NATO OTAN

International Military Staff
Etat-Major Militaire International

Brussels - Belgium

15 July 2025 IMSM-0198-2025

ALL MILITARY REPRESENTATIVES

NATO'S CHEMICAL, BIOLOGICAL, RADIOLOGICAL AND NUCLEAR DEFENCE CONCEPT

1. The Military Committee approves the public disclosure of NATO's Chemical, Biological, Radiological and Nuclear Defence Concept and its publication as a printed booklet and posting to the NATO Public website.

2. This document clears IMSWM-0204-2025 and all SDs thereto.

15 July 2025 at 17:36
Remigijus Baltrenas
Lieutenant General, LTU Army
Director General
International Military Staff

Annex:

A. NATO's Chemical, Biological, Radiological and Nuclear Defence Concept.

Copy to: IMS SDL CG+SC+SCR, IMS-P&C, IMS-O&P, IMS-L&R, IS-DPP.
Originating Office: P&C - PC-NCAB.
Action Officers: LtCol Unzeitig, P&C (7375); LtCol Dr. Kollmer, P&C (5313).
Tasker Number: IMS/2025/1489
Taxonomy: Defence Capability and Planning (DEF) - DEF - Defence Capabilities

NATO's Chemical, Biological, Radiological and Nuclear Defence Concept

Table of Content

PART I - INTRODUCTION

Background

1. NATO's deterrence and defence posture are based on an appropriate mix of nuclear, conventional and missile defence capabilities, complemented by space and cyber capabilities. It is defensive, proportionate and fully in line with NATO's international commitments.

2. Since the Lisbon Summit in 2010 NATO Heads of State and Government have consistently noted the relevance of CBRN Defence as part of NATO's overall deterrence and defence. The NATO 2022 Strategic Concept (Reference A), endorsed at the Madrid Summit, reiterates the importance of CBRN defence, noting that "we will continue to invest in our defence against Chemical, Biological, Radiological and Nuclear threats. We will enhance our policies, plans, training and exercises and assess our capabilities to ensure that these requirements are integrated into our deterrence and defence posture".

3. Furthermore, "NATO's security environment has grown more complex and challenging since 2009, when Allies agreed NATO's Comprehensive, Strategic-Level Policy for Preventing the Proliferation of Weapons of Mass Destruction (WMD) and Defending against Chemical, Biological, Radiological and Nuclear Threats. Today, we face a world in which the potential use of CBRN materials or WMD by state and non-state actors remains a central and evolving threat to Allied security. It is a world in which NATO increasingly cannot assume that the international norms and institutions related to the proliferation or use of WMD will ensure our security, and in which scientific and technological innovation and other emerging trends have accentuated CBRN risks to the Alliance".

4. The Vilnius Summit confirmed the urgency of the implementation of NATO's new CBRN Defence Policy and the investments into the military capabilities required to effectively operate, fight and prevail in any environment, and to ensure national and collective resilience against CBRN risks and threats.

5. NATO's CBRN Defence Policy states that NATO populations, territories and forces will be defended and secure against the threat or use of CBRN materials and WMD. The Alliance will enhance the resilience of its nations and societies against the full spectrum of CBRN threats and encourage cooperation between Allies to enhance international norms. The proliferation, threat or use of WMD and their delivery systems will not undermine NATO's deterrence and defence. Therefore, NATO forces must be able to operate effectively, fight and prevail in any environment.

6. Moreover, "NATO remains clear-eyed about the CBRN challenge: Allies will have all the appropriate tools to ensure that potential adversaries do not perceive that they can gain a clear advantage against NATO by using, or threatening to use, CBRN materials".

7. NATO will undertake its CBRN defence related activities with NATO Partners and NNEs in accordance with the NATO Strategic Concept and the Comprehensive Approach Action Plan.

8. NATO's CBRN Defence Policy therefore establishes the framework upon which the Alliance will understand, plan, posture, exercise, train, equip, and assess its capabilities in order to counter WMD proliferation and ensure that we deter and defend our Alliance against all CBRN threats.

Purpose, Aim and Scope

9. This concept translates NATO's CBRN Defence Policy into a strategic direction and guidance for all NATO Allies and NMAs. Furthermore, it informs the requirements for CBRN defence capabilities, fully integrating into and enhancing the NATO Military Instruments of Power (MIoP) necessary for accomplishment of the Alliance's deterrence and defence.

10. This concept establishes common and harmonized approaches to develop, maintain and sustain effective CBRN defence consistent within the procedural understanding of the CBRN Defence Lines of Effort (CBRND LOE) prevent, protect, and recover, and to contribute to Allied security across the full spectrum from peacetime vigilance through crisis to conflict.

11. CBRN defence in Multi-Domain Operations (MDO) mandates utilizing defence capabilities to counter CBRN attacks or incidents occurring in the Maritime, Land, Air, Space and Cyberspace operational domains.

12. The aim of this concept is to provide the conceptual framework for credible and coherent NATO CBRN defence, encouraging CBRN defence capability development by drawing upon the collective competencies of all Allies and NATO bodies through an integrated and holistic political, military and civilian approach. Furthermore, it will recognize the undeniable importance of Civil-Military Interaction (CMI), allowing the Alliance to face the CBRN threats and challenges of the rapidly changing security environment. Consequently, this concept provides NATO, national authorities and decision-makers at all levels with a strategic direction to foster CBRN defence capability development across all areas to strengthen the Alliance's resilience.

13. This concept is guided by a shared and lasting commitment to prevent the proliferation of WMD, protect the Alliance against CBRN incidents, and support recovery from the consequences of any such use.

14. This concept distinguishes the political, civilian and military dimensions of NATO's CBRN Defence Policy, based on its integrated approach, while remaining consistent with the NATO's CBRN Defence Policy LOE of prevent, protect and recover. Moreover, it envisages NATO CBRN defence against a more complicated CBRN threat environment, dominated by ambiguity and uncertainty. This concept clearly addresses the hybrid character of CBRN threats, the aggravating factor of the emerging and disruptive technologies (EDT) and the devastating impacts of climate change, particularly in the urban environment. This concept focuses on CBRN defence. All relevant aspects of preventing proliferation and countering WMD are outlined in the Weapons of Mass Destruction Disablement Functional Concept and other subordinated documents.

15. Information Sharing between NATO, NATO Partners and Non-NATO Entities (NNEs) will be done in accordance with relevant NATO policies and procedures, as well as security agreements as appropriate.

PART II - CONCEPTUAL FRAMEWORK

16. This chapter describes the role of CBRN defence in the implementation of NATO's political and military strategy. It also contributes the ongoing wider military adaptation and modernization of the Alliance.

17. It details how an integrated and credible CBRN defence supports NATO's deterrence and defence posture in line with its 360-degree approach from peacetime vigilance through crisis to conflict.

18. The chapter also underscores the CBRN defence mission and tasks, as well as the role of CBRN defence in NATO crisis prevention and management.

19. National and collective resilience contributes to NATO's deterrence and defence posture, as well as reinforces the execution of the Alliance's core tasks. NATO's Seven Baseline Requirements for national resilience provide a comprehensive framework to support the effective enablement of Allied armed forces and of NATO's core tasks. The Baseline Requirements include measures for CBRN defence preparedness.

20. CBRN defence in support of resilience requires successful two-way collaboration between Allies' military and civilian authorities. It requires two mutually reinforcing layers and their corresponding interdependencies. Therefore, strengthening both the civil enablement of the military and the military support to civilian authorities is fundamental.

