

system factors that shape and impact on these. Capacity at the second level – the entity or organisation level – applies both to government agencies/units and private-sector enterprises. Capacity assessment at this level also highlights the interactions between entities within the broader system. The third level of capacity is the individual level which also includes small networks of individuals. This level addresses the individual's capacity to function efficiently and effectively within the entity and within the broader system. Capacity assessments are designed according to the individual's function and relationship to the entity. Capacity at each level can be approached in terms of dimensions (Table 1).

Table 1: Capacity dimensions

Broader system level	Entity level	Individual level
❖ Policy dimension – e.g. value systems. ❖ Legal/regulatory dimension – e.g. rules, laws, norms, standards. ❖ Management/accountability dimension – e.g. entities and stakeholders that function within the system. ❖ Resources dimension – e.g. availability of human and financial, information resources. ❖ Process dimension – e.g. interrelationships, interdependencies and interactions among the entities.	❖ Mission and strategy dimension – e.g. role, mandate, interactions with stakeholders. ❖ Culture/structure and competencies dimension – e.g. management values and style, standards, organisational structures. ❖ Processes dimension – e.g. relationships with other entities, management, planning. ❖ Resources dimension – e.g. human, financial, information resources. ❖ Infrastructure dimension – e.g. physical assets.	❖ Job requirements, skill levels, and needs. ❖ Training, re-training, individual learning, on-the-job-training. ❖ Accountability, ethics. ❖ Access to information, networking. ❖ Performance, professional conduct. ❖ Values, attitudes, morale, motivation, professional integrity. ❖ Inter-dependencies, inter-relationships, teamwork. ❖ Job sharing. ❖ Communication skills.

Source: UNDP 1998.[33]

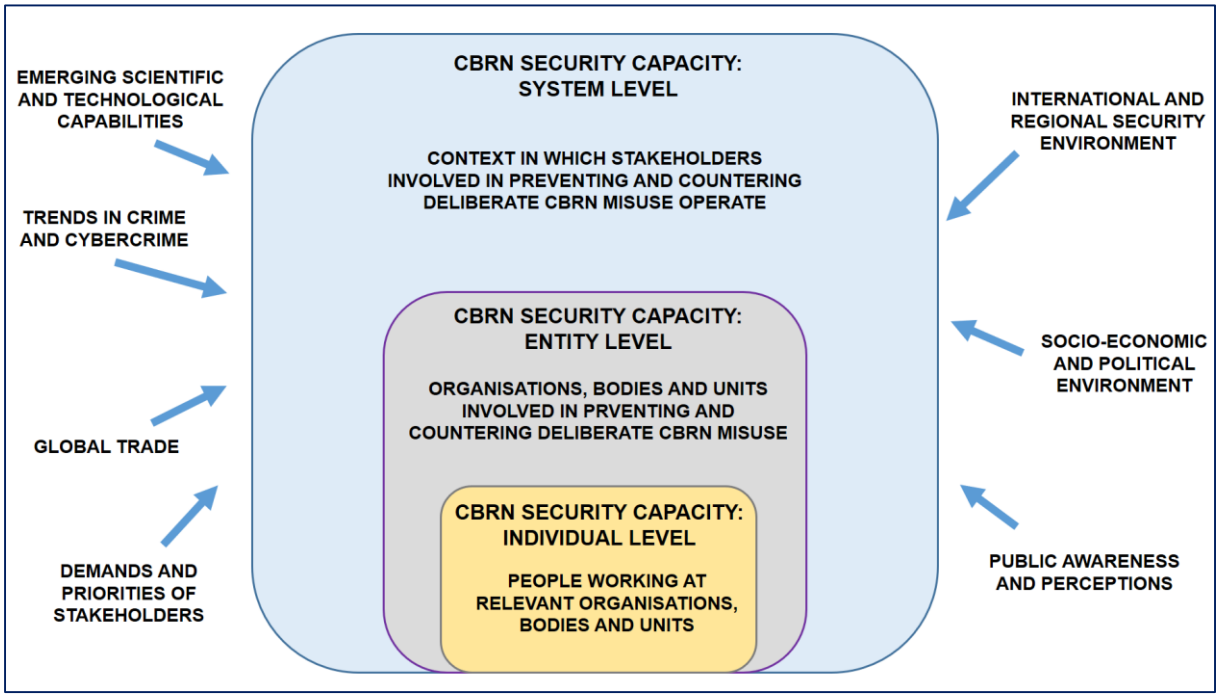
[33] Adapted from United Nations Development Programme, *Capacity Assessment and Development: In a Systems and Strategic Management Context*, Technical Advisory Paper No 3, January 1998.

