NATO STANDARD

AEP-4834, VOLUME I

NATO TEST AND EVALUATION OPERATING PROCEDURES (NTOP) FOR CHEMICAL AND BIOLOGICAL DETECTION, IDENTIFICATION AND MONITORING EQUIPMENT

GENERAL INFORMATION

Edition A, Version 1
DECEMBER 2020

NORTH ATLANTIC TREATY ORGANIZATION

ALLIED ENGINEERING PUBLICATION

Published by the
NATO STANDARDIZATION OFFICE (NSO)

INTENTIONALLY BLANK

NORTH ATLANTIC TREATY ORGANIZATION (NATO)

NATO STANDARDIZATION OFFICE (NSO)

NATO LETTER OF PROMULGATION

4 December 2020

1. THE ENCLOSED ALLIED ENGINEERING PUBLICATION AEP-4834, VOLUME I, Edition A, version 1, NATO TEST OPERATING PROCEDURES (NTOP) FOR CHEMICAL AND BIOLOGICAL DETECTION, IDENTIFICATION AND MONITORING EQUIPMENT - GENERAL INFORMATION, which has been approved by the nations in the NATO ARMY ARMAMENTS GROUP (NAAG), is promulgated herewith. The recommendation of nations to use this publication is recorded in STANREC 4834.

2. AEP-4834, Volume I, Edition A, version 1, is effective upon receipt.

3. This NATO standardization document is issued by NATO. In case of reproduction, NATO is to be acknowledged. NATO does not charge any fee for its standardization documents at any stage, which are not intended to be sold. They can be retrieved from the NATO Standardization Document Database (https://nso.nato.int/nso/) or through your national standardization authorities.

4. This publication shall be handled in accordance with C-M(2002)60.

Zoltán GULYÁS
Brigadier General, HUNAF
Director, NATO Standardization Office

INTENTIONALLY BLANK

RESERVED FOR NATIONAL LETTER OF PROMULGATION

INTENTIONALLY BLANK

RECORD OF RESERVATIONS

CHAPTER	RECORD OF RESERVATION BY NATIONS
Note: The reservations listed on this page include only those that were recorded at time of promulgation and may not be complete. Refer to the NATO Standardization Document Database for the complete list of existing reservations.	

INTENTIONALLY BLANK

RECORD OF SPECIFIC RESERVATIONS

[nation]	[detail of reservation]
Note: The reservations listed on this page include only those that were recorded at time of promulgation and may not be complete. Refer to the NATO Standardization Document Database for the complete list of existing reservations.	

INTENTIONALLY BLANK

TABLE OF CONTENTS

INTENTIONALLY BLANK

1 Introduction

This document is the first volume (Volume I) of the NATO Test and evaluation Operating Procedures (NTOP). These documents are the foundation of a common test and evaluation (T&E) procedure for chemical or biological (CB) detection, identification or monitoring (DIM) equipment, as approved by the NATO NAAG Detection, Identification and Monitoring Panel (DIMP) chartered under the NAAG JCBRND-CDG. The aims of the DIMP are to identify opportunities for sharing information and T&E data in order to reduce unnecessary duplication of efforts.

Nota bene: for the first edition, radiological (R) substances are not taken into account (see document AEP-75 dedicated on "Capability and systems requirements for nuclear and radiological detection, identification and monitoring equipment").

1.1 Background

Despite armament control agreements and initiatives, some actors continue developing field chemical, biological, radiological and nuclear (CBRN) weapons. This trend is more pronounced in areas of chronic political instability where NATO may be called upon to mount operations. Additionally, there have been recurring instances of terrorist and other *ad hoc* groupings that embrace CBRN threats as a powerful means of prosecuting their interests. Scientific advances, leading to the development of new and more potent CB agents and their means of delivery are reinforcing these processes, aided by the increasingly free migration of information and expertise around the world. At the same time, the continuing process of global industrialization opens up the wider possibilities of accidental release or deliberate misuse of toxic industrial materials (TIM).

DIM is one of the five enabling components of CBRN defence with physical protection panel (PPP), hazard management panel (HMP), knowledge management panel (KMP), training and exercise panel (TEP) and doctrine and terminology panel (DTP). It enables units to take timely and appropriate actions following CBRN attacks and TIM release (CBRN incidents) whilst also warning other units at risk. DIM is needed to rapidly recognize CBRN incidents, characterize, analyse and determine the hazards involved, delineate areas of contamination, and monitor changes over time.

The need for increased harmonization and standardization of concepts and procedures used for T&E of CB DIM equipment is highlighted for several reasons: on-going procurement programs for CB DIM capabilities (point and stand-off sensors; and networks) as well as the expressed intention to launch such programs in several Alliance members, in combination with the current lack of agreed performance standards and T&E procedures.

Conceptual and procedural harmonization, and ultimately standardization (as/if warranted), could facilitate Alliance-wide implementation of reliable and resource-effective "best practices" regarding T&E of CB DIM equipment. Harmonization and standardization may thereby contribute to speed up and facilitate the development, qualification and fielding of reliable and interoperable capabilities that will be able to defend against CB threats that may face the Alliance on today's as well as tomorrow's battlefield. Alliance-wide harmonization and standardization of T&E processes for CB DIM equipment may be considered as a crucial first step towards enabling reliable exchange and interpretation of T&E results across the Alliance. It may also allow NATO organizations and Alliance member states to compare different capabilities and T&E results from different T&E programs against each other on equal terms.

1.2 Purpose

The main goal of the NTOP documents is to provide the defence and security community (governments, research laboratories and industries) guidance for T&E. This conceptual and procedural harmonization and standardization will provide the community with detailed, substantial and coherent data that could enable the comparison of different CB DIM equipment tested at different locations and/or times.

Development of CB DIM equipment for either “detect-to-warn” or “detect-to-treat” applications demands performance evaluation against CB threats. To achieve that goal, development of test concepts, facilities, fixtures and instrumentation are required to provide a framework for accurate and reliable CB DIM equipment assessments. The NTOP documents aim to provide guidance on appropriate facilities, instrumentation, and methods for accurate and scientifically defensible reference data where the collected information can be evaluated and compared to data collected elsewhere according to the same NTOP. By defining these requirements, the T&E community increases confidence in CB DIM equipment.