Multi-Domain Operations

21. In the context of MDO, CBRN threats and CBRN incidents can disrupt military operations, cause mass casualty situations, may overwhelm critical infrastructure as well as have long-lasting effects on civilian populations and the environment. Therefore, it is crucial to consider CBRN defence and response capabilities as an integral part of planning and executing MDO.

22. NATO must develop strategies to sustain an effective CBRN defence across all domains. The integration of CBRN defence capabilities into MDO must encompass all aspects of CBRN defence enabling components.

23. While using all MIoP to maintain an effective CBRN defence, MDO must also utilize for Non-MIoP as they provide important capabilities against CBRN Threats.

24. CBRN defence must be synchronized, as a part of integrated planning. In addition to that, CBRN defence must support Force Protection (FP). Therefore, the collaboration between the different military branches, the Allied nations, as well as military and civilian authorities, is essential to ensure effective coordination and response to CBRN incidents.

NATO Crisis Response Process and CBRN defence

25. The Alliance must be prepared to perform a whole range of Article 5 and non-Article 5 crisis response operations (CRO) in circumstances that, in many cases, will be difficult to predict. NATO Allies have a shared interest in contributing to stability and managing conflicts together. In this essence, due to one of its three core tasks, the Alliance will build on the unique capabilities and expertise which are developed and implemented for

NATO's crisis management. To that end, the Alliance will strengthen the investments in crisis response, preparedness and management through exercises, and leverage its ability to coordinate, conduct sustain and support multinational CRO.

26. NATO Allies will develop an appropriate mix of CBRN defence measures, expertise and capabilities enabling NATO to respond to a crisis involving the threat or use of WMD or CBRN material.

27. The NATO Crisis Response System (NCRS) provides the Alliance with a comprehensive set of options and measures to manage and respond to crises, including sudden shifts in the security environment, with the necessary degree of agility, discrimination, progressiveness and responsiveness, taking full advantage of both available and emerging tools and capabilities. Therefore, the NCRS, which provides the Alliance's overarching procedural architecture within both military and non-military crisis response planning processes, should be designed and coordinated.

PART III - THE EVOLVING CBRN THREAT

28. NATO faces a security environment in which CBRN threats have grown more numerous and more diverse, in which state and non-state actors pose a greater threat of WMD use and proliferation, and where technological trends are rapidly amplifying these risks. Allies recognize the scope of the changing threat and the steps necessary to ensure Alliance's security in this challenging context.

29. NATO faces a widening spectrum of chemical threats, ranging from traditional chemical materials to so-called Fourth Generation Agents (FGA) and pharmaceutical-based agents (PBA), that may challenge detection, response and protection measures.

30. Biological agents also pose unique and enduring challenges to NATO deterrence and defence operations, including deliberate use of biological agents, accidental release and contact with endemic and imported diseases.

31. EDT could create dual-use capabilities which affect NATO's security environment in increasingly diverse ways. New technologies, including nanotechnology, synthetic biology and additive manufacturing, threaten to enable development of even more effective or more lethal CBRN material, including those that can overcome protective measures and resist detection, decontamination, or medical countermeasures. Artificial Intelligence (Al) technology could be misused to design highly toxic chemical and contingous biological agents.

32. Potential implications and effects associated with the existence of cyber threats must also be reflected and addressed by CBRN defence.

33. CBRN materials can be employed by potential adversaries to challenge the thresholds of detection and identification with the intention to create ambiguity, delay or prevent attribution, and impair decision-making processes, which are hallmarks of hybrid threats.

34. Understanding CBRN risks and threats and possible countermeasures to WMD proliferation trends, networks and a potential adversary's WMD capabilities and intentions, is vital to developing responses. Intelligence gathering and analysis plays a crucial role in identifying potential adversaries' CBRN capabilities, intentions and potential targets and provide decisive information for the CBRN defence planning. This information supports decisionmakers and their CBRN defence staff to develop effective strategies, allocate resources to counter CBRN threats and establish an appropriate FP.

35. NATO's defence against CBRN threats must also address their nexus with cyber threats. The internet is a key channel for the proliferation of WMD-related technical knowledge and expertise. Malicious cyber actors may attempt to undermine NATO's capacity to prevent and effectively respond to a CBRN incident by targeting NATO or Allied communications and information systems. Cyberattacks against critical infrastructure highlight the risk that cyber capabilities could be used to compromise industrial or scientific infrastructure with the intent to cause the release of toxic industrial chemicals or another CBRN incident.

36. In MDO, cyberspace is a critical domain that might be exploited by adversaries to disrupt CBRN defence capabilities and measures or compromise sensitive information. Robust cybersecurity countermeasures are necessary to safeguard CBRN-related communication, data and control systems from cyber threats.

37. Cyberspace and the increasing digitalization of critical infrastructure sectors and the associated industrial systems, particularly the digitalization of chemical, biological, radiological and nuclear facilities, is changing the nature of cyber-risks. These conditions, coupled with the rapid advance of cyber technology and the multiple opportunities, increases the level and type of CBRN threats.

38. Disinformation and malicious cyber activity following a CBRN incident aiming to disrupt a coherent Allied respons and illustrate the nexus of hybrid and CBRN threats.

39. The development of new CBRN materials, including those that are more difficult to detect, trace, or investigate, and novel means of targeting and delivery, may generate new opportunities for CBRN use alongside hybrid techniques. These developments might also implicate new challenges for CBRN defence and its capabilities.

PART IV - CBRN DEFENCE FUNDAMENTALS

40. This chapter describes the main fundamentals of CBRN defence through the applied NATO's integrated approach which focuses on breaking the CBRN incident chain (as early as possible) beyond the two-core principles and commitments.

41. NATO's two core CBRN defence principles and commitments are anchored by strategic enablers, which are crosscutting capabilities that enable the Alliance to fulfil full range of the commitments. As displayed in the figure below, the strategic enablers facilitate NATO's efforts to defend against CBRN threats and WMD. It also displays how NATO's CBRN Defence Policy rests upon the complementary, mutually reinforcing principles and commitments, including the framework of CBRND LOE Prevent, Protect and Recover.

Figure 1: NATO's CBRN Defence Policy Principles and Commitments.

Core Principle and Commitment 1 – Enhanced and Integrated CBRN Defence Military Capabilities

42. Allies will continue to improve and adapt the sustainability, ability to deploy, and interoperability of their capabilities for the evolving and demanding strategic environment. The Alliance supports the development of CBRN defence capabilities through its Joint CBRN Defence Capability Development Group (JCBRND CDG). National capability development plans will support the full and timely implementation of CBRN defence capabilities, in particular those required by the Alliance in line with the NATO Defence Planning Process (NDPP).

43. NATO forces must be prepared to prevent conceptualization, development, possession, proliferation and use of WMD and CBRN substances, including related expertise, materials, technologies and means of delivery, and to mitigate their effects. Basic, enhanced and specialised CBRN defence capabilities contribute to the CBRND LOE, enabling NATO forces to operate, fight and prevail in a CBRN environment.

44. To achieve this NATO Allies must take into consideration the requirement to fully implement NATO CBRN defence, as well as integrate appropriate national CBRN defence capabilities at all levels into force structures.

45. The following integrated approach describes how the implementation of the NATO CBRN defence capabilities along the CBRND LOE will meet the requirements to achieve maximum effect and efficiency.

The NATO CBRN Defence Integrated Approach

46. The CBRND LOE addressed in NATO's CBRN Defence Policy provide the framework for CBRN defence within NATO. Together with the integrated CBRN defence military capabilities, the basic, enhanced and specialised CBRN defence capability proficiency levels lay out an integrated approach for NATO CBRN defence.

