STANDARDS RELATED DOCUMENT

SRD-1 to AJMedP-3

GUIDE TO MEDICAL INTELLIGENCE

Edition A Version 1
AUGUST 2020

NORTH ATLANTIC TREATY ORGANIZATION

Published by the
NATO STANDARDIZATION OFFICE (NSO)

INTENTIONALLY BLANK

NORTH ATLANTIC TREATY ORGANIZATION (NATO)

NATO STANDARDIZATION OFFICE (NSO)

NATO LETTER OF PROMULGATION

31 August 2020

1. The enclosed Standards Related Document, SRD-1 to AJMedP-3, Edition A, Version 1, GUIDE TO MEDICAL INTELLIGENCE, which has been approved in conjunction with AJMedP-3 by the nations in the Military Committee Medical Standardisation Board, is promulgated herewith.

2. SRD-1 to AJMedP-3, Edition A, Version 1 is effective on receipt and supersedes AJMedP-3-1, Edition A, Version 1 which shall be destroyed in accordance with the local procedure for the destruction of documents.

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.

for

Dieter Schmaglowski
Deputy Director NSO
Branch Head P&C

Zoltán GULYÁS
Brigadier General, HUNAF
Director, NATO Standardization Office

INTENTIONALLY BLANK

TABLE OF CONTENTS

CHAPTER 1 INTRODUCTION

1.1. MEDICAL INTELLIGENCE INTRODUCTION

Medical intelligence is defined in detail in AAP6; but in summary it is the result of analysis of all-source information regarding health threats, foreign medical capabilities and other health topics of relevance to national or NATO military operations.[1] The analysis is produced with the intent of providing decision advantage to government policy-makers and military commanders regarding health policy and strategic and tactical operations.

The individual nations that comprise NATO and partners align the responsibility for medical intelligence analysis differently. Many nations assign the responsibility to the medical elements of one of the nation's military services. Other nations assign the responsibility to the nation's defence intelligence service. Some nations have adopted a hybrid approach where the responsibility for the medical intelligence mission is shared by both the military medical service and an intelligence organization. This is not necessarily because they find collaboration easy and smooth, but because both disciplines hold important keys to achieving an optimal outcome. There are indeed advantages and challenges with each organizational framework, but the goal remains to provide decision advantage to the nation and the alliance on complex medical topics affecting the military, the health of the force, or national security. The constraints that govern the activity of medical services given by the Geneva Convention are discussed in Annex D.

The organizational framework each nation adopts for their medical intelligence effort impacts important factors affecting the information, analytic methodologies, scope and production and dissemination of the final medical intelligence product. Nevertheless, it is not the intent of the NATO Medintel Panel to prescribe organization or analytic structure to our member nations. The content of this document does not represent consensus within the member nations the way a STANAG does. Instead, our goal in producing this handbook is to offer examples of perspectives and methodologies that have proven successful in providing decision advantage in some nations. Our hope is that in sharing these successful examples we can provide instruction and guidance that other nations in the alliance can adopt and adapt to their own efforts for the improvement of the larger NATO medical intelligence capability, and that a common understanding of the diverse perspectives on medical intelligence will facilitate cooperation and sharing among all the NATO nations.

[1] Medical intelligence (medintel) is the product of processing medical, bio-scientific, epidemiological, environmental, infrastructure, capabilities and other information related to human or animal health. This intelligence, being of a specific technical nature, requires informed medical and other specialist expertise."

1.1.1 Preamble

Even though medical intelligence (medintel) has probably existed out of sheer necessity, in various shapes and forms, for as long as we have records of military activity, it may be considered a rather new and continuously evolving discipline. This handbook which accompanies STANAG 2457/AJMedP-3, is meant to be a living standards-related document (SRD) that details ways in which various aspects of medical intelligence may be performed within nations and command structures.

The way medintel is conducted and how the products are put to use differs widely within NATO, depending on the national priorities, resources available as well as access to formal training. It is often combined with other duties within a national force health protection (FHP) capability, and is therefore sometimes confused with other related activities. It may erroneously be equated with medical planning.

This handbook offers an insight into tools and methodologies used by various member and partnership nations. It should not be regarded as a strict part of the standardization requirements, but rather a book of inspirational recipes and texts that may be tried out, modified or adopted as they are. Methods used by one nation may not suit another nation, and the development of new technologies as well as rapid changes within disease ecology and political climate means that we must constantly adapt and evolve. Some of the texts are attributed to identifiable persons or countries, others are more the product of collaborations within the medintel panel.

Differentiating between medical information and medical intelligence may be difficult, and the two expressions may to some degree describe the same thing. However, medical information tends to hold a higher degree of certainty and be more established knowledge of the type health authorities and medical advisors may provide. Medical intelligence, however, indicates a product that tends to contain more uncertainty and it should be of a more predictive nature. It is also written into a specific operational context assessing the possible operational implications in order to help the decision makers avoid pitfalls. As intelligence proven right may quickly turn into information and as there is no clear-cut distinction, the two terms are proposed used under the joint item of MI2 (Medical Information and Intelligence).

CHAPTER 2 THE ROLE OF MEDICAL INTELLIGENCE IN THE COMPREHENSIVE APPROACH

2.1. INTRODUCTION

In addition to the classic *sensu strictu* military intelligence (INTEL) and in line with the Comprehensive Approach[2], the execution of military operations in the complex strategic environments of the 21st Century requires an unprecedented understanding of all the PMEESIIH[3] domains. This is not possible without making use of the Knowledge Development (KD) process.

KD should be a proactive, networked process, covering both collection, analysis, storage and dissemination of information, thus providing commanders and staff at all levels with a comprehensive understanding of complex environments, including the relationships and interactions between systems and actors within the engagement space. This can be achieved by utilising e.g. Geographical Information Systems (GIS) in addition to networking with the various Subject Matter Expert (SME) communities. This represents a transformation from the current traditional reactive approach, only supported by sporadic contributions from Subject Matter Experts (SMEs). Traditionally, the acquired knowledge is often neither fused, de-conflicted nor shared in a well-established manner.

The Medintel Panel would like to thank COL Vincenzo LaGioia (ITA, ret) and his team for of how producing medintel may best be resolved in future. This is presented in depth in the following chapter.

2.2. KNOWLEDGE DEVELOPMENT

2.2.1 Purpose of Knowledge development

The primary purpose of KD is to continuously **support and underpin situational awareness (SA) and the subsequent decision-making. This has to be initiated early** and is done in response to indications of an emerging security or safety problem, as well as during the planning, execution and evaluation of ongoing operations. Situational Awareness in NATO is an enabling capability which seeks to uniformly deliver the required level of information and understanding in the engagement space.

---

[2] The comprehensive approach appears to be a global concept that is often associated with civil-military cooperation; however, it goes beyond the existing NATO doctrine on enhanced civil-military cooperation (CIMIC). Furthermore, it is often mentioned in conjunction with counterinsurgency, Provincial Reconstruction Teams (PRT-Afghanistan), peace operations, stability operations and crisis management. For more information, see for instance http://www.natolibguides.info/comprehensiveapproach

[3] Political, Military, Economic, Environmental, Social, Infrastructure, Information, Health

2.2.2 Scope of Knowledge Development

KD depends on breaking down the traditional barriers and stovepipe organizations as well as encouraging ease of access and exchange of information. It also implies a reorientation of military intelligence activities, as these are primarily focused on **threats** descending from actual or potential adversaries within a specific country or region, while the Comprehensive Approach requires information and knowledge regarding interaction and influences of all key factors across a much broader operational environment. This includes **hazards** and **capabilities,** as may be obtained by the complementary use of non-military sources, e.g. from IOs, NGOs, private and commercial organizations, as well as the many Governmental Organisations (GOs) and Agencies. The final result should be a comprehensive picture of the operational environment.