The purpose of NTOP documents is to describe the basic framework for T&E of CB DIM sensors and CB sensors networks. This framework should:

- provide a common foundation for T&E procedures and methods;
- provide common ground for data sharing and interpretation;
- allow consistent evaluation of data, equipment and devices;
- provide a quality assurance framework;
- offer guidance for governments, research laboratories, industries and other users on necessary elements of testing.

2 Document description

2.1 Scope

The NTOP documents take into account the following scopes:

- chemical point detectors (CPD), see Annex A;
- biological point detectors (BPD), see Annex B;
- chemical stand-off detectors (CSoD), see Annex C;
- biological stand-off detectors (BSoD), see Annex D;
- CB sensor networks (SN), see Annex E.

2.2 NTOP documents architecture

The entire NTOP document consists of two main volumes (entitled I & II), with a 3rd optional volume (III):

- volume I – General Information and NTOP scope;
- volume II – Common (harmonized/standardized) T&E framework, including recommended minimum requirements and best practices for T&E operations;
- volume III – Countries Specific Methods (as/if warranted).

This document (Volume I) provides a general introduction and an overview of T&E concepts and defines the scope of the NTOP effort.
Volumes II are important documents for the T&E community because it will describe minimum requirements and best practices. It is divided into five sub-volumes:

- volume II-A for CPD;
- volume II-B for BPD;
- volume II-C for CSoD;
- volume II-D for BSoD;
- volume II-E for SN.

Volume(s) III will be optional. Some nations or Alliance partners will be able to write them if they want to detail their own specific test procedures.

2.3 Application

The NTOP documents outline the general T&E concepts and procedures recommended for all Alliance's partners and focus on field and laboratory test operations as a baseline for data exchange or sharing.

Current test plans provide specific laboratory and field trial information, analysis methods, and test conditions based on the type of information required, evaluation needs, and decision(s) to be supported for individual test programs. The NTOP documents are intended as a reference for test plan development in order to maximize the value of individual T&E programs in an Alliance-wide context without burdening or compromising the success of those programs, through the establishment of a harmonized T&E framework. The NTOP documents should serve as a baseline and therefore applicable by all Alliance partners. However, most or all Alliance partners have their own national threat assessments as well as access to different types of test facilities and infrastructure. Therefore, the NTOP documents are focused on establishing and describing a set of minimum requirements and best practices regarding T&E of CB DIM equipment in order to provide a harmonized T&E framework to the community.

NTOP serve as a guide for test plan development. Moreover the NTOP documents may also help inform the broader community (*e.g.* users, stakeholders, materiel developers and industry of CB DIM equipment) about how test operations are planned and executed, test data is collected, and test results can be used to support decision-making regarding technology readiness levels (TRL) and equipment and/or capability development.

The procedures described in the NTOP documents are intentionally general in nature. Specific test procedures will be based on national test organizations and internal Standard Operating Procedures (SOP). They are often tailored/custom developed to support individual T&E programs, and should therefore be further delineated in the test plans. These SOP could be documented in the proposed Volume III.

2.4 Limitations

The NTOP documents do not describe the full range of tests or precise procedures that are required to perform a complete evaluation of the functional performance of CB DIM equipment.

The NTOP documents should therefore not be considered as an alternative to the use of detailed test plans. As such, the NTOP volumes are only intended as reference documents regarding minimum requirements and best practices. The specific test plan for a T&E process should be based on the specific test objectives, current data and evaluation needs, and type of decisions to be supported. As a minimum, they should also contain enough information about the concepts and procedures to define each trial, analysis method, and test conditions in sufficient details. This information will allow the T&E process to be unambiguously interpreted from a technical perspective and preferably be reproduced by others (at least in principle).

The NTOP documents may be subject to change. They should be updated if advances in technology facilitate the development of novel CB DIM equipment or alternatively new T&E capabilities (*e.g.* concepts, procedures, facilities, or instrumentation) that change the foundation and applicability of the proposed T&E framework.

Because some T&E processes require the use of warfare CB substances, country specific legislation will have to be taken into account. This aspect places a significant reliance on testing using CB simulants.

2.4.1 Scope of CPD

Concerning the form of the substance, the NTOP documents will focus on:

- gas and vapour;
- liquid and solid (bulk substance or contaminated surfaces);
- aerosols.

Because the test operations - including concepts, fixtures, procedures, and requirements - can be different according to the substance form, priorities are set for the first edition of Volume II (Priority for CPD: gas and vapour).

2.4.2 Scope of BPD

Concerning the form of the substance, the NTOP documents will focus on:

- aerosols;
- threats in matrices other than air, *e.g.* on surfaces, in liquids.

Because the test operations - including concepts, fixtures, procedures, and requirements - can be different according to the substance form, priorities are set for the first edition Volume II (Priority for BPD: aerosols).

2.4.3 Scopes of CSoD and BSoD

In general, the T&E strategy selected for stand-off testing will depend on different factors. These include the technology under test and the chosen application/scenario. The technologies can be divided into two broad classes:

- mid or long range stand-off systems that are intended for early warning of an impending gas or aerosol cloud threat ();
- short range stand-off systems that are primarily intended for surface contamination threats (the expression “short-range stand-off” used in this document is defined as a non-contact,

proximal optical method for CB threat detection). These persistent surface contamination threats are assumed not to pose a vapour hazard; therefore, they are not amenable to vapour detection methods.

There are three classes of scenarios:

- gas/vapour (chemical) cloud;
- aerosol (biological or chemical) cloud;
- surface contamination (biological or chemical).

Moreover, the stand-off sensors could be divided in two technology types, active or passive. Active stand-off sensor is defined as an optical technique that involves a light source to interrogate the scene, while passive stand-off sensor utilizes only the intrinsic light of the scene.