47. The CBRND LOE encompass the different phases of pre-, during and post-CBRN incident. Together, these phases form the CBRN incident chain. Important for the understanding of this concept is that the phases must not be considered as separate or distinct, but rather that they support and supplement each other.

48. Based on this approach, CBRN defence offers opportunities, delineated through the phases of pre-, during and post-CBRN incident, to interrupt the CBRN incident chain as early as possible through planning, preparing and implementing appropriate measures. The purpose of these measures is to achieve appropriate effects within the respective CBRND LOE.

49. Applied to a CBRN incident, this effects-based approach can be seen as a chain of interdependent events and activities. In the context of this concept, it describes a CBRN incident chain as shown in the following figure.

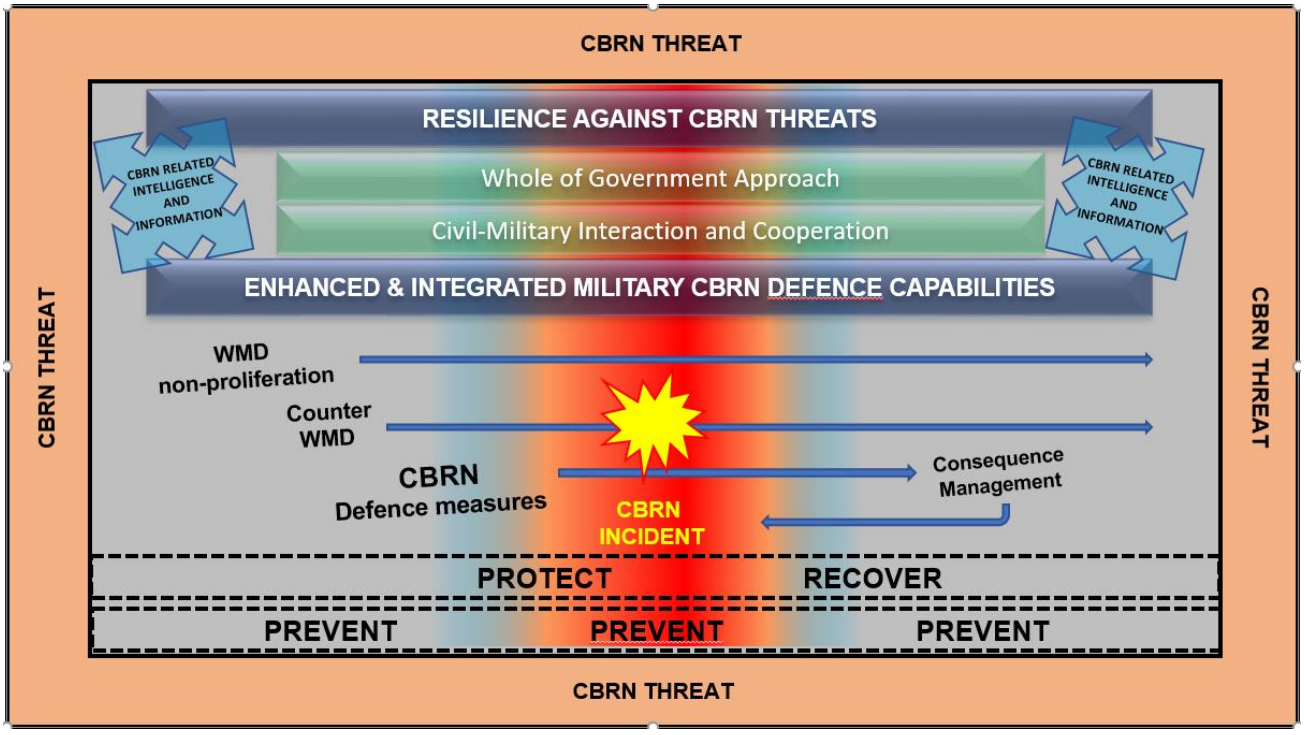

Figure 2: Example for a presumed CBRN incident chain.

50. NATO forces, units and entities must be fully prepared and ready to effectively operate, fight and prevail in a CBRN environment and to support national civilian authorities in case of a CBRN incident.

51. Deterrence is an important criterion for the success of an effective and efficient CBRN defence, along with ensuring strong civil preparedness. Therefore, CBRND LOE must be robustly and sustainably supported by military CBRN defence and civil CBRN response capabilities and complementary non-military activities.

52. Consequently, the emphasis of NATO CBRN defence must be on the “Prevent” CBRND LOE. Therefore, NATO CBRN defence capabilities must be appropriately staffed, equipped and integrated in support of political and diplomatic activities in order to prevent the occurrence of CBRN incidents. This approach will contribute to deterring potential adversaries from the use of WMD and CBRN material.

53. However, all CBRND LOE support the plans, procedures and activities intended to contribute to the prevention of WMD use or CBRN incidents. They must also be taken into consideration throughout all levels of operations planning, providing a basis for conducting effective CBRN defence on operations pre-, during and post- CBRN incident.

54. Moreover, in case of deployment Host Nation support is vital. Therefore, standardised communication, interoperability and sufficient capability stocks will be important requirements.

CBRN Defence Lines of Effort

55. Breaking the CBRN incident chain must consider the following key aspects:

a. The CBRND LOE.

b. The integrated levels of CBRN defence military capabilities.

c. The behaviour, actions or recognised intent of a potential adversary to acquire, possess, threaten to use, prepare and conduct an attack with WMD, CBRN weapons and CBRN devices.

d. The principal CoAs are to prevent the acquisition of WMD, deter or counter the use of WMD, reduce potential adversaries’ extant WMD capabilities, disrupt WMD delivery, prevent follow-on attacks and mitigate effects of WMD use and to counter its narratives.

e. Cross-disciplinary collaboration includes science and technology, CBRN medical support and biodefence to develop medical countermeasures (MedCM), diagnostic platforms, operational bio-surveillance and casualty/patient care systems, as well as information and intelligence sharing.

56. NATO’s integrated approach toward CBRN defence is conducted within a continuum of possible potential adversary actions. These events are expected to occur anywhere along this continuum, at any time and by multiple adversaries.

57. From an operational point of view, the objective of CBRN defence is to identify options to actively contribute to and support actions aimed at breaking a CBRN incident chain as early as possible.

Prevent

58. The “Prevent” CBRND LOE sets the framework for a systematic, holistic and integrated approach for both preventing the proliferation of WMD and defending against CBRN threats. The most effective contribution of CBRN defence to deterrence and defence posture can be provided through the effective and efficient prevention of proliferation of WMD and CBRN material.

59. The process of development, acquisition, fielding and sustainment of relevant and credible CBRN defence capabilities as well as training and exercises heavily contributes to the “Prevent” CBRND LOE. This process must be exploited by information activities. Supporting information activities against adversaries’ intentions regarding CBRN related activities might also help prevent the employment of CBRN substances.

60. Successful implementation of the “Prevent” CBRND LOE may avoid or disrupt adversary acquisition or employment of WMD and CBRN material. The ability to conduct countering WMD and interdiction operations, including by sea, plays a central role in preventing the proliferation of WMD and CBRN material, their means of delivery, and related materials and technologies.

Protect

61. The “Protect” CBRND LOE focuses on maintaining the ability of Allied forces, with mutual support of civil response capabilities, to continue conducting operations in a CBRN environment. This includes measures to identify such threats and hazards to reduce the vulnerability, to prevent or mitigate the effects of a WMD attack or a CBRN incident, as well as preparations to respond.