2.2.3 Direction in Knowledge Development

KD is driven either by the information and knowledge requirements relating to potential areas of strategic interest prior to a crisis, or by the Commanders Critical Information Requirements (CCIRs) in established operations. System Analysis, an integral part of the KD, is a continuous, iterative and collaborative analytical process, employed to holistically examine the engagement spaces. This integrates the analyses of all the PMEESIIH domains. The additional factors Health (H) and Environment (E) contributed from medical intelligence (medintel) provide critical contributions to KD, supporting the overall situational awareness by giving a more complete picture.

As a matter of fact, Out of Area operations and expeditionary operations typically occur in unfamiliar engagement spaces. These are often disrupted settings where forces may be exposed to a range of environmental health challenges usually not present in their home base. In addition, there are numerous potential threats negatively impacting on the individual health or on operational objectives. This may be due to hazards linked to collateral effects of operational activities, or even asymmetric warfare and terrorist use of Weapons of Mass Destruction (WMD).

2.2.4 Medical intelligence contributions in the Operational Planning Process

Robust and comprehensive Force Health Protection (FHP) programs should be implemented by the Commanders in order to face all the predictable health challenges. These are based on proposals issued by the responsible medical staff. However, for unfamiliar environments they may only be properly developed and continuously adjusted when relying upon a so-called Comprehensive Preparation of the Environment (CPOE), which has to be applicable, timely, specific and relevant at all times. This applies from the initial planning stage, throughout the operation (including the Operational Planning Process), as well as during (execution of operations), redeployment and evaluation.

These activities have to include the assessment of hazards of operational concern such as infectious diseases, environmental and industrial health issues, public health events and Chemical, Biological, Radiological and Nuclear (CBRN) threats, as well as an assessment of host nation and opponent medical capabilities/infrastructures.

It is important to highlight that these assessments may also feed the CPOE for other than FHP purposes, at any level, and this may have certain legal implications (ref. Annex D. on Geneva Conventions and medintel).

All these areas belong to medical intelligence (medintel), which according to the definition is "*intelligence derived from medical, bio-scientific, epidemiological, environmental and other information (sources) related to human or animal or environmental health. This intelligence being of a specific technical nature, requires medical expertise throughout its direction and processing within the intelligence cycle*."[4]

2.3. MEDICAL INTELLIGENCE AS PART OF KNOWLEDGE DEVELOPMENT

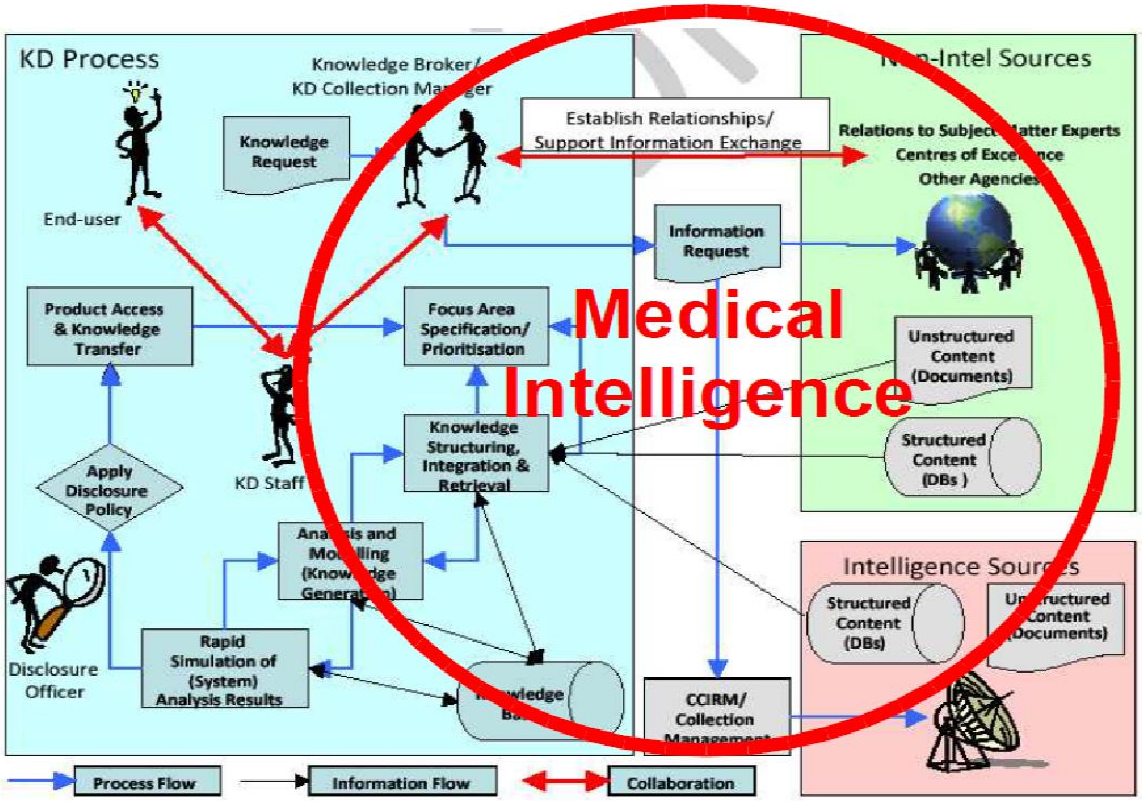
2.3.1 Position of medical intelligence.

With regard to the KD concept, medical intelligence does not fully fit into the classical threat-centric Intelligence, as it only exceptionally deals with belligerent-driven health threats (which mostly are due to asymmetric warfare). More commonly, medintel is focusing on prevailing environmental health hazards, natural and man-made, that are commonly present in the engagement spaces. ***That is the reason why medintel – according to different National approaches – can reside in the Intel domain without denaturalising its main purposes and role.***

In light of this, medical intelligence has a two-way relationship with the KD, as it feeds into but is also fed by the KD process, contributing to the situational awareness and to the CPOE through analysis, modelling, integration and prioritisation of structured and unstructured information coming from **Intel** and **Non-Intel sources**. This also includes **Reach-Back Analysis** supported by Centres of Excellence (Figure 1).

[4] AAP-6

Figure 1: Medical intelligence stands astride all the domains (KD, Non-Intel Sources, Intelligence Sources).



However, medical intelligence assessments may be either exploited to give input to the overall force protection concept (**medical use of medintel**) or to support other-than force protection operational purposes (**non-medical use of medintel**).

CHAPTER 3 THE ROLE OF MEDICAL INTELLIGENCE IN THE DECISION MAKING PROCESS

3.1. MEDINTEL SUPPORT TO THE DECISION MAKING

Medintel, as an INTEL subset, serves several essential purposes in decision-making process, supporting **planning (OPP[5])** and/or **execution of operations (OPS[6])**, at any levels:

- strategic,
- operational,
- tactical,

with qualified **joint intelligence preparation of the operational environment (JIPOE)**.

JIPOE is a systematic, cyclical and dynamic process, closely connected to the individual stages of the commander's decision-making process and closely meshed with the Intelligence Cycle.

As a matter of fact, during the JIPOE process, new intelligence requirements are identified and entered into the Intelligence Cycle.

The results of the process are represented graphically on a series of overlays, concerning the operational environment as well as the adversary's and other actors' features. These can all be prepared well in advance, but just before and during operations, current updates can be included to reflect changes in key factors that may affect force activity across the spectrum of conflict.

Medintel benchmarks primarily are:

- ***Health Hazard:*** *anything with the potential to cause harm to health (well space-time related);*
- ***Health Threat:*** *a circumstance that can cause harm to the health, linked to an adversary's intent & capability, as well as a target's vulnerability.*
- ***Health Risk:*** *the probability of the occurrence of an event or incident and the assessed health consequences thereof.*

As a consequence, the **medintel-oriented overlays,** belonging to the **JIPOE Area Evaluation step or as a stand-alone product (MedIntel Preparation of the Operational Environment - MIPOE)**, are aiming at meeting the Commanders requirements, at providing the Commanders a consistent comprehensive support

[5] Operational Planning Process
[6] Operations

before/during/after any operational involvement, and at achieving a medical situation awareness, by taking into account:

- Environment: encompassing basic data about the physical natural setting (topography, climate & vegetation, hydrogeology, natural resources etc), the anthropic background (population, IDPs, refugees, human activities, socioeconomic features, industrial sites, etc.);
- Health: including environmental health (water & sanitation, air & soil quality; hazardous facilities, as landfills/waste disposal, TIM[7], road traffic accidents); infectious diseases of operational concern - transmissible to humans and/or animals, including vector & reservoir assessments; dangerous and poisonous animals and plants;
- Medical capabilities/infrastructures: including HCWs data, hospitals, vaccination clinics (and childhood immunization rates), drug factories, pharmacies, blood banking, hyperbaric chambers, medical & scientific CoEs, ambulances, medevac capacity;
- CBRN capabilities/infrastructures: including study and research centres, dual use capabilities, military production/storage/mixing & filling sites, proving grounds, biosafety – 3 & 4 laboratories, radiotherapy units.