The stand-off technology in this document will use the rational when describing distance between the hazard and the detector, as described in Figure 1:

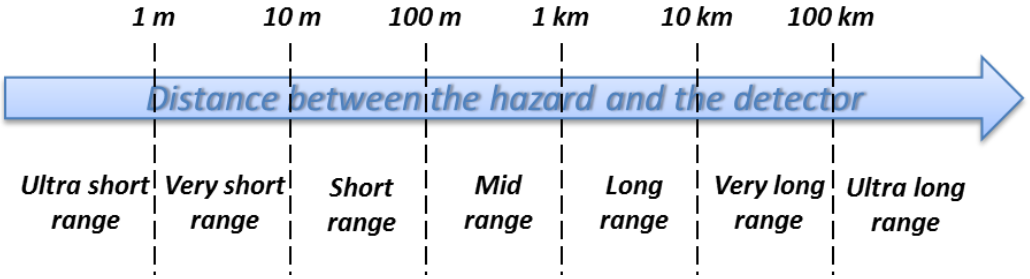

Figure 1: Description of distance between the hazard and the detector

Because the test operations, including concepts, fixtures, procedures, and requirements, can be different according to the substance form and the distance, priorities may be given for the Volume II first edition.

2.4.4 Scope of SN

The NTOP documents are limited to T&E of the CB DIM capabilities in a sensor network.

2.5 Cross-tests

Cross-tests (or inter-laboratory tests) between different nations are considered. The aim is to:

- validate the NTOP documents;
- verify that all the minimum parameters have been taken into account;
- verify the universal applicability of the NTOP documents;
- update NTOP documents by comparing results obtained from different nations.

To perform such cross-tests, nations will have to perform testing of similar equipment on which tests will be conducted and establish a test plan.

The cross-tests may be performed according to nationally developed test plans (based on national interpretation of the NTOP documents) as well as according to jointly developed test

plans. The former will assess the unambiguity, clarity and completeness of the guidance, minimum requirements and best practices put forward in the NTOP documents. The latter will assess variability/reliability of test data generated at different locations in the context of test operations executed according to the NTOP framework.

2.6 NTOP review Procedure

This NTOP will be reviewed to reflect the current facilities and methods. Formal reviews will occur periodically. Within the DIMP, operational and technical experts could initiate them in syndicates dedicated to NTOP. Unscheduled reviews may be done if significant changes have been made to facilities, methods and procedures. Any amendments will then be forwarded to the country representative for presentation at the subsequent DIMP meeting.

The method for NTOP edition and version changes is as follows:

- an edition is defined as a major change in the document that affects the procedure during testing. Examples include adding or removing a testing method, testing new material, or using new materials (*e.g.*, simulants). When an edition change has been made, the old document is considered obsolete and should be discarded. When a new edition is created, the version number resets at ‘1’;
- a version is defined as a minor change in the document that does not affect the overall procedure during testing. Examples include a clarification of statements, grammar or spelling corrections, adding tables, or incorporating pictorial descriptions.

For large changes, a reference to the old edition would be appropriate, along with the location of the changes. For a version change, only a description of the location of the change is required.

3 Testing Overview

The ideal strategy would be performing T&E with live CB warfare substances delivered in a threat-representative format under operational circumstances in relevant operational environments. This is, however, a utopic strategy for several reasons, including but not limited to health and safety issues, and even legal constraints on the use of CB warfare substances outside of specialized and licensed containment laboratory facilities.

The practical strategy chosen is usually a compromise consisting of a selection of test operations performed in various test facilities and environments.

Three different test approaches can be considered :

1. laboratory testing;
2. field testing;
3. operational testing.

In addition, some tools based on modelling and simulation could be used both at the early stage of design but also to complete the other T&E approaches.

Laboratory testing and field testing are the most important test approaches for the research, development and test and evaluation (RDT&E) community, which constitute the main subject

of the NTOP documents. Technical experts, supported by an operational team if warranted, can generally perform such testing.

Operational testing is performed to assess equipment performance under operational circumstances in relevant operational environments. It is designed to evaluate the effectiveness and suitability of the system with respect to its intended use. The testing is performed by the end-user (operators) or a dedicated operational test team.

All these approaches are performed with a relative association to the TRL of the CB DIM equipment under test (see Annex F). According to the TRL, the purpose of the T&E operations can be different, and only some test approaches may be relevant. Moreover, the test approaches can range from being fully integrated to being completely independent from each other. Not all test approaches must be realized in all situations.

At the early stage (design, proof of principle, *etc*.), some modelling and simulation tools can be used before laboratory, field and operational test data is generated. In the area of T&E, modelling and simulation tools can be used when T&E are too expansive, dangerous, time-consuming or too complex for instance. Modelling and simulation can also be based on the data sets obtained from both field and laboratory testing. It can include data-driven environmental background models, sensor/detector models, dispersion models, *etc*.

For T&E of CB DIM systems, three main classes of test materials can be used: live CB warfare substances, CB simulants and interferents.

The range of different test facilities and environments serve to complement each other in that they allow for different aspects of the performance of CB DIM equipment to be investigated at different levels of realism regarding threat, environment and operational circumstances.

An overview of each test approach is described below. More detailed information on test operations are provided in the NTOP volumes II.

3.1 Test Approach 1 – Laboratory Testing

Laboratory testing is performed to assess equipment performance in a controlled environment. They offer the possibility of controlling test parameters that may affect the T&E results. If test parameters cannot be controlled, they should at least be measured accurately. The controlled experimental conditions associated with laboratory testing results in a high level of experimental reproducibility. This reproducibility allows test processes to be repeated to generate test data that can be subjected to statistical treatment to increase the associated statistical confidence.

Laboratory testing can be divided into different sub-categories depending on the substance (B or C), the form of the substance (gas/vapor, liquid, solid, or aerosol) and the type of CB DIM systems (point or stand-off). Examples of sub-categories include gas/vapour/aerosol chamber testing, wind tunnel testing and surface contamination testing. More details are given in NTOP volumes II.