CBRN security capacity is defined as the ability to perform functions of relevance to CBRN security – that is to prevent and counter the misuse of CBRN materials and information – effectively, efficiently, and sustainably.[34] CBRN security capacity (Figure 6) encompasses:

1) An enabling system that underpins various aspects of CBRN security through the provision of policies, regulatory arrangements, infrastructural setting, and processes underpinning inter-agency and stakeholder interactions.
2) Entities and organisations such as competent authorities, specialised agencies, and non-governmental stakeholders but also institutional departments, units, committees, designated officers etc.
3) Individuals with competencies and skills to perform CBRN security risk management tasks and functions in accordance with their roles and responsibilities.

[34] Adapted from United Nations Development Programme, *Capacity Assessment and Development: In a Systems and Strategic Management Context*, Technical Advisory Paper No 3, January 1998.

Figure 6: CBRN security capacity modelling



Source: Based on UN FAO[35]

CBRN security capacity at different levels is approached in terms of dimensions. Table 2 looks at the dimensions of capacity at the system, or national level. Each dimension comprises indicative modalities. The suggested modalities are generic and common to the chemical, biological, or radiological/nuclear domain. The list of modalities presented in Table 2 is not exhaustive.

[35] Adapted from Food and Agriculture Organisation of the United Nations (UN FAO), *FAO Biosecurity Toolkit*, 2007.

Table 2: Dimensions of CBRN security capacity

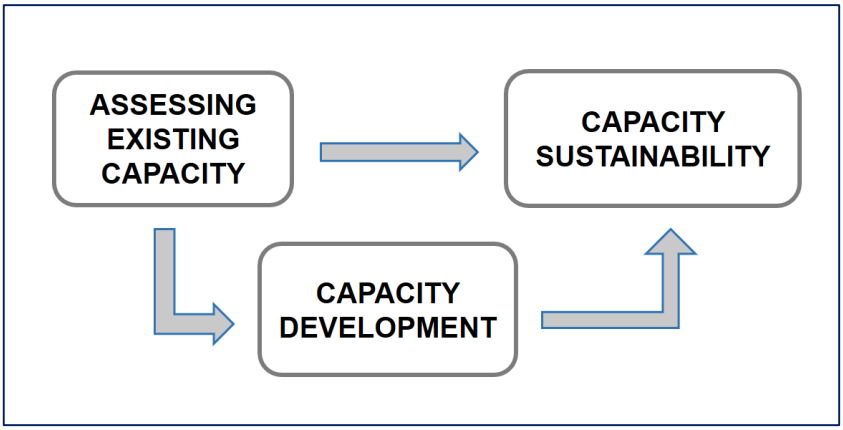
Level / Dimension	System (national) level
Policy / regulatory	Indicative modalities include national instruments that are consistent with the goals of CBRN security such as: ❖ policy frameworks; ❖ legal acts and regulations; ❖ certification and licensing; ❖ standard-setting documents; ❖ guidelines; ❖ voluntary initiatives such as sector-wide codes or charters.
Institutional dimension	Indicative modalities include entities and organisations that perform roles and functions of relevance to CBRN security such as: ❖ competent authorities; ❖ specialised agencies; ❖ departments or units; ❖ institutional committees; ❖ designated officers.
Operational dimension	Indicative modalities include processes of relevance to CBRN security such as: ❖ training, skill development, and competence validation; ❖ risk assessment at the national or sector-wide level; ❖ scientific/technical advice and data sharing; ❖ intelligence gathering; ❖ material accountability; ❖ inspection regimes and verification of certificates; ❖ authorisation of activities involving sensitive or dual-use items or goods; ❖ detection and reporting of suspicious activities; ❖ early warning and incident notification; ❖ inter-agency operability and coordination in case of a deliberate CBRN event; ❖ incident response – e.g. provision of medical care, incident-site management, decontamination; ❖ forensics, diagnostics, and sample analysis;