All these overlays can offer the Commander a detailed ***situation awareness*** about a lot of domains of possible operational concern.

Intel assessments – including medintel ones – descending from these depicted items, as resulting from analysis and fusion of different data in order to have the **needed predictive value,** may be hyperlinked to the overlays.

The principal medintel commitments are:

a. to provide a health & environment threat/hazard assessment and relative risk assessment, as well as HN medical capabilities upon which Commander's staff (medical planners and FHP officers) can develop and plan for medical support and FHP countermeasures across the full spectrum of operations ranging from Article V to non-Article V operations.
b. In this view medintel may also contribute to Counter Intelligence (CI) in denying an adversary the opportunity to conduct terrorism or sabotage attacks against friendly forces, by identifying friendly force's vulnerability.
   Medintel issues identification rely upon:

   - baseline assessments, aiming at supporting the **OPP**,
   - current JISR reports, about unusual/unexpected public health events of possible operational or international concern (PHEOCs/PHEICs[8]), aiming at generating *alert* in support of execution of operations (**OPS**);

c. to support the strategical and operational decision making by providing specific assessments valuable for non-medical uses (VIP's health status, research advances, medintel assessments as indicators for overall INTEL purposes).

[7] Toxic Industrial Materials , including TIC (chemical), TIR (radiological), TIB (biological)
[8] Public Health Event or Emergency of Operational/International Concern

To accomplish this role, medintel can't be only considered a plain Intelligence Product, but needs to be accounted as a full Intelligence all-sources Functional Discipline or Process, different from other intelligence collection disciplines by source type (HUMINT, IMINT, SIGINT, etc.), as covering a peculiar role in developing space-time related and evidence-based hazard assessment as well as relative risk assessment.

Therefore, its products can involve technical and forensic responsibilities to the decision-making Authority, and so de facto behaving as a peculiar discipline, sometimes featured with stand-alone products.

3.2. MEDINTEL AND THE ENVIRONMENT- TWO SIDES OF THE SAME COIN

(SWE)

Deployed personnel regularly face an environment[9] torn by the consequences of conflict or disasters. The need to be concerned about the force health aside, challenges of environmental disruption also brings a need to ensure that the overall operation will strengthen and not hamper the often fragile environment of the receiving nation.

The majority of the environmental damage that occurs in times of conflict is collateral, or related to the preparation and execution phases of wars and to the coping strategies of local populations. Identifying environmental risks and key drivers of vulnerability can help prevent conflict in the future and increase the prospect for achieving the strategic end state of the mission and facilitate a sustainable development in the receiving nation, in support of the comprehensive approach.

During NATO-led military activities, the NATO commander and the sending nations (SNs) should therefore proactively ensure the health and safety of their own forces as well as operate in a manner that protects the environment.[10]

Each nation ultimate bears the responsibility for the actions of its own forces when conducting military activities. Furthermore, NATO and the Participating Nations also have a collective responsibility for the protection of the environment (EP). As a minimum, the Host nation's (HN's) environmental laws must be respected, however where Participating Nations and/or Contributing Nations EP standards are more stringent than HN ones, they should be applied as long as not contravening to HN law and as far as reasonably practicable. Where HN environmental laws do not exist, applicable EP standards must be agreed upon a consensus by participating nations during the planning process. In addition, an Operation plan (OPLAN) must include specific guidance in the form of an EP Annex (usually Annex E).[11]

---

[9] AAP-6; The surroundings in which an organization operates, including air, water, land, natural resources, flora, fauna, humans, and their interrelation.

[10] STANAG 7141 (Ed. 6 of 15 May. '14 / AJEPP-4) - Joint NATO EP Doctrine during NATO-led Military Activities

[11] MC469/1 (14 Oct. '11) - NATO Military Principles and Policies for Environmental Protection (EP)

Both health and the environmental aspects therefore determine the need for and the flow and structure of environmental information and environmental-related intelligence.[12] Whereas medical intelligence focus on health threats to the individual soldier as well as health threats of significance for mission success, environmental information and environmental-related intelligence support environmental protection and looks at future threats and trends of strategic significance. That environmental-related intelligence can be utilized in early warning capabilities i.e. anticipating future events, weak signals detection and trends analysis.

An example list of information requirements on environmental issues can be found in Annex C.

[12] Environmental intelligence is an emerging subset of intelligence, and hence an integral part of an overall intelligence assessment. In STANAG 6500 for instance, Environmental Intelligence is mentioned as an integral part of planning and preparation for an operation. An agreed upon definition similar to the one for medical intelligence is however yet to be defined.

CHAPTER 4 INFORMATION REQUIREMENTS AND MEDINTEL PRODUCT TYPOLOGY

Medintel products are issued by medintel organization:

1. Usually in order to accomplish the needed Information Requirements, among which:

- Commander's Critical Information Requirements (CCIR), concerning all the areas that are either critical to the success of the mission or represent critical hazards or threats and encompass Friendly Forces Information Requirements (FFIRs) and Priority Information Requirements (PIRs);
- PIR (Priority Information Requirements): intelligence requirements (among CCIRs) anticipated by the Commanders and his staff as considered vital to the planning and the execution of courses of action as these requirements drive the collection and production effort;
- Specific Intelligence Requirements (SIR) and Essential Elements of Information (EEI) complement each PIR and provide a more detailed description of the requirement by allowing the production of a more detailed collection plan and task list;

2. Less frequently, proactively, in the absence of specific requirements when considered valuable to stakeholders.

As a consequence, it's possible to differentiate at least the followings MedIntel products:

- Medintel Basic products: assessments tailored to a specific operational scenario, used as reference material for planning and as a basis for processing subsequent information or intelligence. They have to take into account baseline health/environment data concerning a peculiar Country/Area of Interest in order to give the due support to the OPP:
- Environmental Health Hazards: relative risk assessment linked to climate, air, soil and water status (quality, quantity, distribution, sources), waste management and landfills, sanitation, industrial sites and TIM polluting sites (civilian and military), road traffic accidents, collateral damages of natural or operational activities, poisonous animals & plants;
- Biological hazards: communicable diseases: identification and relative risk assessment due to infectious diseases of operational concern, transmissible to humans and/or animals (incidence/prevalence rates, geographical distribution, immunization rates in childhood), to vectors and reservoirs;
- CBRN threats: relative risk assessment from possible intentional releases of CBRN agents from WMD resources or from dual-use/covert facilities;
- Medical capabilities: assessments of medical resources in term of quality/quantity of infrastructures and beds, manning (HCWs), equipment and hygiene, specialized units (trauma/surgery centres, ICU, CCU, CT scans, NMR or PET scans, burnt units, hyperbaric chambers, radiotherapy units),

ambulances, helipads, closest airports & seaports for medevac purposes, blood supply, pharmacy, laboratories, pharma-industries.

Medintel Basic products may be developed:

- according to the attached format (Annex E);

- graphically as MIPOE (MedIntel Preparation of Operational Environment), in a multilayered approach, in order to coordinate and integrate a large quantity of information with ease of comprehension and speed.