Laboratory test may offer the opportunity to conduct tests with both CB warfare substances and CB simulants in a controlled and safe environment. Laboratory T&E should preferably be performed using CB warfare substances and not CB simulants to evaluate properly the performance of CB DIM equipment in terms of sensitivity, probability of detection, response time and false alarm rate. However, comparative laboratory testing between CB warfare

substances and CB simulants can be used to establish warfare substance-to-simulant correlations that are needed to extrapolate test results from open air CB simulant-only testing (*e.g.* field testing).

In order to address detection probability and false alarm rates of the CB DIM equipment during laboratory testing, synthetic background testing can be performed by reproducing a mixture of interferents that are naturally present in operational environments.

3.2 Test Approach 2 – Field Testing

Field testing offers the possibility of performing T&E with a relatively high level of environmental and operational realism. Ideally, testing should be carried out under different environmental conditions that reflect military operational environments (desert, tropical, cold weather and urban area, *etc*.).

The control of key experimental parameters is limited, particularly the local meteorological and environmental conditions. It may be possible to take advantage of local weather trends and monitor key parameters (*e.g*. atmospheric conditions, background fluctuations, *etc*.). However, a large number of replicated tests will generally be needed to ensure sufficient statistical confidence. The difficulty with low experimental reproducibility in combination with high logistical burden and test complexity usually makes outdoor field testing relatively costly and resource demanding compared to laboratory testing.

Field testing should ideally be performed using live CB warfare substances to evaluate properly the performance of the CB DIM equipment in terms of sensitivity, detection probability, response time and false alarm rate.

However, due to health and safety issues and even legal constraints on the use of live CB warfare substances outside of specialized and licensed containment laboratory facilities, field testing is generally limited to CB simulants only.

Field background testing can be performed to address false alarm rate of CB DIM systems. Since no intentional substance generation is involved, open-air background testing may at least in principle be performed in any real world environment both with and without relevant ongoing operational activities. In this case, only false positive rates could then be addressed.

3.3 Test Approach 3 – Operational Testing

Operational testing can be performed on CB DIM equipment as soon as safety testing has been performed.

Therefore, operational testing should be conducted in representative military environments with military operators under different environmental conditions that reflect operational uses and CONOPS. The performance in real conditions of service operated by the end-user itself may differ from results obtained from laboratory and field testing. The operators may have different competencies, backgrounds and training courses may be necessary prior to conducting the operational testing.

Operational testing must endeavour to resemble real user situations as much as possible, and be integrated in the already established working routines/combat drills of the users. This will include several activities, for example:

- operation and maintenance of the device wearing combat equipment and/or personal protective equipment;
- shooting with both automatic rifle and submachine gun;
- audio and visual alarm tests;
- combat drill (*e.g.* crawling, slow and fast walking speed, *etc*.);
- patrol;
- fire movement;
- reorganization;
- decontamination.
- *etc*.

If possible, some of the tasks can be performed under exposure of appropriate simulants. Possible live CB warfare substance operational testing can be done by the participating national end-users in relation to CBRN warfare substance training exercises (*e.g.* Precise Response arranged annually in Canada).

Operational testing of prototypes is an early involvement of end-users in the development process, which can give valuable information and directions for further development. The end-users may, based on their operational expertise and experience, help direct the test procedures to ensure reliable and relevant test results. Operational testing as early as possible in the development cycle may improve the integration and compatibility of the CB DIM equipment for later operational use.

Operational testing may involve the use of live CB warfare substances or CB simulants to generate challenges in a similar fashion as for field testing.

Operational testing on prototypes first mass-produced or MOTS/GOTS/COTS/NOTS (see glossary for the definitions) equipment is usually conducted in order to confirm that the CB DIM equipment fulfils the military requirements in real conditions, and to verify the reliability of equipment. The goals can be to:

- define the rules and the limits of employment in the field;
- validate the maintenance and logistics system;
- verify the integration of the system in its broader logistics and operational environment.

3.4 Complementary tools for the previous test approaches – Modelling and Simulation

Modelling is creating a “model” to represent a system. A model may be the same as the original system or sometimes approximations make it deviates from the real system.

Simulation is a technique of studying and analysing the behaviour of a real world or an imaginary system by mimicking it by mean of computer script.

A simulation works on a mathematical model that describes the system. In a simulation, one or more variable of the model is changed. The resulted changes in other variables are then observed. Simulations can make possible users to predict the behaviour system.

T&E of CB DIM equipment (sensors and sensor network) can be conducted through simulations. Simulation comprises an artificial description of reality. It is the process that let T&E community conduct some tests based on models representative of the system. Behaviours and properties can be simulated under some given conditions. The end result includes both assessments and limitations for the models used to build up the artificial world. However, simulations can be in many cases the only option for T&E of technological solutions for a given task at a given place. For CB DIM equipment network, the choice of CB DIM equipment type, possible combinations of different CB DIM system types and placement of the CB DIM equipment are examples of questions that can be analysed through simulation. Repeatability of a simulation is a key strength.

Modelling and simulation of CB DIM equipment (sensors and related networks) can provide critical input during the hardware development phase, the design of CB DIM systems or related network and eventual testing of a developed or fielded system. Simulation can provide assistance in several different ways. It can allow the developer to compare the system under test with existing technology and provide theoretical level of performance. It can also provide the developer the ability to test numerous scenarios with several and defined input parameters. Important insight can be gained, for example, into the sensitivity of various parameters. This can be quite helpful in designing tests and allowing the tester to assess critical parameters while reducing the cost of the test. For field testing, this could mean the difference between being able to test or not, which could improve cost-saving, ensure resource-effectiveness.

Models can be static during the whole simulation run or dynamic with the possibility to influence and adjust parameters during the run with *e.g.* changes in temperature and wind or variation of source strength and position. Models can be calculated in real time during the run or be pre-calculated.

Simulation of a CB DIM equipment can be described in a chain model (Figure 2) which includes models for source, dispersion, CB DIM systems and communication (*e.g.* a network model).[1] There is a correlation between the included models and when it comes to data exchange between the models, they should have equivalent resolution. To be able to compare test results from different simulations, the models performance and input data must be well documented.