	❖ incident investigation, identification of suspects, attribution, and establishing accountability; ❖ risk communication.
Technical dimension	Indicative modalities include infrastructure and resources (human, financial, information) for implementing CBRN security: ❖ specialised equipment (e.g. for agent/material identification and detection; decontamination; personal protection); ❖ systems for the physical protection of sensitive materials, equipment, and information; ❖ systems for tracking and tracing of sensitive material; ❖ systems for secure data storage, electronic record keeping, and exchange; ❖ secure computer networks; ❖ secure ICT networks; ❖ trained personnel; ❖ professional competence and expertise; ❖ training and re-training opportunities; ❖ technology development, procurement, and maintenance.

Methodology for CBRN security capacity assessment

Capacity is not a fixed state and maintaining existing capacity is *per se* a dynamic process. Whereas capacity assessment is generally associated with capacity development, it could also provide important insights into the factors that contribute to and impact capacity sustainability (Figure 7).

Figure 7: Role of capacity assessment



Source: Authors

The proposed methodology offers an indicative structured approach for conducting a CBRN security capacity assessment at the national level. The methodology seeks to generate a holistic snapshot of national CBRN security risk governance including relevant policy and regulatory arrangements, types and roles of stakeholders, stakeholder interactions, and available resources. It could be used to inform policy-making and programming through the identification of needs and good practices. The development of the methodology rests on the following assumptions:

- CBRN security falls within the remit of multiple international regimes.
- CBRN security cuts across different sectors within government and civil society.
- CBRN security capacity entails a shared commitment among stakeholders to the goals of CBRN security risk management.

The methodology comprises three phases:

1) Context scoping;
2) Review and analysis;
3) Use of results.

The purpose and structure of each phase are described below.

Context scoping

The purpose of this phase is to profile the general context within which the CBRN security capacity assessment is taking place. Key aspects to be addressed here could include the reasons for conducting the assessment; the risk and threat environment at the national, regional, and/or international level and relevant trends and factors of national security significance; and the range of stakeholders involved in CBRN security at the national level.

A national CBRN security capacity assessment could be conducted for different reasons and these are likely to define the entire assessment process. For example, the setting of a capacity assessment triggered as a result of a local security incident or CBRN emergency would differ considerably from that of a periodic capacity assessment. Emerging risks or changes in the national or regional security landscape could also provide a rationale for assessing national CBRN security capacity. It is possible that an assessment is conducted within the framework of broader security initiatives or initiatives that focus on national preparedness for CBRN events regardless of their cause.

CBRN security risks are multifaceted and not always straightforward to predict, not least because individual states are not insulated from global trends and dynamics that drive high-impact security concerns. Whilst local risks are the utmost priority, screening the broader security environment prior to conducting the assessment allows keeping track of emerging threats and ensuring that these are considered as part of national CBRN security risk governance.

Stakeholder mapping helps identify sectors, organisations, and entities within government (including sub-national authorities) and civil society that perform functions of relevance to

CBRN security, or otherwise play a role or are involved in CBRN security risk management. Stakeholders could be categorised by their respective roles and responsibilities. Keeping the scope of stakeholder mapping as broad as possible during this phase can provide important insights into stakeholder interdependencies and relationships during the capacity assessment.

Review and analysis

The purpose of this phase is to provide a systematic overview of key aspects related to CBRN security governance at the national level. This is the core phase of the assessment process during which data are collected and analysed. Using the CBRN security capacity model outlined above, it is possible to organise the assessment so as to cover the following broad themes:

- Overall national systems context encompassing policy, legal, and regulatory frameworks, and organisational arrangements including distribution of core functions and coordination;
- Delivery and performance of core functions that are relevant to CBRN security;
- Linkages, interdependencies, and communication across sectors and stakeholders.[36]

Boxes 2-5 provide a set of indicative questions for each of the CBRN security capacity dimensions.[37] The boxes are supplemented with guiding notes on data collection and analysis. Figure 7 (7.1 and 7.2) shows an indicative template for organising capacity assessment data.