2. Medintel Current products: reflect the current situation at either strategic, operational or tactical level concerning a peculiar health and/or environmental issue of possible concern, for FHP purposes as well as for non-medical purposes, supporting the overall INTEL assessments. They assess impact of current operating environment on personnel & the impact of operations on environment and local population/infrastructure, pointing out why they are relevant (the so what factor) and include predictive assessment. They can offer greater granularity than basic intelligence, but are normally time sensitive, usually perishable, snapshots, even though can contribute to further refine the basic products. Medintel Current products include possible impending health risks issued with reference to public health unusual/unexpected events or to public health events of operational/international concerns (PHEOCs/PHEICs) assessments.

3. Medintel Report (MEDINTREP): is a report that is sent spontaneously whenever the information it contains is considered likely to require the urgent attention of the receiving commander or his staff, such as for confirmed alerts. It can be structured in narrative form as described in AD80-3 or formatted as in this latter document or in ADatP-3.

4. Medintel Summary or Bulletin (MEDINTSUM): concise periodic summary of MedIntel inputs on the current situation, designed to update the current intelligence picture and highlight important developments concerning health and environment issues during the reporting period related to a commander’s area of intelligence responsibility. Its distribution should include all those whose responsibilities and interests may be affected by the contents.

5. Medintel Target products and Medintel Thematic reports: assessments either concerning sensu strictu INTEL targeting (target exclusion & collateral damage estimation) or taking into account particular aspects of situation/phenomena related to the health/environment domain and their possible impact on operational environment for medical or non-medical uses. Among these, there may be predictive evaluations on regional health or movements of populations as consequences of climate changes or results of violence, use of public health data as indicators of local institutional proficiency, VIP’s health status assessments, etc.

6. Replies to RFIs (Request For Information): medintel assessments concerning peculiar thematic issues originated by superordinate, subordinate or adjacent Organization in order to acquire or refine information/assessment concerning an area

or a specific matter of interest as decided with the medintel or INTEL collection plan. The receiving organization will treat the incoming RFI as an intelligence requirement, undertaken on behalf of another organization. Replies to RFIs may be fulfilled by issuing medintel stand-alone assessments or by medintel contribution to INTEL replies when an all-discipline approach is needed.

As a medintel organization – according to different National approaches – can reside either in the intel domain, as well as in the medical domain, or both, the mentioned medintel product list may be made up of differently named products however aiming at the same purposes.

INTENTIONALLY BLANK

CHAPTER 5 MEDINTEL METHODOLOGY

5.1. MEDINTEL METHODOLOGY

Final Risk Assessment is a process under the Commander's responsibility and is usually performed by his staff, by taking into account all the elements of the COP (friendly forces, mission, enemy, terrain, CoAs, vulnerabilities, etc.), in order to evaluate at any level (strategic, operational, tactical) a predictable comprehensive risk to military units engaged in a specific setting or operations and mission.

Relative Risk Assessment (RRA) concerning health issues is one of the medintel's core businesses and contribute to the Final Risk Assessment.

RRA results from applying the operational risk matrix, as outlined in this chapter, taking into account *hazard/threat severity and probability*, *to a healthy and fit general population devoid of any protective or preventive countermeasure*.

Medintel assessments rely upon precise methodologies aiming at obtaining valuable products, different according to the peculiar matters taken into account.

For practical purposes it is possible to highlight the following critical methodological approaches.

The relative risk assessment (RRA) process for medintel purposes is aiming at defining the baseline levels concerning the most important health issues of operational concern, the trigger factors the baseline vulnerabilities.

The prioritization of the multitude of environmental health hazards/threats, to be identified and assessed among those deeply impacting upon operational effectiveness, determines which of them have a credible potential to become a health or environmental danger to the operational effectiveness of a military unit.

The **environmental health risk assessment methodology** can be summarized as follows:

In order to assess and grade the relative risk of immediate or delayed health effects due to exposure (population thresholds) to environmental issues, it is useful to refer to some publications:

- US publication TG[13] 230, for chemical exposures;
- ICNIRP guidelines: for limiting exposure to time-varying electric, magnetic, electro-magnetic fields (up to 300 GHz);

[13] Technical Guide 230 "Environmental Health Risk Assessment and Chemical Exposure Guidelines for Deployed Military Personnel"

- IAEA International Basic Safety Standards for Protection against Ionizing Radiation and for the Safety of Radiation Sources, for ionizing radiations.

The **infectious disease risk assessment methodology** has to be applied in order to identify which communicable diseases can pose serious immediate or delayed health concerns and/or have operational impact on an exposed military population. One useful approach is the US developed IDEAL[14] methodology.

The **CBRN threat domain encompasses three different methodological pillars:**

- **CBRN threat categorization,** in order to rank different agents according to their value descending from potential/possible intentional releases (prioritization process);
- **CBRN threat assessment,** a full threat assessment, performed by taking into account the threat constitutive factors assessed concerning an actor or an area of interest: agent scoring, capability, intent, vulnerability;
- **CBRN threat plausibility assessment,** by applying a decisional algorithm to a suspected Public Health event in order to evaluate its plausibility of a natural/unnatural origin.

[14] Infectious Diseases Investment Decision Evaluation Algorithm

5.2. NATO FORCE PROTECTION MODEL

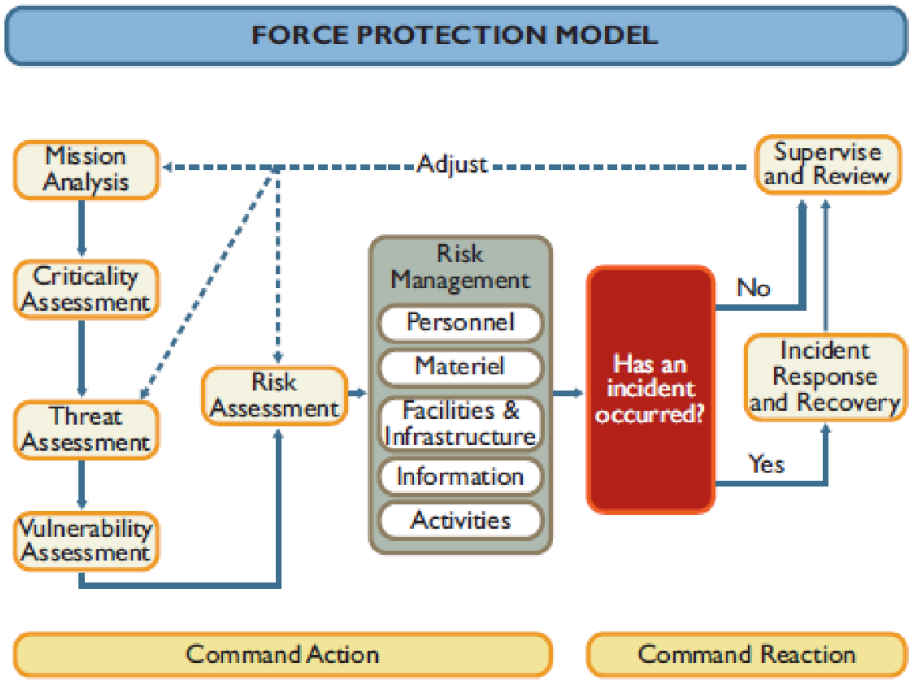


Figure 2: The Force Protection Model.
Illustration and text from AJP-3.14, p. 2-1 –2-2

The risk management process is divided into eight steps:

a. Identify the assigned and implied tasks through **mission analysis**.

b. Identify those assets that are critical to mission success (**criticality assessment**).

c. Determine likely threats and hazards to personnel and those assets that are critical to mission success (**threat assessment**).

d. Identify vulnerabilities that could be exploited by threats and the impact of incidents on the force's effectiveness, thereby affecting mission success (**vulnerability assessment**).

e. Determine the risks to mission success from an assessment of the ability of the threat to exploit identified vulnerabilities, and accidental and environmental hazards caused by human error, topography, climate, weather and the presence

of TIM[15] and endemic diseases that pose risks to personnel and critical assets (**risk assessment**).

f. Identify and implement appropriate FP controls and measures to reduce risk to a level acceptable to command and calculate and monitor the residual risk or gaps in order to manage the mission (**risk management**). Willingness to accept risk is likely to be influenced by political constraints.

g. Identify and implement incident response and recovery controls and measures including the development and implementation of an emergency response and recovery plan (**incident response and recovery**).

h. Maintain, reassess, and amend FP controls and measures throughout the mission (**supervise and review**).