62. A prerequisite for the “Protect” CBRND LOE is full implementation of basic and enhanced CBRN defence capabilities, enabling NATO forces to operate, fight and prevail in a CBRN environment.

Recover

63. The “Recover” CBRND LOE is a complex process and involves many resources, capabilities, and capacities. All functions, activities and measures of this CBRND LOE should begin immediately following a WMD attack or a CBRN incident and must be conducted in parallel to and coordinated with the civilian emergency response.

64. The primary responsibility for CBRN consequence management resides with the affected Nation’s government or authorities. Military CBRN defence capabilities must be able to support civilian authorities to conduct CBRN response measures.

65. CBRN defence capabilities, measures and efforts contribute to the “Recover” CBRND LOE in order to restore essential capabilities, protect health and safety and provide

emergency relief, as well as to support civilian authorities should the Alliance suffer a WMD attack or CBRN incident.

CBRN Defence Lines of Effort within Core Principle 1

66. Prevent: NATO's CBRN defence capabilities provide an essential preventive and deterrent effect, by reducing the advantage that any adversary could hope to gain by the employment of WMD or CBRN material. Pre-crisis coordination, arrangements and planning at a national level are necessary to support a whole-of-government approach to CBRN preparedness and prevention.

67. NATO Allies must acknowledge that the development and implementation of CBRN defence capabilities is fundamentally a national responsibility. Although Nations have made progress in addressing capability gaps for CBRN defence, they must further enhance the ability to “Prevent” by continuously investing necessary national resources allowing them to meet the NATO levels of ambition.

68. Protect: NATO Allies will protect their populations, territories and forces against any CBRN threats and WMD by enhancing and integrating all of their national CBRN defence capabilities. The pursuit of the whole-government approach will ensure a robust and efficient CBRN defence for the Alliance.

69. Allied forces must be able to operate, fight and prevail in a CBRN environment. Therefore, NATO Allies must strengthen their forces in all services with integrated basic, enhanced and specialised CBRN defence capabilities. Moreover, NATO supports these national capabilities, including through the Combined Joint CBRN Defence Task Force (CJ-CBRND-TF) and the technical and scientific support provided by the NATO CBRN Reachback Element (CBRN RBE).

70. Recover: CBRN defence capabilities enable NATO Allies to recover from the consequences of WMD use or a CBRN incident. Therefore, Allied forces will uphold a continuity of operations and support the recovery of affected populations, territories and forces.

71. Military, civilian and medical CBRN defence and response capabilities are essential elements for the recovery from any WMD or CBRN material use. Therefore, CBRN defence and response, as well as medical personnel must be educated, commonly trained and fully prepared to recognise and provide efficient joint support to recover from the consequences of WMD use or a CBRN incident.

CBRN Defence Enabling Components

72. The framework within which capabilities associated with the CBRN defence LOE are identified and developed are the CBRN defence enabling components. The capabilities based on the CBRN defence enabling components actively contribute and support CBRND LOE to interrupt the CBRN incident chain from a conceptual point of view as early as possible. It is essential that NATO Allies are not only fully capable based on the following CBRN defence enabling components, but are also ready to respond to a CBRN incident in an appropriate timeframe.

73. Currently, CBRN defence is organized around five enabling components, the foundations of which are established based on CBRN defence policy, doctrine, capabilities, procedures, organizations, training and technological development.

74. Given the rapid developments in EDTs and the need to ensure all CBRN LOEs are addressed with relevant capabilities the framework of the CBRN Enabling Components needs to be flexible and the current architecture continuously reviewed and further developed to stay relevant.

Detection, Identification, Monitoring

75. The purpose of Detection, Identification, and Monitoring (DIM) is to collect and process CBRN related information. Essentially, DIM provides qualitative and quantitative analysis of CBRN substances with a significant level of identification. DIM is enhanced by network enabled detection and identification technologies.

76. DIM contributes to CBRN Knowledge Management (KM) through the CBRN layer of a common operational picture, which enables timely and appropriate actions after CBRN incident, including CBRN Warning and Reporting (W&R). DIM significantly enables CBRN forensics and Technical Exploitation (TE). Medical diagnosis and health surveillance may also contribute to this component, especially for biological incidents.

CBRN Knowledge Management

77. CBRN KM aims to collect and manage CBRN-related information from one or several sources, along with the dissemination of raw and/or analysed information. It provides situation awareness to decision-makers and their staff, thus contributing to information superiority and timely decision-making.

78. CBRN KM closely links with the intelligence cycle, gaining information from the CBRN Reachback, contributing to the Joint Intelligence Preparation of Operational Environment, enhancing planning and enabling execution of operation.

Physical Protection

79. Physical protection combines measures and equipment intended to enhance the survivability of personnel and materiel in a CBRN environment. Physical Protection should provide individual and collective protection, CBRN hardening, equipment and materiel protection as well as critical military infrastructure protection.

80. Physical Protection should also be considered for mission-critical elements through the entire chain of command, to maintain and achieve all military objectives established for the operation to be conducted in a CBRN environment, together with two-way support provided from and to civil authorities.

Hazard Management

81. Hazard Management (HM) is an enabling component for forces seeking to avoid contamination, recover personnel, regenerate equipment and restore infrastructure to maintain or re-establish operational tempo and effectiveness. HM combines preparatory and

responsive measures and should be an advanced, prepared and integral part of operational planning.

CBRN Medical Countermeasures and Casualty/Patient Care

82. CBRN Medical Countermeasures (MedCM) include, pharmaceuticals, biologics, and vaccines. They are categorised into pre-exposure or post-exposure prophylaxis (protection), pre-treatment (treatment enhancers), and immediate therapy (first aid), as well as medical therapy. Pre-exposure medical countermeasures rely on a trigger based on threat assessment. Post-exposure medical countermeasures depend on a detection, intelligence or medical trigger. MedCM must be issued to personnel under national guidelines but declared to Allies, to ensure effective medical interoperability and reduced risk of adverse drug interactions. Medical products that are produced against CBRN materials and clinically tested and certified should be notified to Allies.

83. CBRN casualty/patient care extends from point of exposure through to rehabilitation. This may include combined injury with trauma or environment exposures (heat and cold), specific medical capabilities, including MedCM and other treatments, casualty/patient hazard management (decontamination, isolation, quarantine), forward deployed and enhanced diagnostics and specialist medical evacuation. Health surveillance is also a key medical function that supports the detection and monitoring of a CBRN incident or disease outbreak.

CBRN Defence Enabling Components within Core Principle 1

84. Given the nature of the current security environment, the emphasis on Core Principle 1 should be for the integrated and enhanced CBRN defence enabling components which actively contribute and support CBRND LOE to interrupt the CBRN incident chain as early as possible.

85. In addition, CBRN defence enabling components mutually support each other. The CBRN environment and conditions will indicate the priority and the level of involvement, before, during and after a CBRN incident.

CBRN Defence Requirements

86. The development and/or revision of qualitative and quantitative requirements might be stipulated by policies or Lessons Identified (LI) / Lessons Learned (LL) from missions, supported, guided or requested by concepts and informed by doctrines, standards or technical progress in EDTs.

87. CBRN defence contributes to the survivability and protection of Allied forces. As a joint military function, CBRN defence capabilities have to meet new enduring challenges across all operational domains.

88. CBRN defence capabilities must be prepared to support simultaneous operations implementing CBRND LOE anywhere, at any time and against multiple potential actors.