[36] Adapted from Food and Agriculture Organisation of the United Nations (UN FAO), *FAO Biosecurity Toolkit*, 2007.
[37] The questions presented in Boxes 2-5 are adapted from Food and Agriculture Organisation of the United Nations (UN FAO), *FAO Biosecurity Toolkit*, 2007.

Box 2: CBRN security capacity – Policy/regulatory dimension

Indicative questions

- Which existing policies (at central, regional, or local level) contain goals and objectives, and/or establish priorities of relevance to CBRN security?
- Which stakeholders have been involved in the formulation of these policies?
- Which existing laws or regulations (at the central, regional, or local level) are relevant to CBRN security?
- How are stakeholders' roles, responsibilities, and rights defined in these laws?
- To what extent are relevant national regulations harmonised with international frameworks and standards?
- Which existing national standards, guidelines, or recommendations are relevant to CBRN security?

Many international instruments (e.g. conventions, treaties, guidance documents, standards, etc.) that are relevant to CBRN security are domain-specific in the sense that they focus exclusively on biological security, chemical security, or nuclear security aspects. Whilst certain national policies or regulations may refer to all three categories, others may cover a particular domain. The indicative questions address national instruments that cover chemical, biological, and radiological/nuclear security issues both collectively and separately.

Box 3: CBRN security capacity – Institutional dimension

Indicative questions

- Which organisations and entities serve as competent authorities at the national, regional, and local level with responsibility for:
  - making policy decisions related to CBRN security?
  - planning and implementing programmes and activities related to CBRN security?
  - providing advice, policies, and support to international functions and coordination related to CBRN security (e.g. contact points for relevant international organisations, conventions and treaties, or initiatives)?
- Which other government and non-governmental stakeholders are involved in CBRN security and how (e.g. role in the formulation of policies and plans, compliance with

policies and regulations, performing incident response functions, providing relevant training etc.)?
- Do any inter-agency / multi-stakeholder mechanisms (e.g. committees, working groups, task forces) that perform functions of relevance to CBRN security exist?

It is possible that some of the information relevant to this capacity dimension is already available as a result of the stakeholder mapping during the context scoping phase. The indicative questions seek to assist with fine-tuning the initial stakeholder overview and to highlight areas of cross-sectoral cooperation.

Box 4: CBRN security capacity – Operational dimension

Indicative questions

- How do competent authorities and bodies involved in CBRN security at the national, regional, and local level communicate and share information:
  - with each other?
  - with relevant national stakeholders (e.g. other government agencies, industry, science/research/academia, general public)?
  - with each other in case of emergency / crisis situation?
  - with other national governments?
  - with relevant international organisations?
- What core functions are performed at the national, regional, and local level to support the prevention of misuse of CBRN materials and related information? Which stakeholders are involved in the delivery of these functions?
- What core functions are performed to facilitate national preparedness in case of a deliberate CBRN incident? Which stakeholders are involved in the delivery of these functions?

It is possible to use the MASC-CBRN Training guide when completing this element of the capacity assessment methodology. This guide features practical scenario-based exercises which are designed to facilitate consideration on CBRN security risk management. The exercises could be used for reviewing the roles and responsibilities of different stakeholders and validating established standard operating procedures.