The Nato Force Protection Model is integrated in the operational planning process. The major purpose of the FP planning is to support the Commander with a foundation for the force composition (organisation, abilities) that is required from a FP perspective to accomplish the Oplan. Another purpose is to analyze what ROE, current legislation and any SOFA, MOU and MTA could mean to FP and integrate this in the Oplan.

The Risk Management mechanism major function starts when the Commander has chosen an option for further planning (and when the operation is on-going). It's purpose is to minimize risks (in a resource-optimized way) associated with the assets that have been deemed necessary for *achieving the mission* (critical assets).

The NATO FP Model uses a broad perspective, and a large number of potential threats against critical assets and personnel are analysed (compare step e. above). Unacceptable risks are lowered by introducing various protective actions (step f. and g.)

The results of the FP planning work are orders, directives, procedures etc. In an Oplan these are found primarily in Annex J (Force Protection). Other important sections are Annex D (security), Annex E, Environment and Annex U (CBRN). Furthermore, there are arena- and function-specific directives for FP in respective Annex.

Troop Contributing Nations (TCNs) are responsible for providing their own FP, and for contributing to the wider protection of the Allied force to which they are assigned. TCNs must inform the Allied JFC if their FP concepts or capabilities differ significantly from that prescribed by NATO, the assigned command or are otherwise considered deficient.

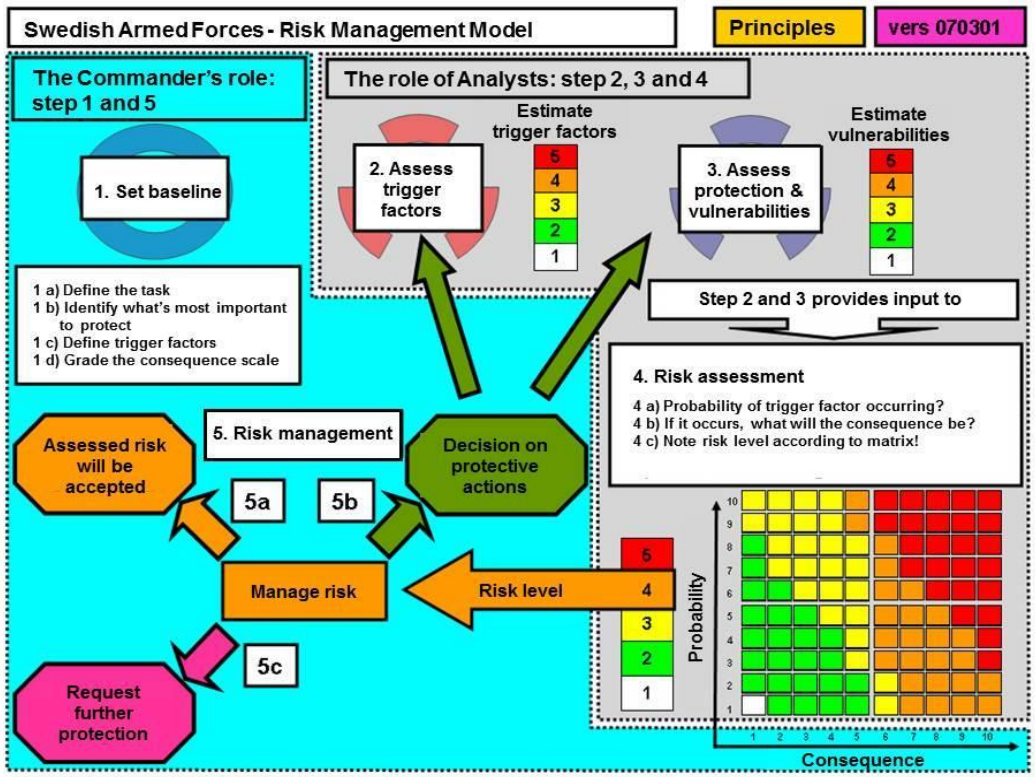
[15] Toxic Industrial Materials

5.3. SWEDISH ARMED FORCES RISK MANAGEMENT MODEL

(SWE)

The Swedish Armed Forces uses a risk assessment model as a part of the decision making processing when planning and managing operations. The details of this process is presented below.

Figure 3: The Swedish Armed Forces Risk Management Process



Step 1. Determine the basic values

The Risk Management Process starts with the Risk Manager (the Commander) determining four basic values (1a – 1d). In this step, the Risk Manager provides the directions and delimitations that are required for further work. Without this input from the Risk Manager, the analysts are forced to make assumptions, which in the worst case can lead to decisions made on faulty basic values. ***Therefore, it is of utmost importance that the Commander takes responsibility already early in the process.***

1a. Define the task

This means in principle ”A decision at large” or when appropriate a mission analysis:

- What should be done?
- Who should do it?
- Why should it be done?

- Where should it be done?

When should it be done/when should it be finished?

1b. Identify what's most important to protect

When the task is performed according to 1a, which critical assets could be endangered? Which ones are the most relevant? Examples of critical assets can be life and health of personnel, operational capacity of a unit etc.

1c. Define trigger factors

When the task is performed according to 1a, which threats can attack or affect the critical assets identified and prioritized in 1b? There can of course be many potential threats, and to identify all of them can be very labor-consuming. The role of the Commander is therefore to limit the analysis, by deciding which of the most important threats should be analyzed.

1d. Grade the consequence scale

If a prioritized critical asset should be affected, damaged or completely destroyed on account of a certain threat, what would the possible consequence be? The Commander envisions the possible outcome in five or ten ”result spaces”, which are put onto a consequence scale coupled to the actual critical asset and type of threat.

In a risk management process, that requires a lot of work, the Commander cannot produce on his own all necessary information for step 1, and is therefore reliant on his staff to produce the alternatives. However, it is always the Commander that makes the final decision on what should be used in further planning work.

Step 2: Assess trigger factors

The type or types of threats which the Commander has decided on to further analyze should be broken down to concrete unwanted events, phenomenon's or attack modus operandi.

N.B. The break-down process should be taken to such a level that the threats are possible to manage in a protection- and vulnerability perspective (Step 3). This is very important – if the threats are described in too general terms, the room for interpretation will be too big, and further analysis will be rendered impossible.

Step 3: Assess protection & vulnerabilities

In this step our current protection is identified and measured against the threats that were concretized in step 2. Note that our protection can be preventive, active or passive and/or be of a more recuperative character. The purpose of the protection is the same, i.e. diminish the probability/consequence of a certain threat.

The assessment of our protective capacity against a certain concrete threat results in a vulnerability assessment. The vulnerability is graded on a scale from 1-5. Every vulnerability level has a number and a colour, where level 1 (white) stands for “no visible vulnerability” and level 5 (red) stands for “very high vulnerability”. In other words – large flaws in protection means large vulnerability and vice versa.

Step 2 and 3 (and 4) are supported by the Risk Analysis Tool. This is a large Excel sheet which ensures that all factors are recorded and nothing is forgotten

Step 4: Risk assessment

Based on step 2 and 3, hopefully there is enough relevant information to proceed to step 4 and assess the risk. This is done jointly, i.e. the functions that performed step 2 and 3 meet again and assess together the probability for a certain concrete threat to happen, and if so, what could the consequence be.

4a. Assess the probability of a certain threat

What is the probability a threat? In the assessment, not only the threat in itself is taken into account, but also our behaviour, our protective resources, our security awareness and our exposure in time and space. The probability is estimated on a probability scale ranging from 1 to 10.

4b. Assess the consequence if a threat should happen

If a threat happens – would it penetrate existing protective actions? Will there be a consequence for the actual critical asset? In that case, what? Could the consequence be lessened by some active, consequence-reducing protective measure (e.g. medical resources)? The result of the assessment is verbalized and checked off against the consequence scale decided by the Commander. The result will be a value between 1 and 10.