[1] FOI MEMO 5400 2015, Sensors and Sensor Networks – from a modeling point of view

Figure 2: Chain of sub models

T&E can also be performed by simulating a CB DIM system with data from previous test or artificial/simulated data, *e.g.* to test integration components and data distribution within the network.

The NTOP documents deal only with “sensor model”. The other models described in Figure 2 are out of the NTOP scope.

3.5 Test materials

As already described, the ideal strategy would involve live CB warfare substances delivered in a threat-representative format under operational circumstances in relevant operational environments.

The three main classes of test materials used for T&E of CB DIM equipment are:

- live CB warfare substances;
- CB simulants;
- interferents.

In addition to the identity of the test material, several other properties of the test material (*e.g.* production procedure, purity, wet/dry preparation, additives, *etc*.) as well as the delivery system (*e.g.* wet/dry delivery, generation mechanism, particle size distribution, amount of mechanical stress, *etc*.) can have a strong impact on the characteristics of the resulting challenge.

3.5.1 CB warfare substances

Chemical warfare substances or TICs can be in different forms (gas/vapour, liquid, solid, and aerosol as listed in D/100 triptych[2]/STANREC 4835[3]).

Biological threat substances are a diverse group of microbial pathogens and biological toxins (D/100 triptych[2]/STANREC 4835[3], or consolidated NATO B warfare substance list, if available), including Gram-positive bacterial spores (*e.g. Bacillus anthracis* spores), vegetative Gram-negative bacteria (*e.g. Yersinia pestis*), RNA viruses (*e.g.* Marburg virus) and DNA viruses (*e.g. Variola major*) and biological toxins (*e.g. botulinum* toxin).
Testing with B warfare substances is generally restricted to specialized and licensed (containment) laboratory facilities.

3.5.2 Simulants

3.5.2.1 Chemical simulants

The selection of suitable C simulants for C DIM systems testing exploits different physical phenomena and characteristics of the real C warfare substances. It is recognized that not only the physical and chemical (spectroscopic included) properties are important but also the form in which the simulant is delivered (*e.g.*, gas, liquid, solid or aerosols).

Simulant selection will depend on the C DIM equipment under test and the test objectives. The best selection of simulants will depend on the correlation between physical and/or chemical properties of the substance and simulant depending on the technique used by the DIM device. Simulant selection is also affected by several other considerations, including health safety and environmental regulations.

3.5.2.2 Biological simulants

Biological simulants are a diverse group of microbial organisms and biological proteins that are used as surrogates (simulants) for B warfare substances. Commonly, they have as many shared features with B warfare substances as possible, but without any or at least significantly reduced associated health hazard.

Selection of B simulants for T&E of B DIM equipment will generally depend on the B DIM detector or system under test, the practical use of simulants for test operations and the test objectives. Simulant selection is also affected by several other considerations, including health and safety and environmental regulations.

A sub-class of B simulants, often referred to as agent-like organisms (ALOs), are biological organisms or proteins that are more closely related to B warfare substances than conventional B simulants. But they can in certain cases still be used outside of specialized and licensed containment laboratory facilities since they have been attenuated (*e.g.* vaccine strains) or inactivated (*e.g.* by gamma radiation or chemical inactivation) to not represent a serious health hazard.

[2] CBWA early warning and detection triptych (NATO UNCLASSIFIED/Releasable to PfP). AC/225(JCGCBRN)D(2011)0003 (PFP).
[3] STANREC 4835 AEP-4835 NATO Capability and System Requirements for CB DIM Equipment, in course of publication (NATO UNCLASSIFIED/Releasable to IP)

Testing with B simulants is generally restricted to laboratory testing and field testing on open air test ranges with the necessary environmental permissions.

Even when laboratory testing with B warfare substances is an option, it may often be necessary to also perform laboratory testing with B simulants in parallel to establish and document warfare substance-to-simulant correlation to extrapolate test results.

3.5.3 Interferents

Interferent studies are usually conducted to determine the effect of interfering substances on the performance characteristics, *i.e.* sensitivity, probability of detection, response time and false alarm rate, of a CB DIM equipment. Interferents can be attributed to atmospheric, environmental, and/or man-made targets. It is known that such interferents may give rise to false alarms.

A promising approach in the area of interferent and background testing is the convergence between the two into synthetic background testing. Synthetic background testing involves laboratory testing with multiple interferents in an attempt to recreate characteristic properties of the background encountered in natural environments. By characterizing the natural background in relevant operating environments (*e.g.* rural, urban, maritime, industrial, *etc*.), it might be possible to define standard backgrounds that can be used for synthetic background testing. Such standardized synthetic background testing may dramatically improve the relevance of performance evaluations from laboratory testing. The ability to exploit the main benefits of laboratory testing, including high statistical confidence and possibility of using CB warfare agents, while at the same time improving the realism of the testing by recreating (simplified) real world environmental backgrounds, can be a powerful combination.

INTENTIONALLY BLANK

ANNEX A: Chemical Point Detection (CPD)

A chemical point detector responds to the presence of chemical substances within its own spatial location. It may detect CWA in the form of gas, aerosol, solid or liquid, and the intended use is for warning and protection.

Detection papers, colour tickets, colour tubes and continuous gas/aerosol sampling detectors are examples of CWA point detectors.

Electronic detectors are often capable of sending the detection result to an operator remote of the detector.

INTENTIONALLY BLANK

ANNEX B: Biological Point Detection (BPD)

During the last 20 years, a variety of different BPD devices and systems has been developed to provide:

- detect-to-warn BPD capability: biological point detectors are based on near-real time spectroscopic sensor technologies (*e.g.* optical particle counting and sizing combined with laser-induced fluorescence LIF);
- detect-to-treat BPD capability: integrated biological DIM systems based on various configurations of automated/online or manual/offline air sampling with or without front end triggering (*e.g.* by a near-real time detector), sample processing and preparation, and wet chemistry-based molecular assay techniques (*e.g.* polymerase chain reaction and/or antibody-based immunoassays).