89. Operational principles and procedures relating to CBRN defence must be harmonised in all forces taking into account the following levels of proficiency, so that they are prepared to be employed quickly, effectively, robustly and sustainably in multi-domain operations.

Basic CBRN Defence Capabilities

90. The basic level requires all personnel to have basic CBRN defence proficiency in order to be able to survive and continue with the mission pre-, during and post- CBRN incident.

91. The basic capability must ensure the survivability of personnel through individual protection equipment and immediate measures pre-, during and post- CBRN incident.

92. At the basic level, personnel are required to recognize, react to and report a CBRN incident as early as possible.

Enhanced CBRN Defence Capabilities

93. The enhanced level requires additional proficiency by selected, trained and equipped CBRN defence personnel to ensure each unit level can continue to conduct operations following the threat or use of CBRN material.

94. Time is an essential factor for the success of CBRN defence measures. Therefore, necessary CBRN defence tasks need to be carried out by appropriately selected, trained, and equipped personnel from all arms and branches.

95. The enhanced capability must ensure the continuation of conducting operations in a CBRN environment while maintaining physical protection measures.

Specialised CBRN Defence Capabilities

96. The specialised level requires the highest proficiency by CBRN defence personnel. With their equipment and training, these forces provide specialised CBRN defence capabilities.

97. The specialised capability has to assure the qualified accomplishment of CBRN defence missions and tasks by specialised CBRN defence units pre-, during and post-CBRN incident.

98. Specialised CBRN defence capabilities provide supplementary capabilities that have to be tailored to enable operational success in specific mission types, including countering WMD, and to support MDO in a CBRN environment. This includes access to other CBRN-related capabilities and disciplines, to support CBRN defence such as inter alia EOD, medical support and forensics.

Capability Development considerations

99. All lines of development are to provide the Alliance with the military capabilities necessary to counter WMD proliferation, to operate effectively, to fight and prevail in a CBRN environment and to enhance national, collective defence and resilience against CBRN threats of all types.

100. In order to support NATO's core tasks effectively and efficiently, Allies will engage in a continuous process of reforming, modernising and transforming their national CBRN defence capabilities and capacities. To adequately prepare, equip and train CBRN defence forces, Allies must further develop modern, interoperable, deployable and sustainable CBRN defence capabilities.

101. The Alliance supports the development of robust, mobile, automated, interoperable and efficient CBRN defence capabilities through its JCBRND-CDG. This concept also informs the NDPP to support national capability development and planning.

102. The risk of naturally occurring or accidental biological threats can, likewise, add to the complexity of the security environment. Consequently, Allies must develop sufficient capabilities and capacity to counter these challenges that might disrupt NATO societies and strain national civil and military response capacities across all domains.

103. Potential biological threats to Alliance populations, territories and forces must be identified before they lead to a disruptive outbreak, impacting operational effectiveness, epidemic and pandemic. Therefore, bio-detection and analysis must be strengthened with close collaboration between civilian and military medical services.

104. Above all, NATO Allies must be able to rely on the capability and availability of Allied CBRN defence forces. This must be ensured through the following lines of capability development:

a. Doctrine: The operational CBRN defence doctrines will be developed throughout the CBRN LOE. In order to strengthen CMI, NATO Allies should enhance cooperation to develop common doctrinal standards for civil and military CBRN assets. CBRN defence is a joint capability and an enabler to the protection of forces and populations.

b. Organization: NATO and the Allies must include CBRN defence capabilities within their organizations, especially CBRN defence specialists capable of conducting all required CBRN defence tasks. The capabilities have to be reflected in respective doctrines and the DDA Family of Plans. Allies will sustain sufficient civil-military CBRN response and defence capabilities. To strengthen the organizational CMI structure, Allies should develop common knowledge and understanding, practical response capabilities, as well as joint protocols and procedures.

c. Education and Training (E&T): E&T of all forces, medical staffs and specialised CBRN defence units is a national responsibility. NATO provides and coordinates an extensive portfolio of CBRN Defence education and training for NATO forces, participating Allied national forces and civilian personnel and authorised partners in accordance with the NATO Education, Training, Exercises and Evaluation Policy. E&T should be organized as an integrated part of every training activity in order to also promote and harmonize CBRN defence procedures within NATO and multinational forces at all levels.

(1) Operating in a CBRN environment creates unique physical and psychological stressors that can be overcome through awareness and

understanding the nature of the CBRN threat. Additionally, confidence and reliability on CBRN equipment must be continuously established through consistent and realistic training, such as live agent training.

(2) Robust exercising of CBRN defence tasks in a variety of complex scenarios is essential to be prepared to counter this threat and to operate in a CBRN environment. Joint training and exercises remain key enablers for enhancing interaction and cooperation to foster better CBRN preparedness amongst civilian and military CBRN personnel. Moreover, NATO accredited Centers of Excellence (COE), especially the JCBRN Defence COE in the Czech Repbulic, and NATO Education and Training Facilities make important contributions to Alliance CBRN defence.

d. Materiel: Allied CBRN defence forces must be provided with modern, robust CBRN equipment that adheres, where applicable, to NATO standards. Materiel development plans should be flexible and able to adapt to the new challenges of the security environment, as well as to leverage from LI/LL. Overall, gender and inclusivity needs to be considered and implemented to ensure force readiness. The provision of CBRN defence materiel for Allied forces is a national responsibility. In order to improve interoperability, Allies should be committed to harmonizing requirements and standardization goals and regulatory alignment.

e. Leadership Development: CBRN defence E&T of commanders and staff-officers ensure awareness and understanding of CBRN threats and risk, and therefore, contributes to an effective and efficient decision-making on CBRN prevention and response measures. CBRN defence E&T for leadership has to be regularly reviewed and updated towards current requirements. NATO, as well as national courses, should provide in depth knowledge and skills for the entire leadership.

f. Personnel: Mission requirements and adequate individual protection equipment in connection with basic CBRN defence E&T will allow Allied forces to continue operating and fighting in a CBRN environment. In addition, enhanced and specialised CBRN defence personnel are required to be highly educated and trained in CBRN defence, allowing them to provide appropriate support and assistance.

g. Facilities: CBRN defence E&T facilities should provide for goal-oriented E&T for all levels and certify specialised CBRN defence personnel.

h. Interoperability: Operational principles, procedures and materiel development relating to CBRN defence must be harmonised and regularly updated, enabling Allied forces to be employed quickly, effectively, robustly and sustainably in joint, combined and MDO. The common standards and force integration efforts ensure interoperability among Allies and Partners.

Core Principle and Commitment 2 – Improved Resilience against CBRN Threats

105. As stated in the Strengthened Resilience Commitment, resilience is a national responsibility and a collective commitment. Alliance resilience is the individual and collective

capacity for Allies to prepare for, resist, respond to and quickly recover from strategic shocks and disruptions, and to ensure the continuity of the Alliance's activities. NATO's seven Baseline Requirements for national resilience provide a comprehensive framework to support the continuity of critical functions in society, and at the same time, the effective enablement of our armed forces, as well as of NATO's core tasks. The Baseline Requirements include measures of CBRN preparedness.

106. An attack with CBRN materials or a large-scale CBRN incident could have devastating consequences for our societies and the critical infrastructure upon which they depend. This could have potential impacts on the baseline areas and affect Allied societies to support military operations. Even a comparatively limited employment of CBRN substances may require significant attention from civil authorities, demand considerable resources to mitigate impacts and complicate the Alliance's readiness and responsiveness.