4c. Assess the risk

The probability value (1-10) and the consequence value (1-10) are put into the risk analysis matrix. The risk level (colour according to matrix) is noted.

Step 5: Manage the risk

When the risk has been analysed, the Commander has to take a stand on one or more decision alternatives:

a. Decide that the assessed risk level is acceptable compared to target effects or mission accomplishment and costs for diminishing risk (conscious risk-taking).

b. Decide on further protective actions using own resources to diminish risk.

c. If the unit's own resources are insufficient, ask for support from superior Commander.

In the latter case, c), the superior Commander will take over the responsibility for risk management.

The superior Commander can, if he has the mandate, order the junior Commander to solve the task at present risk level, but at the responsibility of the superior Commander.

The superior Commander can, if he has the mandate, order the junior Commander to solve another task instead, with a lower risk level.

Alternatively, the superior Commander can supply the resources needed to reduce the risk level.

The risk management decision shall be accompanied by a **plan for follow-up**. The follow-up plan can take many shapes, e.g. a plan for a new risk assessment at a certain date, a plan for how decided protective actions should be implemented or how a situation with an unacceptable risk level should be handled until new protective actions are implemented.

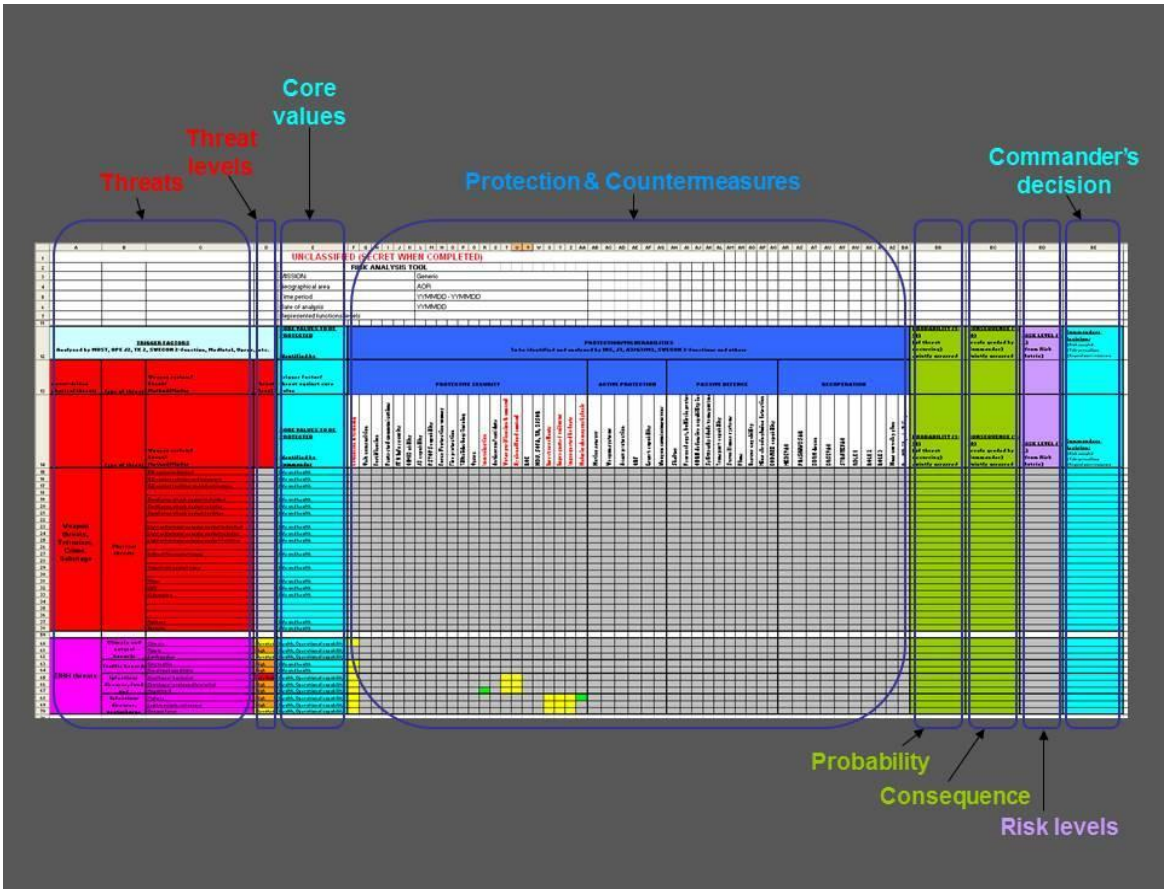


Figure 4: The Risk Analysis Tool of the Swedish Armed Forces

5.3.1 NATO FP Model and Swedish Armed Forces Risk Management Model in a NATO-led operation

It is important to note that even if the NATO FP Model and Swedish Armed Forces Risk Management Model have clear similarities, they are not identical.

In a NATO-led operation where Sweden participates, both processes exist in parallel, but with different purposes:

- The NATO FP model takes a holistic approach to *all risks that affect the ability to solve the task* and provides a basis for orders regarding a complete concept for FP from the international Force Commander. These orders must be followed by a Swedish Contingent, or alternatively flag national exceptions or limitations (e.g. caveats).

- The Swedish Armed Forces Risk Management Model centres around the risks that the Swedish National Command assesses to be most relevant for the operation.

It can be risks that affect the possibility to solve the task, but it can also be other risks of special national interest. In some cases, the national risk assessment can affect the NATO operation, for example if the Swedish contingent upholds a higher protective level than the one ordered by the international Force Commander.

An especially important issue to take into consideration is that an international Force Commander can have a different view on the risks associated with the operation compared to the Swedish national view. One reason can be differing views on what should be considered critical assets and how they should be valued. Likewise, views on what should be considered as acceptable risks could vary. This can potentially be problematic. For example, an international Force Commander could use Swedish resources in a way that is totally acceptable from his risk management perspective, whereas it would be unacceptable from a Swedish risk management perspective.

5.4. BASELINE INFECTIOUS DISEASE RISK METHODOLOGY

(USA)

5.4.1 Introduction

The following is a proposed standardized methodology that guides and structures baseline infectious disease risk assessment. Specific procedures have been developed for selection of diseases of potential military significance and for assessment of the risk of individual diseases, the combined disease risk within transmission categories, and the overall country risk level.

5.4.2 Baseline Assumptions

1. Personnel are healthy, active-duty members medically qualified for deployment, with a competent immune system, good nutritional status, routine childhood immunizations, and no chronic debilitating medical problems.

2. Personnel typically have no natural immunity to most tropical diseases.

3. Personnel are living in field conditions typical of a tactical military operation .

4. Personnel have frequent off-duty exposure to the local economy.

5. Personnel are dispersed throughout an area and may be mobile, resulting in a variety of different exposures (i.e., not everyone is usually exposed to the same small focal area).

6. Risk level assumes that NO COUNTERMEASURES are being implemented.

5.4.3 Methodology for Assessing Individual Disease Risk

A proposed methodology for assessing the risk of an individual disease is based on the analytic framework outlined in the figure below.