The primary function of a BPD device or system when operated as a BPD capability will be to discover the presence of biological hazards in time to provide an operational benefit/added value under operational circumstances. The onset of human health effects following exposure to biological threat substances will be generally delayed, as long as appropriate medical countermeasures are readily available. Then, it could be still possible to achieve an operational benefit/added value without achieving exposure/contamination avoidance.

At least by definition, BPD capabilities will therefore not be limited to the use of BPD devices or systems with near-real time response capabilities. They may involve the use of BPD devices or systems with response times ranging:

- from near-real time detect-to-warn (*i.e.* detection in time to enable exposure/contamination avoidance);
- to delayed (*e.g.* minutes to hours) detect-to-treat (*i.e.* detection in time to enable administration of medical countermeasures resulting in reduced morbidity/mortality compared to post-symptomatic clinical recognition but not in time to enable exposure/contamination avoidance).

It is therefore necessary to develop and assess the performance requirements for BPD devices or systems in context with all other elements of the actual defence system architecture in which the BPD capability is to be operated, including but not limited to the biological (CBRN) defence doctrine, CONOP, and tactics, techniques and procedures.

INTENTIONALLY BLANK

ANNEX C: Chemical Stand-off Detection (CSoD)

Stand-off detection systems could be used in large indoor facilities; however, for relevant military threat scenarios they are expected to be primarily operated outdoors. Like some point detection systems, stand-off detection systems are generally based on optical spectroscopic methods. The required stand-off distances for testing are generally too long to be performed indoors. For stand-off technologies, it may be possible to do indoor chamber tests. However, these tests will not take into account a realistic atmosphere between the system and the target. This issue is due to the difficulty in recreating realistic environmental conditions in confined spaces.

For military research and development (R&D) activities, most of the development has focused on passive and active stand-off systems that exploit the atmospheric infrared transmission windows. For passive stand-off systems, the focus has – for instance - primarily been on passive Fourier transform infrared (FTIR) systems and infrared (IR) multi- or hyperspectral imaging systems. For active systems, R&D has been focused on light detection and ranging (LIDAR)-based systems. For long-range stand-off detection, passive FTIR systems have shown the most success[4], but FTIR sensors are by no means ideal. The FTIR systems rely on the difference in temperature between the cloud and the background to be successful and they only provide composite line-of-sight concentration x length (CL) measurements. Actually, CWA stand-off detection methods rely mostly on the vibrational spectral properties of the substances. This approach works mainly because air is composed mostly of nitrogen and oxygen that are transparent in IR wavebands. However, water, carbon dioxide and ozone do have IR spectral signatures, which may interfere with target chemical (*e.g.* CWA, TIC) signatures.

It should be noted that stand-off detection systems based on IR spectroscopic signature measurements should be able to identify a threat regardless of whether it is a vapour or an aerosol or deposited liquid or solid. However, for the purpose of this standard method, the expected threat dissemination methods will provide chemical clouds assumed to be primarily in vapour form, due to the relative maturity of this approach *vs.* chemical aerosol generation methods.

[4] Gittins, C. M.; Hinds, M. F.; Lawrence, W. G.; Mulhall, P. A.; Marinelli, W. J. In *Remote sensing and selective detection of chemical vapor plumes by LWIR imaging Fabry-Perot spectrometry*, Proceedings of the International Symposium on Spectral Sensing Research, (ISSSR) 2001, 2001; 2001; pp 294-302.

Lavoie, H., E. Puckrin, and J.-M. Thériault, "Measurement of toxic industrial chemicals, chemical warfare agents and their simulants, A LWIR passive standoff detection study," Technical Report, DRDC Valcartier TR 2006-634, April 2007.

Lavoie, H.; Puckrin, E.; Thériault, J.-M.; Bouffard, F., Passive standoff detection of SF6 at a distance of 5.7 km by differential FTIR radiometry. *Appl. Spectros.* 2005, 59(10), 1189-1193.

Polak, M. L.; Hall, J. L.; Herr, K. C., Passive Fourier-transform Infrared Spectroscopy of Chemical Plumes: An Algorithm for Quantitative Interpretation and Real-time Background Removal. *Appl. Opt.* 1995, 34, 5406.

Thériault, J.-M.; Puckrin, E., Remote sensing of chemical vapours by differential FTIR radiometry. Int. J. Remote Sens. 2005, 26, 981-995.

Schildkraut, E. R.; Connors, R.; Ben-David, A. In *Initial test results from ultra-high sensitivity passive FTIR instrumentation (HISPEC)*, Proceedings of the International Symposium on Spectral Sensing Research (ISSSR) 2001, 2001; 2001; pp 365-374.

INTENTIONALLY BLANK

ANNEX D: Biological Stand-off Detection (BSoD)

Like chemical stand-off detection, the operational goal of BSoD is to detect a biological threat (like bio aerosol-airborne cloud, deposited or bulk biological matter, *etc*.) without physical sampling. Currently, specific methods like immunology-based or polymerase chain reaction (PCR) present the potential to furnish specific biological information in a timely manner (currently in less than 1 hour: this delay is being continuously reduced to a few minutes). On the contrary, faster methods based on spectroscopy and photonic led to generic information, or even classification of previously acquired bio samples' signatures. The concept of use could be the rapid triggering of some collection systems to launch more specific but time-consuming identification methods.

Like chemical stand-off detection, the first step is to get signatures in controlled conditions (for instance in a closed chamber for controlling concentration, temperature, hygrometry, bio background nature, interferents, *etc*.). Field trials can be launched through outdoor releases by respecting local regulations that prevent dispersions of live B agents. Tests with BWA surrogates (*e.g.* like sporulated *Bacillus atrophaeus*) can be performed in authorized areas.

State-of-the-art BSoD technologies are limited in terms of technology readiness level (TRL). It is due to the challenge of a sensor being both sensitive and specific enough. Traces of highly pathogenic biological agents have to be detected inside a continuously fluctuating and complex biological background. The atmosphere is replete with a plethora of biological and organic matter (soots, pollens, fungi, naturally present bacteria, viruses, *etc.*) both airborne and deposited onto a variety of surfaces. Moreover, we deal with the concern of selectivity. Spectroscopic-based methods typically furnish spectral information that can be limited in terms of discrimination to distinguish the B threats whose pathogenic power is genetically codified.