107. Allies will enhance the resilience of Allied nations and societies against the full spectrum of CBRN threats, not permitting both state and non-state actors to compromise Allied commitment to national resilience. While noting that resilience against CBRN threats remains a national responsibility, the Policy further encourages cooperation between Allies to reduce vulnerabilities and enhance international norms. Allies also agreed that governments and first responders should possess the full range of capabilities required to predict and respond effectively to a CBRN incident on their territory. Timely, accurate and evaluated intelligence is critical to generate a shared understanding among Allies' first responders.

Civil preparedness considerations within CBRN Defence Lines of Effort

108. Prevent: National resilience against CBRN threats contributes to NATO's security at all points of the spectrum from peacetime vigilance through crisis to conflict. Coordination, arrangements and planning, specifically pre-crisis, at a national level is necessary to support a whole-of-government approach to CBRN preparedness and prevention.

109. NATO military forces could, as appropriate and upon request, support civilian authorities in bolstering national capabilities.

110. Protect: One of the three core functions of NATO Civil Preparedness is to provide essential services to the population. This includes assistance and support to national authorities in protecting Alliance populations and critical infrastructure against the consequences of major disasters and/or CBRN incidents.

111. The principal aims of NATO Civil Preparedness addressing CBRN issues are to:

a. Exchange information with national civil authorities of the hazards posed by CBRN substances in order to support national planning and preparedness decisions, including prioritisation of resource allocations.

b. Support effective cooperation between Allies' civilian military authorities within NATO itself and as appropriate with international organisations.

c. Provide guidance, as appropriate, to national authorities on how to deal with the consequences of a CBRN incident (e.g., E&T, exercising, public information, societal resilience, communications capability).

d. Provide guidance, as appropriate, to Allied national civil authorities on alerting the public, emergency responders and critical infrastructure operators of CBRN threats and potential response actions.

e. Identify how NATO capabilities and the coordinated national capabilities of individual Allies can support stricken Allies if requested.

112. To support civilian authorities, NATO's military forces require effective, secure civilian services and infrastructure, particularly in transportation, telecommunications, information technology services, energy, food and water supplies, law enforcement and in the medical field.

113. It is the responsibility of the National authorities to prepare legislation regarding crisis management principles of CBRN and Toxic Industrial Materials (TIM) incidents (principles of crisis response in environments with CBRN and TIM pollution resulting from activities by state actors or non-state actors and terrorists, natural disasters and/or accidents). Cooperation between civil and military institutions should be increased with continuous E&T activities on the issues of response to TIM incidents.

114. Recover: NATO Allies must be fully prepared to recover from the impact of a CBRN incident affecting their populations, territories and forces, whatever its origins, and to assist their partners, if necessary.

115. Once a CBRN incident occurs, national authorities have the primary responsibility for leading the recovery and for ensuring effective civil-military coordination at the national level. NATO supports such efforts, as appropriate, through deployable assets, E&T, exercises and policy guidance.

Civil-Military Interaction

116. Military CBRN defence capabilities and civil preparedness support and reinforce each other, but they are separate and distinct and neither can replace the other. Military CBRN readiness and responsiveness and national resilience demands effective, two-way planned, exercised and resourced civil-military interaction.

117. CMI encompasses activities between NATO military bodies and non-military actors to foster mutual understanding that enhances effectiveness and efficiency in crisis management and conflict prevention and resolution. In on-going operations, civil authorities and Alliance military forces should work together to provide disruption, interdiction and response operations.

118. The COVID-19 pandemic reinforced the importance of cooperation between civilian and military authorities in a crisis and the potential contributing role of CBRN defence capabilities. It highlighted that Allied military forces can be called upon to provide significant support to national civil authorities as a key instrument of national resilience, in cooperation

with other relevant actors. Conversely, effective civilian support to military forces is indispensable to accomplishing military objectives.

119. Military CBRN defence capabilities in support of national civilian response plans differ across nations and reflect distinct national plans, priorities, approaches and even national legislation. In the past, military units and activities often constituted a critical component of successful response operations. Military support to civil authorities should be integrated into existing emergency operations plans, procedures, training and exercises whenever possible.

120. When a stricken nation affected by WMD attack or use of CBRN material needs international assistance, it can reach out to a number of international organizations, including the Euro-Atlantic Disaster Response Coordination Centre (EADRCC). This centre is NATO's principal civil emergency response mechanism in the Euro-Atlantic area and is active all year round, operational on a 24/7 basis, involving all NATO Allies and partner countries. The Centre functions as a clearing-house system for coordinating both requests for and offers of assistance, mainly in case of natural and man-made disasters.

121. Civil emergency managers and first responders at the local, regional and national levels should understand roles and authorities pertaining to military support of civil authorities and should build relationships with military authorities within their communities prior to such CBRN incidents occurring. Establishing and maintaining effective and timely communication between civilian and military authorities to provide coordinated response and recovery from such a CBRN incident will be fundamental.

122. Conversely, military commanders should also develop an awareness of civilian capabilities to support military operations where appropriate.

123. Military authorities should evaluate requests received from civilian authorities for:

a. Readiness (impact on the military's ability to support deterrence and perform warfighting).

b. Cost (including the source of funding).

c. Legality (compliance with relevant laws, plans and procedures).

124. Many of these issues can be jointly planned in advance with pre-scripted mission assignments to facilitate a more rapid coordination process. Based on the planning scenarios and considering the actual deployment time of the military forces, these assignments may specify the type of assistance that is required, a statement of work, a project cost and source of funding.

125. Success is based on civil and military authorities building and maintaining relationships and developing capabilities to prevent, protect against, respond to and recover from major incidents. This also includes resetting respective CBRN capabilities to be able to respond to subsequent attacks.

126. To further promote enhanced cooperation between civil and military authorities on CBRN, in 2019, the North Atlantic Council adopted "Non-Binding Guidelines for Enhanced Civil-Military Cooperation to Deal with the Consequences of Large-Scale CBRN Events".

These guidelines identify the following guiding principles for successful civil-military interaction:

a. Mutual understanding of the military and civilian plans and procedures as a baseline for cooperation, thus respecting each other's autonomy in decision-making.

b. Mutual understanding of different roles, responsibilities, enabling components and legal limitations of civil and military authorities.

c. Cooperation between civil and military authorities should be based on and supported by national legislation, policy, strategy and joint action/implementation plans.

d. Military support must be requested by civilian authorities according to national legislation. The military should always remain in support of civil authorities.

e. Cooperation in peacetime, during preparedness phases, builds the foundation for effective civil-military cooperation.

f. Shared stockpile for equipment, medical countermeasures and personal protective equipment provides cost-effective resilience for both domestic response and out of area missions.

g. Planning scenarios should be based on managing a no-notice CBRN incident in a peacetime environment, without prepositioned civilian or military resources.

h. Collaborative organisational structures and personnel exchanges provide the foundation of effective cooperation at all levels.

i. Establishing and maintaining continuous and effective communication with correspondent civil and military counterparts at local, regional, national, and international levels.

j. Cooperation in development programmes, project design and project implementation can produce better outcomes.

k. Cooperation on the monitoring and evaluation of plans, programmes, and activities facilitates better understanding of results.

l. An emphasis on learning and adapting enables more effective cooperation when integrated throughout the defence cycle.

127. In addition, in 2021, the Council approved "Non-Binding Guidelines on Civil-Military Medical Cooperation in Response to CBRN Mass Casualty Incidents". The principal recommendation of these guidelines is that nations develop mechanisms for an integrated approach, including civil military cooperation, across the health sectors, to support the planning, preparedness, training, capacity building and burden sharing and medical response and recovery to a CBRN incident of any scale, including mass casualty.