Box 5: CBRN security capacity – Technical dimension

Indicative questions

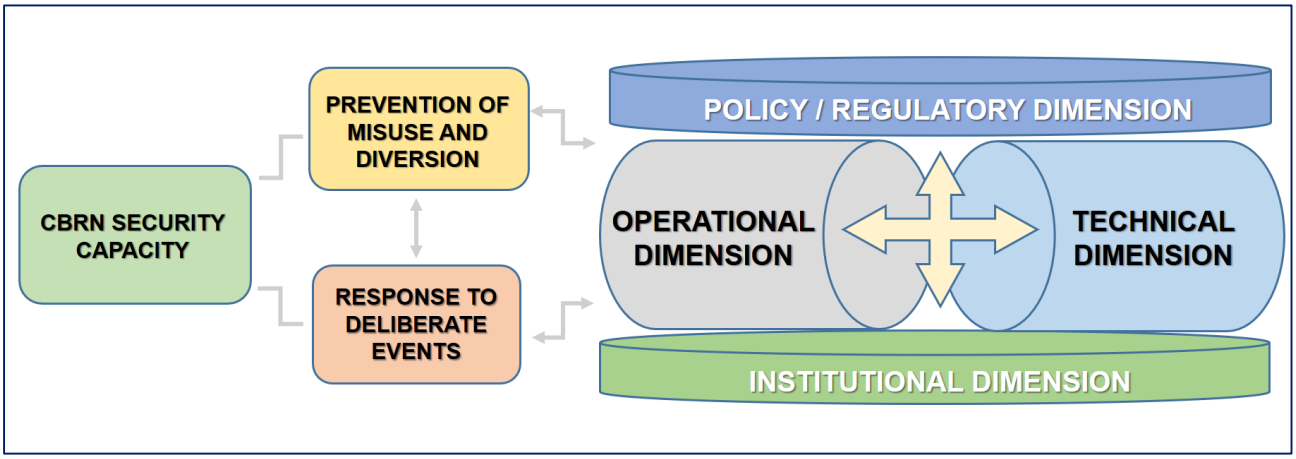
- Which government agencies serve as competent authorities with responsibility for providing technical and financial resources for programmes and activities related to CBRN security?
- What infrastructure and technical equipment are available at the national level to perform functions of relevance to CBRN security?
- What opportunities for CBRN security training and professional development programmes are available to competent authorities and other government and non-government stakeholders?

This element of the methodology focuses on the availability and distribution of resources for CBRN security. Data collected here can help facilitate choices between competing fiscal priorities and enable allocating available resources to sectors where these are most needed.

Figure 8 outlines the CBRN security capacity assessment process (8.1) and provides an indicative template for organising data collection (8.2).

Figure 8: CBRN security capacity assessment methodology

8.1 Process overview



8.2 Indicative template

CBRN security capacity dimension / CBRN domain	POLICY / REGULATORY			INSTITUTIONAL			OPERATIONAL			TECHNICAL		
	Defence / civil protection	Counter-terrorism	Oversight of activities	Defence / civil protection	Counter-terrorism	Oversight of activities	Defence / civil protection	Counter-terrorism	Oversight of activities	Defence / civil protection	Counter-terrorism	Oversight of activities
BIOLOGICAL												
CHEMICAL												
RADIOLOGICAL / NUCLEAR												

Source: Authors

CBRN security cuts across different sectors. The indicative template outlined above is intended as a tool for the systematic organisation of the data collected as part of a CBRN security capacity assessment. Information about the different capacity dimensions can be divided into categories. A list of suggested categories is provided below:

- Defence and civil protection – this category refers to national preparedness for deliberate CBRN incidents and crisis management.
- Counter-terrorism – this category refers to the process of minimising CBRN security risks posed by non-state actors.

- Oversight of activities involving CBRN materials and related information – this category refers to institutional safety and security for activities involving CBRN materials and related information.[38]

Use of results

The scope of this phase will depend on the purpose of the CBRN security capacity assessment. For example, the assessment results could be used to map and formulate transferable good practices; to identify options and intervention points for maximising efficiency; or to define needs to achieve desired capacity. It is important that the results of the capacity assessment are shared across sectors and communicated among stakeholders to provide a common reference framework for CBRN security risk management at the national level.

[38] The suggested categories are described in MASC-CBRN, *Online Database*, 2021. Also see Tatyana Novossiolova and Maurizio Martellini, *Effective and Comprehensive CBRN Security Risk Management in the 21st Century*, EU Non-Proliferation and Disarmament Papers Series, No 75, June 2021.

4. Conclusion

The range of CBRN threats is evolving in a highly globalised environment. These threats are systemic which has important implications for the sustainability of CBRN security capacity, including the need to identify country-specific CBRN security priorities and maintain a multi-layered system for CBRN security risk management. CBRN security falls within the purview of government agencies and specialised bodies in the area of defence, law enforcement, border control, strategic trade management, intelligence gathering, safety and security oversight, health security, and crisis management. Besides competent authorities that perform core functions, stakeholders across government and non-government sectors can play an important role in delivering essential services and developing relevant initiatives to support the implementation of actions that contribute to enhancing the prevention, detection, preparedness, and response to CBRN threats.