For the long-range technique (from 100 meters to several kilometres), LIDAR-based systems have been developed to use the backscattering light of micrometric-sized airborne particles as a tracker of a suspicious cloud. By adding UV laser radiation, it is possible to get characteristic signatures based on UV laser-induced fluorescence (UV LIF). Polarization phenomena have also been exploited to distinguish bio aerosols.

By reducing the analytical distance, similar principles to the well-known BPD techniques have been tested to detect and classified deposited aerosols with the aims at building classification databases: laser-induced fluorescence (LIF), atomic emission-based method like laser-induced breakdown spectroscopy (LIBS), *etc*.

INTENTIONALLY BLANK

ANNEX E: Sensor Networks (SN)

A Sensor Network (SN) is a group of autonomous sensors or sensor nodes that provide CBRN incident detection through monitoring of physical parameters of a CBRN threat agent or TIM (radiation, chemical signature, *etc*.). Individual sensors in a network are deployed over an area of interest. This area coverage provides immediate warning to forces located within the area and supports follow-on action to determine the actual area of contamination. In this context, a sensor is defined as an equipment that detects, and may indicate, and/or record objects and activities by means of energy or particles emitted, reflected, or modified by objects[5].

A DIM component – as specified by means of the expertise of DIMP - detects and characterizes CBRN incidents, identifies the substances and hazards, delineates areas of contamination, and monitors the changes and is used for the tasks of surveillance, reconnaissance and survey. The Knowledge Management Panel (IMP) concerns the management of all form of CBRN defence related information : systematic information collection, issuing of critical warning messages, exchange of CBRN information, reach back capacity, analysis, storage, exploitation and the provision of CBRN assessments and advice for the planning operations prior, during and after CBRN incidents.

A carefully integrated system of CBRN sensors[6] can be a valuable tool for the task of CBRN protection, providing information for early warning and decision support to the CBRN defence in an effective way. The network could, for example, enable a central monitoring site to be built up which would reduce the need for personnel and/or expertise at the local measuring sites. The network would also enable functions to be automated and the compiled information to be used simultaneously for different processes or functions. A key function of an integrated system is that the integrated sensors are to deliver situation awareness and an updated CBRN common operational picture. A sensor network[7] will also allow data from several sensor resources to be analysed and calculated as composite components, giving improved reliability and a better basis for decisions.

A CBRN sensor network can be built up as a stand-alone network for CBRN monitoring or as part of an existing Communication and Information System (CIS). A standardized exchange of information between a stand-alone network and components in a CIS would also make it possible to build up different combinations of networks[8].

---

[5] AAP-6, NATO Glossary of terms and definitions (English and French)

[6] In ATP-45, the following benefits of sensor integration and networks are stated:

- CBRN sensor integration will provide the commander with an enhanced ability to detect, monitor, analyze and respond to a CBRN incident. Sensors and sensor management systems utilizing common standards will allow for the use of many types of sensors across multiple functions such as command and control systems;

- CBRN sensor integration will enable CBRN defence specialist and other designated personnel to update the common operational picture (COP) with CBRN and TIM-related information. Sensor integration will allow the transfer of data automatically to and from CBRN sensors and provide commanders, units, and command, control, communications and computers, and intelligence, surveillance, and reconnaissance (C4ISR) systems with warnings (*e.g.* alerts, alarms) and reports to affected units and throughout the battle space.

[7] Sensor monitoring and control is a sub function of sensor integration. It is implemented according to STANAG 4586 Edition 4, AEP 84 Volume I (previously known as STANAG 4586 Edition 2 version 4).

[8] Sensors and sensor management systems utilizing common standards will allow for the use of many types of sensors across multiple functions such as command and control systems (see ATP 45).

The detection capability of a sensor network must be well-balanced with regard to the threat in question and the environment in which the network will be placed. A sensor node can consist of one or several sensors that constitute a measuring site within the network. A sensor node can be in a fixed position to monitor a vulnerable object, *e.g.* a base area, a risk object or an on-going incident. A sensor node can also be positioned on a mobile platform, *e.g.* a patrol vehicle, UGV, UAV or a reconnaissance vehicle[9].

[9] Although STANAG 4586 is an unmanned aircraft vehicles (UAV) related standard, it is still relevant to all CBRN sensors integration efforts regardless of the platform for the following reasons:

- the UAV can be conceptual; therefore ground sensors can be integrated using this standard;
- provides a flexible architecture that allows for controlling and monitoring the vehicle and/or the sensor(s) by one or multiple hosts. It is recommended that only one host is allowed to have positive control of a given entity (*e.g.* sensor in this case);
- supports tactical low bandwidth networks;
- allows for the development of a common sensor controller due to standard commands and configurations;
- adding a new type of sensor (*e.g.* metrological) is possible by defining a few messages for monitoring and control of that specific new sensor type;
- STANAG 4586 is part of the overall multi-domain expansion effort currently underway in NATO.

ANNEX F: Technology Readiness Levels (TRL)