128. Allied militaries and the NCS have CBRN defence expertise, from the strategic to the operational and tactical levels, which could benefit their civilian counterparts' expertise. Under most circumstances, Allies' national response to a CBRN incident would be led by national civil authorities, with national military support tasked as required and consistent with

Allied national policies, legislation and normal practice. As NATO's capabilities are first and foremost military, it could be beneficial for Allies to define, at a national level, how to integrate a NATO request for support into a national civilian response.

129. Within CMI, all relevant legal and technical aspects related to a different mandate, responsibilities and a decision-making process of both civil and military entities have to be considered when CMI is to be established and implemented through a multi-layer approach.

130. Examples on this include but are not limited to:

a. Transport (e.g., rotary wing lift, heavy ground transportation for first responders, emergency route clearance including quickly clearing roads or establishing temporary bridges).

b. Medical (e.g., access to MedCM, CBRN first aid provision, extraction units, patient evacuation, medical personnel, field hospitals, specialist medical advice).

c. On-site response (e.g., hazardous material sampling, handling, analysis, and transportation of contaminated CBRN material; decontamination; containment and population protection measures; waste management, search & rescue and Explosive Ordnance Disposal (EOD), units able to cross or to reach heavily contaminated areas, even by gamma radiation, using special vehicles, mortuary services, forensic support, victim identification).

d. Energy (e.g., fuel distribution points and generators).

e. Communications support.

f. Modelling and simulation.

g. Aerial imagery.

131. The cooperation between military and civil authorities shall not be confused with Civil-Military Cooperation (CIMIC) which is a military joint function that integrates the understanding of the civil factors of the operating environment and that enables facilitates and conducts CMI to support the accomplishment of missions and military strategic objectives in peacetime, crisis and conflict.

PART V - CROSSCUTTING FUNCTIONS

132. Crosscutting functions are disciplines that generally converge with CBRN defence across all CBRND LOE. Interlinked with CBRN defence, they contribute to strengthening the deterrence and defence posture of the Alliance.

133. They also support NATO to fulfil its two CBRN defence core principles and commitments.

134. Moreover, these crosscutting functions should be regarded as complementary to the strategic enablers defined in NATO's CBRN Defence Policy. Strategic enablers facilitate NATO's efforts to defend against CBRN threats and WMD whereas crosscutting functions are an integral part of the CBRND LOE.

Joint Functions

135. Shared situational awareness, intelligence and information-sharing are critical enablers for all aspects of NATO's CBRN defence directly supporting decision-making, informing risk management and facilitating improvements to the Alliance's operational capabilities through exercises, procurement and other functions.

136. NATO's CBRN Reachback provides an on-demand source of authoritative technical analysis and expert guidance that facilitates efforts to strengthen deterrence and defence, support operations, conduct exercises and respond to CBRN incidents through a dedicated network.

Medical Support

137. Medical support is a strategic enabler of NATO's CBRN defence. Its crosscutting capabilities enable the Alliance to fulfil the full range of its commitments and facilitates NATO's efforts to defend against CBRN threats and WMD, as well as other operational hazards, including conventional trauma, explosives, environmental exposures and endemic disease. This is consistent with an "all-hazards approach" and is agnostic to cause, whether deliberate, accidental, natural or unknown.

138. The medical system may be the first recognition of a CBRN incident by either observing symptoms and signs, imaging or laboratory diagnostics or pattern recognition, including health surveillance. Medical care is the ultimate risk mitigation for CBRN defence especially on low threat operations in the absence of other protective measures. CBRN (MedCM) may enable pre-exposure protection, post-exposure mitigation and agent-specific treatment in addition to conventional medical management. Medical research will also be required to develop new MedCMs and diagnostics capabilities in response to an emerging threat, as well as knowledge management and information sharing, including medical advice, epidemiology, health surveillance and strategic communications.

139. The five functions of CBRN medical support are:

a. The provision of CBRN medical advice.

b. The contribution to CBRN defensive operations including MedCM.

c. The CBRN protection of medical treatment facilities, personnel, patients and medical evacuation platforms.

d. The provision of CBRN casualty/patient care including the management of any casualty in a CBRN environment, from point of exposure to rehabilitation, and the management of an unusual patient or unknown disease.

e. The planning, preparation and provision of an operational biological response.

140. Core capabilities are deployed on most medical missions, enhanced capabilities are deployed due to an increased threat or in response to an incident and emerging capabilities are those developed in response to an emerging threat or operational requirement. Surge capacity may also be required either in response to the numbers or types of affected, including mass casualty situations, or in response to the impact on the mission or operational effectiveness.

141. Key interactions include medical information sharing MedCM deployment and use, operational bio-surveillance, CBRN medical recognition and CBRN casualty care by non-medical and CBRN patient care by medical personnel, including decontamination.

142. CBRN medical support, as part of a wider resilience contribution, will rely on civil-military interactions. This may be civilian support to the continuing care of military patients, medical support or advice to civilian authorities during a CBRN incident, including mass casualty situations. Both civilian and military healthcare system will be reliant on operational and strategic stockpiles of MedCM, personal protective equipment (PPE) and other medical equipment.

Climate Change and Environmental Protection

143. Changes in operating conditions due to climate change will affect the types of CBRN challenges that NATO forces face and the capabilities required to overcome them. Consistent with the CBRN Defence Policy, the Alliance will incorporate climate change considerations into its work, to enhance CBRN defence capabilities and resilience of the Nations.

144. Allies will increase awareness of potential impacts of climate change on their CBRN security environment, including how changing environmental conditions may alter the physical properties and behaviour of CBRN material, and/or the possible emergence and spread of infectious disease. Allies will take appropriate steps to adapt to these impacts.

145. NATO will ensure that CBRN defence capabilities, including individual and collective protection, chemical and biological detection and identification and medical countermeasures, remain effective in operational context affected by climate change. This may require, inter-alia, accounting for extremes of temperature, humidity and smoke, as well as the ability to operate in environments affected by intensifying natural disasters.

146. Research, design, procurement and life cycle of CBRN capability development need to consider the new conditions created by climate change. Interoperability should also be a priority as Allies adopt new technologies and approaches. Exploitation of these innovative

technologies should be considered while planning and developing CBRN defence capabilities.

147. Climate change alters NATO's operating environments, with potential negative impacts on multiple aspects of CBRN defence. Specifically, climate change can increase water insecurity and desertification concerns. These effects might generate consequences for CBRN defence planning in military operations.

148. CBRN related education, training, exercises and evaluation (ETEE) should incorporate and reflect the climate effects noted above, including changes in the threat environment and the adaptation of specific CBRN defence capabilities. Consequently, Allied forces adequately trained and equipped will be able to minimize or negate any effects associated with Climate change.

149. In order to protect forces and joint operational environment, Allies have to take into consideration hazardous effects of not only CBRN incidents or WMD attacks, but also of implementing countermeasures and procedures by using various chemical compounds and/or conducting waste management.

Gender and Inclusivity Considerations

150. In line with the NATO / Euro-Atlantic Partnership Council Women, Peace and Security Policy and Action Plan, NATO will ensure that gender perspectives are appropriately considered within CBRN defence.

151. Gender Perspective is defined as the ability to detect if and when men, women, boys and girls are being affected differently by a particular situation due to their gender. By integrating a gender perspective and inclusivity into CBRN Preparedness and Defence, NATO can broaden its understanding of CBRN-related risks and impacts, which will improve the effectiveness of preparatory measures, aid recovery and ultimately increase societal resilience.