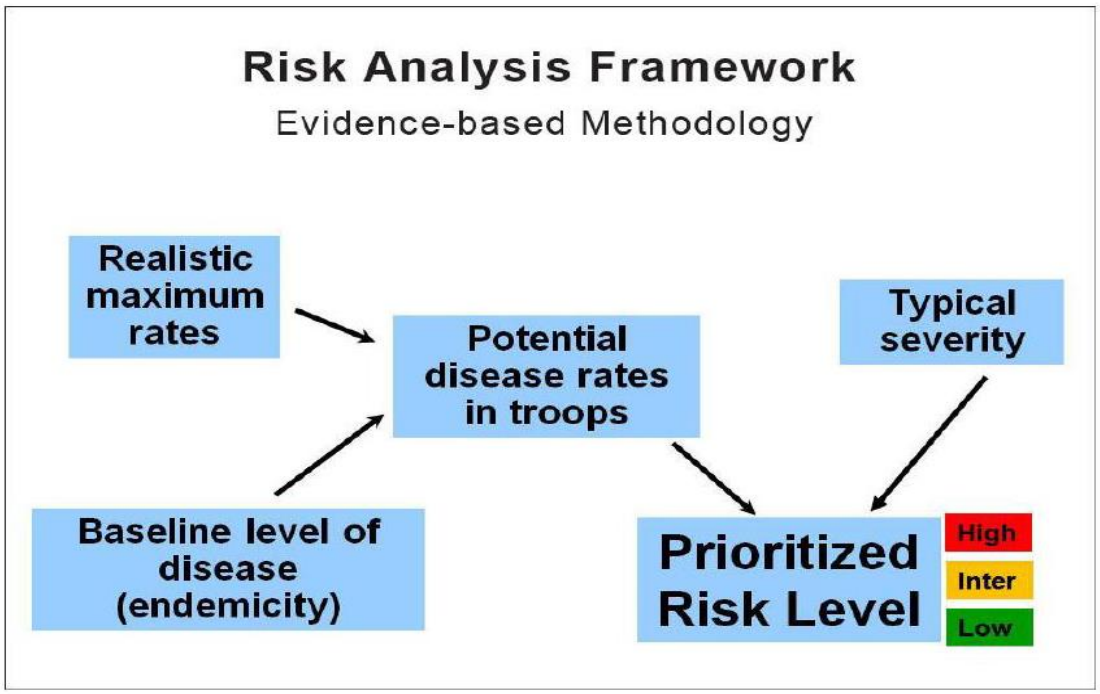


Figure 5: Risk Analysis Framework

Realistic Maximum Rates

For each disease, an estimate of the "worst case" monthly rate of symptomatic infections for a military population under realistic field conditions with very high natural exposure.

Level of Endemicity

In order to estimate how much exposure a deployed force might have to a particular infectious agent in a particular country, assesses the degree of exposure that the local population has to that agent.

Potential Disease Rates in the Force

An order of magnitude scale also can be used for estimates of the potential disease rates in troops deployed to a particular country

Typical Severity

For each disease, the typical severity should be described which categorically addresses the amount of lost duty time expected.

Prioritized Risk Level

In the final step of risk assessment, an overall prioritized risk level (High, Intermediate,or Low) can be assigned for each disease of potential military significance in the country.

The risk level is based on the potential rate per month, derived previously, and the typical severity of the disease.

Ranking Disease Transmission Categories

Diseases can be grouped into categories according to their primary mode of transmission because, in many cases, similar force health protection countermeasures apply to multiple diseases in the same transmission category.

The combined overall risk of each transmission category can be assessed based on the assessment of individual diseases within it.

5.5. ENVIRONMENTAL HEALTH RISK METHODOLOGY

(USA)

An environmental health risk/threat analysis assesses baseline environmental issues in a country or area that could result in adverse health effects in deployed individuals. Most of the information used to make a medical intelligence assessment on

environmental issues is from open sources; however, classified reporting may also be useful.

When assessing the environmental health situation in a given area of interest, it is critical to understand the broader regional issues that can greatly influence the operating environment. For example, current events such as war/conflict and/or weather or geologic events (hurricane, earthquake, tsunami, etc.) can cause serious degradation or pollution of the environment.

Access to water and sanitation in the country (as reported) can give an indication of the level of infrastructure whereas population trends, such as population growth and/or movement and urbanization, can determine the demand or burden on water/sanitation infrastructure. Major economic activities (industrial and agricultural) may adversely impact the environment, depending on existing environmental laws and regulations and the effectiveness of governmental enforcement of those laws and regulations.

Environmental issues that could impact the health of deployed personnel include physical hazards (such as extreme temperatures, high altitude, seismic/volcanic activity, flooding, etc.) and the presence of contaminants in environmental media (air, water, soil, and food) at sufficient concentrations to cause adverse health effects in exposed individuals.

Factors that impact water quality include sources and quality of drinking water, availability of a treated drinking water supply, operational status and maintenance of water supply infrastructure, and access to water treatment chemicals. Some common issues that can degrade the quality of surface and groundwater are contamination with sewage or agricultural and industrial chemicals, saltwater intrusion, and naturally-occurring contaminants (such as arsenic). In the absence of comprehensive water quality monitoring data, waterborne disease trends and recent outbreaks in a region can be used as an indicator of poor water quality.

Air quality can be impacted by many factors including dust and sandstorms; vehicular emissions and the use of leaded gasoline; the level of industrial activity and the amount and type of industrial emissions; natural phenomena, such as volcanic activity; and agricultural burning or forest fires. Many countries have air monitoring stations in selected areas and this type of monitoring data is valuable to assess levels of air contamination.

Soil contamination can result from industrial or mining activity; inadequate waste disposal practices; or leaking pesticide storage containers, petroleum storage tanks, or pipelines. A history of chemical spills in a region may be an indicator of possible soil contamination.

Food contamination (either chemical or microbial) can result from a general lack of food safety and handling practices; lax enforcement of food safety regulations; irrigation of food crops with contaminated water sources; misuse or overuse of agricultural chemicals; algal bloom toxins (seafood) or fungal toxins; or inadequate refrigeration (due to an unreliable power grid). Food- borne illness trends and recent

outbreaks as well as food safety recalls may be an indicator of problems with the national food-safety program.

Reports of contaminated environmental media can be obtained from various reliable sources including: scientific literature; international organizations (WHO, UN organizations, etc.}; country governmental departments (Ministry of Health, Department of Environment, etc.}; military environmental surveillance teams; and news media. This reporting can be compared with established exposure standards (either national or international} to determine levels of contamination and the potential impacts on human health.

A risk/threat matrix (such as the one developed by the National Center for Medical Intelligence/Defense Intelligence Agency) can be used to determine the overall health risk/threat to deployed forces from specific environmental media. The matrix weighs both the probability of exposure and the severity of its effect. Probability of exposure takes into account the likelihood of military personnel being exposed based on the physical properties, location, and environmental media (air, water, soil,and food} of the contaminants. The severity of health effects is assessed by looking at site-specific health effects for the reported contaminant(s}. In cases where specific reporting on negative effects in populations of interest is unavailable, environmental sampling results can be used as a surrogate and compared to applicable environmental guide