Source: Department of Defense (DoD) 2010, Defence Acquisition Guidebook

Technology Readiness Level		Description
1	Basic principles observed and reported.	Lowest level of technology readiness. Scientific research begins to be translated into applied research and development. Examples might include paper studies of a technology's basic properties.
2	Technology concept and/or application formulated.	Invention begins. Once basic principles are observed, practical applications can be invented. Applications are speculative and there may be no proof or detailed analysis to support the assumptions. Examples are limited to analytic studies.
3	Analytical and experimental critical function and/or characteristic proof of concept.	Active research and development is initiated. This includes analytical studies and laboratory studies to validate physically analytical predictions of separate elements of the technology. Examples include components that are not yet integrated or representative.
4	Component and/or breadboard validation in laboratory environment.	Basic technological components are integrated to establish that they will work together. This is relatively "low fidelity" compared to the eventual system. Examples include integration of *ad hoc* hardware in the laboratory.
5	Component and/or breadboard validation in relevant environment.	Fidelity of breadboard technology increases significantly. The basic technological components are integrated with reasonably realistic supporting elements so it can be tested in a simulated environment. Examples include "high fidelity" laboratory integration of components.
6	System/subsystem model or prototype demonstration in a relevant environment.	Representative model or prototype system, which is well beyond that of TRL 5, is tested in a relevant environment. Represents a major step up in a technology's demonstrated readiness. Examples include testing a prototype in a high-fidelity laboratory environment or in simulated operational environment.
7	System prototype demonstration in an operational environment.	Prototype near, or at, planned operational system. Represents a major step up from TRL 6, requiring demonstration of an actual system prototype in an operational environment such as an aircraft, vehicle, or space. Examples include testing the prototype in a test bed aircraft.
8	Actual system completed and qualified through test and demonstration.	Technology has been proven to work in its final form and under expected conditions. In almost all cases, this TRL represents the end of true system development. Examples include developmental test and evaluation of the system in its intended weapon system to determine if it meets design specifications.
9	Actual system proven through successful mission operations.	Actual application of the technology in its final form and under mission conditions, such as those encountered in operational test and evaluation. Examples include using the system under operational mission conditions.

INTENTIONALLY BLANK

ANNEX G: Definitions and Glossary

NATO DEFINITIONS

These definitions come from the NATO Standardization Office (NSO) and the definitions of the terms used by NATO (called "NATOTerm"). They are available on NSO website https://nso.nato.int.

Active	In surveillance, an adjective applied to actions or equipment that emit energy capable of being detected. (AAP-06)
CBRN substance	A chemical or biological substance, a toxic industrial material or a radioactive material, in any physical state or form.
Detection	In chemical, biological, radiological and nuclear defence, the discovery, by any means, of the presence of a chemical, biological, radiological and nuclear substance.
CONOPS	Concept of operations. A clear and concise statement of the line of action chosen by a commander in order to accomplish his given mission.
Evaluation	The structured process of examining activities, capabilities and performance against defined standards or criteria. Note: in the context of military forces, the hierarchical relationship in logical sequence is: assessment, analysis, evaluation, validation and certification. (AAP-06)
Identification	Determination of the presence of a specific CBRN substance. The process of attaining an accurate characterization of a detected entity by any act or means so that high confidence real-time decisions, including weapons engagement, can be made. (AAP-06)
CBRN monitoring	A continuous or periodic process of determining the presence of chemical, biological, radiological or nuclear substances or the occurrence of a nuclear burst. This may or may not include quantification.
Passive	In surveillance, an adjective applied to actions or equipment that emit no energy capable of being detected. (AAP-06)
Point detector	A device that detects the presence of a phenomenon or substance through direct contact.
Stand-off Detector	A device that detects the presence of a phenomenon or substance without direct contact.
Validation	The confirmation of the capabilities and performance of organizations, individuals, materiel or systems to meet defined standards or criteria, through the provision of objective evidence.(AAP-06) Notes: in the context of military forces, the hierarchical relationship in logical sequence is assessment, analysis, evaluation, validation and certification.

TECHNICAL DEFINITIONS

Aerosol	System of solid or liquid particles suspended in gas. [ISO 15900:2009]
Alarm	Audible and visual signal alerting a condition requiring immediate attention or user action. [ISO 8468:2007]
False alarm	Anomaly of the system leading to an unjustified warning or alarm. [ISO 21750:2006]
Precision	The closeness of agreement between independent test results obtained under stipulated conditions. [ISO 3534-1]
Repeatability	Precision under repeatability conditions. [ISO 3534-1]
Repeatability conditions	Conditions where independent test results are obtained with the same method on identical test items in the same laboratory by the same operator using the same equipment within short intervals of time. [ISO 3534-1]
Reproducibility	Precision under reproducibility conditions. [ISO 3534-1]
Reproducibility conditions	Conditions where test results are obtained with the same method on identical test items in different laboratories with different operators using different equipment. [ISO 3534-1]
Response (of a system)	Output quantity of a system. [ISO 2041:2009]
Response time	Time needed for the system (in a wide sense, including hardware and software) to take a decision. It can also be seen as the time for the system to refresh the information. (D/100 – Annex C)
Verification	Examination to confirm that an activity, a product or a service is in accordance with specified requirements. [ISO 13628-7:2005]

GLOSSARY

AEP	Allied Engineering Publication
ALOs	Agent-like organisms
BPD	Biological Point Detection
BSoD	Biological Stand-off Detection
BW	Biological Warfare
BWA	Biological Warfare Agent
CBRN	Chemical, Biological, Radiological and Nuclear
CBRN SN	CBRN Sensor Networks
CIS	Communication and Information System
CL	Concentration x Length
CONOPS	Concept of operations
COTS	Commercial Off The Shelf
CPD	Chemical Point Detection
CSoD	Chemical Stand-off Detection
CW	Chemical Warfare
CWA	Chemical Warfare Agent
DIM	Detection, Identification and Monitoring
DIMP	Detection, Identification and Monitoring Panel
DUT	Device Under Test
GOTS	Government off-the-shelf (product typically developed by the technical staff of the government agency for which it is created)
IR	Infrared
JCBRND-CDG	Joint Chemical, Biological, Radiological and Nuclear Defence Capability Development Group
KM	Knowledge Management
MOTS	Modified or modifiable off-the-shelf, or military off-the-shelf
NAAG	NATO Army Armament Group
NATO	North Atlantic Treaty Organisation
NOTS	NATO off-the-shelf or niche off-the-shelf (product developed by NC3A (for NATO Consultation, Command, and Control) to meet specific requirements for NATO.
NTOP	NATO Test and evaluation Operating Procedure
OPCW	Organization for the Prohibition of Chemical Weapons
R&D	Research and Development
SOP	Standard Operating Procedure
SN	Sensor Networks
SUT	System Under Test
T&E	Test & Evaluation
TIC	Toxic Industrial Chemical
TIM	Toxic Industrial Materials
TRL	Technology Readiness Level
UAV	Unmanned aerial vehicle
UGV	Unmanned ground vehicle

AEP-4834(A)(1)
Vol. I