152. All training and exercising should factor gender into planning assumptions. Furthermore, all planning and measures should consider gender-specific risks related to gender-specific exposure to CBRN weapons and incidents. Undoubtedly, provisions of CBRN-related health care and equipment for military personnel need to integrate gender-specific considerations (e.g. data for biomedical and health-related research, studies and treatment). Protective gear must be adapted for the needs and fits of different genders. A similar understanding is required for the provision of CBRN-specific assistance to civilians.

Explosive Ordnance Disposal (EOD) / Counter Improvised Explosive Devices (C-IED)

153. CBRN explosive ordnance disposal (EOD) is perceived as a challenge for CBRN defence and its countermeasures. The combination of CBRN and explosive threats requires an increased focus on preparation of the force, including CBRN defence E&T.

154. The cooperation between the disciplines of CBRN defence and CBRN EOD needs to be further enhanced and developed. Thus, new standards and principles for an effective cooperation between these two disciplines are essential. E&T requirements for CBRN EOD

have to be reviewed and harmonized. Any discrepancies in terminology and standardisation require timely alignment and harmonization.

155. The response to a CBRN EOD incident is based on the interoperability of appropriate CBRN defence and EOD capabilities.

156. The preparedness for the response to CBRN EOD incidents requires interdisciplinary training based on complex scenarios with CBRN EOD injects during military E&T.

157. The CBRN EOD mission objective is not only to render safe the CBRN EOD, seal any leaks and prepare the explosive ordnance for safe transport and disposal, but it may also (and in many situations definitely will) include forensic sampling, identification of the CBRN substances, weapon intelligence assessment and collection of collected exploitable material (CEM), including as evidence. The CBRN EOD must also consider potential impacts of C-IED attack networks as proliferation networks or actors employing CBRN substances and coordinate with C-IED collective efforts to defeat an improvised explosive device system by attacking networks, defeating devices and preparing a force.

Technical Exploitation / CBRN Forensics / Attribution

158. Close collaboration with technical exploitation (TE) as a unique and valuable source of information, will be required, to gather CEM such as narcotics, chemicals and precursors, explosives, CBRN compounds or other CBRN-contaminated CEM and extract information of operational, intelligence or judicial value. Because TE is part of Joint Intelligence, Surveillance and Reconnaissance, it provides a valuable conduit with the intelligence cycle.

159. To offer relevant information and evidence to political, military and civilian authorities, an appropriate degree of evidence collection, preservation and forensic analysis is required by CBRN forces. This will necessitate the expansion of TE capabilities within CBRN defence by specifying new capability requirements for CBRN mobile and fixed laboratories, sampling teams and Multirole Exploitation and Reconnaissance Teams.

160. Forensics serves the systematic investigation of WMD attacks and CBRN incidents and is an indispensable basis for securing evidence for prosecution. Based on this, the attribution of such acts to an alleged perpetrator takes place after the appropriate evidence has been provided. This process is fundamentally in the hands of the stricken nation, which is responsible for maintaining suitable capabilities.

161. In a supranational context, the implementation bodies of the relevant treaties can support the attribution process, as they have the appropriate capabilities such as expert pools, fact finding teams, etc. NATO can only play a subordinate, supporting role in this context.

162. Credible attribution, supported by an understanding of the information environment, is also important to the strategic communications response to any CBRN incident.

Emerging Disruptive Technology

163. The NATO 2022 Strategic Concept defines the key challenges facing the Alliance and outlines how NATO will address them, reflects this changing context. It affirms that EDTs

bring both opportunities and risks, and that they are altering the nature and character of conflict, acquiring greater strategic importance and becoming key arenas of global competition. As a result, Allies agreed to promote innovation and increase investments in EDTs to retain NATO's interoperability and military edge. Allies will work together to adopt and integrate new technologies, cooperate with the private sector, protect their innovation ecosystems, shape standards and cmmit to principles of responsible use that reflect the Alliance's democratic values and human rights.

164. EDTs are increasingly touching all aspects of life from electronics, to everyday activities such as grocery shopping and banking. These technologies are also having a profound impact on security. Innovative technologies are providing new opportunities for NATO militaries, helping them become more effective, resilient, cost-efficient and sustainable to respond to a WMD attack or a CBRN incident.

165. Technologies, such as autonomous systems, quantum technologies and artificial intelligence (AI), offer new opportunities for how NATO will operate. Those EDTs also present risks for NATO and Allies and have a potential to dismantle CBRN defence or affect current thresholds of procedures. The convergence of biotechnology and AI is an example of EDT synergism of both to support research and development (R&D) and future capability development, but also as a future threat.

Strategic Communication

166. Strategic Communication (StratCom) is an essential enabler of NATO's response to CBRN threats. It is critical to building awareness and support, reinforcing deterrence, enabling recovery and reassuring Allied publics. NATO will continue to employ coherent and calibrated StratCom to convey that NATO and Allies are taking all appropriate steps to prevent WMD proliferation and protect our populations, territories and forces against CBRN threats.

167. StratCom supports efforts to address hostile information activities which increasingly aim to undermine the Alliance. Addressing hostile information activities, including propaganda and disinformation, is an integral element of CBRN defence and incident response.

168. Effective and credible StratCom as a part of NATO's response to CBRN threats also provides an effect to help to deter potential adversaries from undermining the Alliance's collective security.

169. In order to maintain Alliance credibility and cohesion, NATO will continue to execute deliberate and proactive StratCom activities to explain and ensure support for NATO's CBRN defence and counter-proliferation activities and mitigate the effects of hostile information activities, including disinformation and propaganda.

PART VI – CONCLUSIONS

170. The requirements and guiding principles for CBRN defence must be addressed in order to enable NATO to minimize the risks and challenges for Allied forces operating and fighting in a CBRN environment. Consequently, specific measures to support actions aimed at preventing or deterring a WMD attack and breaking the CBRN incident chain as early as possible will enable Allied forces to maintain freedom of movement while encountering CBRN risks and threats in such an environment.

171. The changing security environment requires regular policy, concept and doctrine reviews, as well as the willingness of all authorities to develop and maintain capabilities to meet new challenges.

172. Military CBRN defence capabilities and civil preparedness support and reinforce each other, but they are separate and distinct; neither can replace the other. Military CBRN readiness and national resilience demands effective, mutually planned, exercised and resourced civil-military cooperation contributing to efficient CMI.

173. The development, transformation and modernization of CBRN defence capabilities among the Allies and appropriate NATO bodies and entities is essential for NATO's CBRN defence integrated approach. The necessary capabilities will include, but are not limited to, protective equipment and medical countermeasures, interoperable knowledge management systems, advanced detection and identification systems, recovery systems.

174. The investment into the development of CBRN defence capabilities is the fundamental key element to ensure their appropriate enhancement, transformation and modernisation.

175. NATO establishes the framework upon which the Alliance will understand, plan, posture, exercise, train, equip and assess its capabilities, in order to deter and counter WMD proliferation and to ensure that it can defend the Alliance against CBRN threats from peacetime through crises to conflict.

PART VII - IMPLEMENTATION AND WAY AHEAD

176. This concept will require further implementation steps and actions, such as the revision of existing and the development of new operating and functional concepts as well as doctrinal publications, a review and adaptation of current CBRN defence tasks, capability and training requirements, and the development of new enhanced and integrated CBRN defence capabilities.

177. The established processes for the development of CBRN defence capabilities have to be used in order to meet NATO requirements underpinned by relevant technologies and available innovations in the area of CBRN defence and civil preparedness.