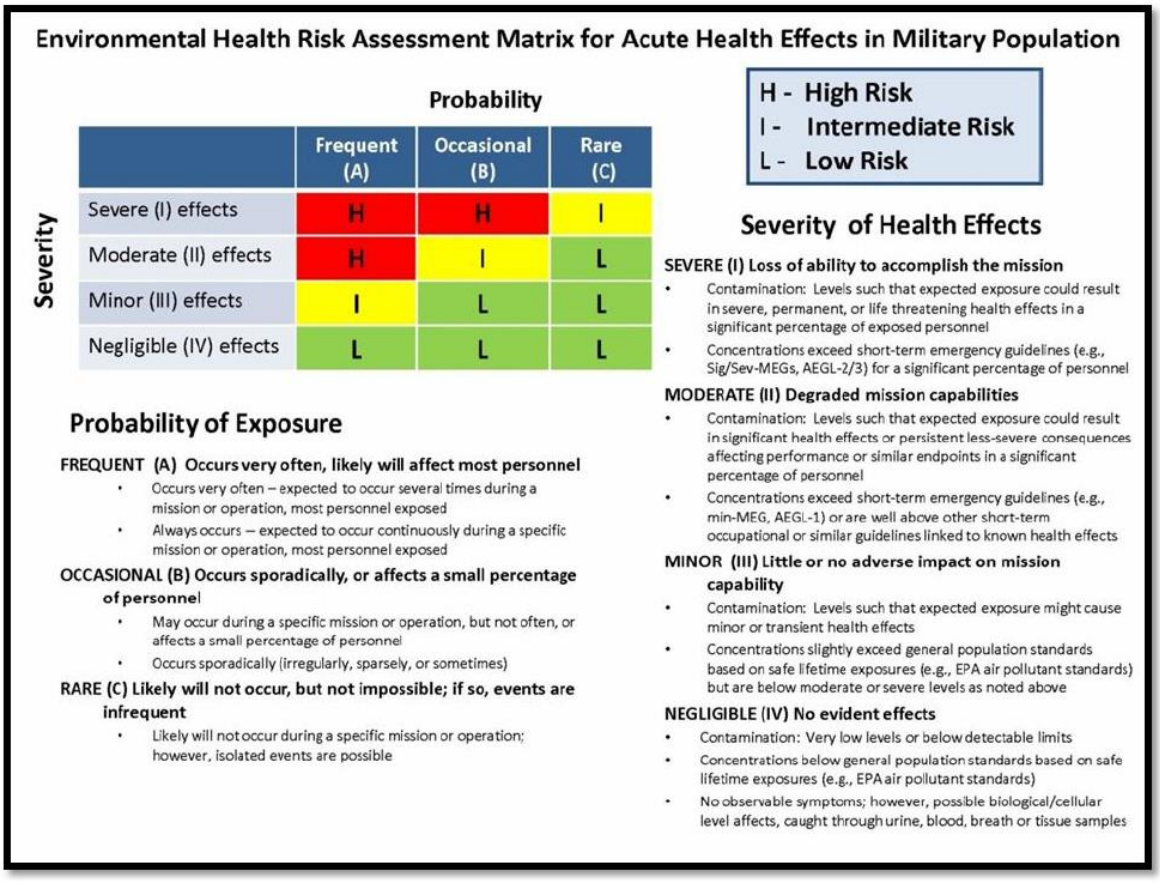


Figure 6: EH Risk Assessment Matrix

lines to determine severity. Selected levels of probability and severity determine the overall health risk in the matrix.

5.6. GENERIC THREAT ASSESSMENT AND REALTIVE RISK: BIOLOGICAL THREAT AGENTS AND WEAPONS

(Col Per Leines Lausund, DVM MPH, Major Knut Amund Grani, DVM and Professor Per-Einar Granum, PhD, previously published in HFM TG 186 technical report)

Preface by COL Vincenzo La Gioia (ITA):

This is a full threat assessment, performed by taking into account the threat constitutive factors assessed concerning an actor or an area of interest: agent scoring, actor's capability & intent, target's vulnerability;

These criteria are liable to be weighted:

1. *"CBRN agent scoring:*
   It is the index descending from the CBRN threat categorization process.

2. *Actor's capability*
   - *Technical skills (scientific R & D programs involving CBRN agents civilian or military; program of development of WMD; high qualified industries/companies in biotechnology, chemistry, pharmaceuticals, vaccine production, food for newborns, high containment biological laboratories, such as BSL[16]-3 & 4, nuclear plant and Uranium enrichment-facilities)*
   - *Technical probability, including different factors, differently weighting for state and non-state actors:*
     - ✓ *Ease of acquisition,*
     - ✓ *Possibility/ease of genetic or other modification,*
     - ✓ *Ease of large scale production / storage,*
     - ✓ *Ease of handling,*
     - ✓ *Ease of weaponization,*
     - ✓ *Ease of dispersion,*
     - ✓ *Aerosol, stability,*
     - ✓ *Atmosphere, water, food stability.*

3. *Actor's intent*
   - *CBRN Health threat indicators & warning (attachment: MedIntel Indicators),*

[16] Bio Safety Level

- *INTEL assessments or reports,*
- *INTERPOL/EUROPOL assessments (terrorists).*

4. *Target's vulnerability*
   - *Ease of exposure (or contamination of route of exposures),*
   - *Security of critical infrastructures,*
   - *Susceptibility of population at risk,*
   - *Ease of detection,*
   - *Individual countermeasures:*
     - ✓ *Diagnostic capabilities*
     - ✓ *Treatment options*
     - ✓ *Prophylaxis options including protective equipment*
   - *Decontamination options or hazard control measures*

The CBRN Threat Categorization is a preliminary step in the evaluation of a possibly existing threat or in the discernment of nature of any Public Health incident/event in order to rank the possible severity of the event and its impact.

5.6.1 Introduction and definitions

Biological threat agents are agents that cause disease or damage to humans, other animals, plants or materiel, to (mis-)quote the NATO definition. Here, we are concerned with the threat and risks that humans may be exposed to if or when a biological threat agent (this publication covers those agents on our list) is used as a weapon or terrorist tool. At our meeting in Norway in May 2010, we achieved consensus on a list of 15 agents that we in the RTG/HFM-186 believe are the most probable threat agents and the ones we should concern ourselves with. This chapter, with an assessment of the relative risk and threat associated with biological threat agents is limited to these, though other agents may be dealt with the same way in order to expand the list.

A common definition of the term "risk" is as an expression of the probability and consequences of an event. When discussing the relative merits of the agents on the list, this event may be seen as "intentional use" expressed as the probability based on the technical challenges that must be met for each agent. The term "risk" is thus used to characterise the product of the probability of intentional use based on technical feasibility, as defined by the underlying factors that are evaluated, and the expected consequences of such use.

The term "threat" usually expresses a product of intent and capability to create an adverse event. The dimension of the threat is usually decided by the degree of intent and the actual capacity of the actor. Capacity is understood as the quantification of capabilities. In order to evaluate the relative threats posed by agents on the list one would have to delve deeper into the minds of potential perpetrators, which is outside the scope of this publication. However, in order to make an attempt at describing the relative threat that could be related to these agents, two dummy entities are used as anonymous examples of a state and non-state actor respectively, and are used to have a baseline "intent" for the purposes of threat description. Detailed capacities and

intentions for both are described and defined later in this chapter. The use of disease in the sabotage role is outside the scope of the document.

When the phrase “Biological Weapon (BW)” is used in this document it must be interpreted as describing a completed attack system using a biological agent as filling, and including all the necessary components in a piece of ordinance (casing, fuse, control mechanisms, safeguards, dissemination or dispersal mechanism/system, etc., and with a militarily accepted efficiency and predictability when used) that has been tested and approved as functional. This process and the development of a product are extremely complicated, expensive and time- consuming, and it would not be expected that a non-state actor could develop such a system unnoticed in today’s environment. Of the known groups, the Aum Shinrikyo in Japan[17] is the one that was closest to producing an actual weapon but did not have the necessary testing and proofing capabilities, and as such they failed.

The non-state actor is assumed to have lesser capabilities and capacities than a state, and also to be unable to produce a biological weapon as described above. The degree of refinement and sophistication of a device used by a non-state actor will of course vary with the abilities, skills, knowledge and opportunities of the actor, but the common phrase used here for this kind of device is BTA or “Biological Terrorism Agent” to cover both agent and delivery mechanisms associated with it.

5.6.2 The technical probability of agent use

Several factors influence the probability of a specific agent being used in or to develop a Biological Weapon (BW) or a Biological Terrorism Agent (BTA). The list of factors is also a list of requirements and challenges to be met during the selection, acquisition, development and use of a biological agent. In most cases, the difference between BW and BTA will be in how well these challenges and requirements can and need to be met. The description of the technical probability of agent use will not differentiate between these two facets, but will be covered in the evaluation of the threat the different agents pose when in the hands of a state or non-state actor based on their level of technical proficiency and their knowledge and skills.

Factors:

- Availability of agent, either in culture collections or in nature, or from diagnostic samples.
- Identifiability, i.e. how well-suited the agent is to definitive identification:
- Differing strains; and
- Differing pathogenicity/virulence in sub-strains.

[17] Monterey Institute of International Studies report; Chronology of Aum Shinrikyo’s CBW Activities; 2001; http://cns.miis.edu (nedlastet 12 Apr 2007) and Hiroshi Takahashi, Paul Keim, Arnold F. Kaufmann, et al.; Bacillus anthracis Incident, Kameido, Tokyo, 1993; Emerging Infectious Diseases • www.cdc.gov/eid • Vol. 10, No. 1, January 2004.

• Culture, describing the degree of skills and conditions necessary to culture or replicate agent.

• Isolation of agent, the difficulty or easy with which it can be “lifted” from a mixed culture.

• Virulence describes the ability of the agent to cause disease when the optimal sub-strain is chosen.

• Stability, describing how well the agent retains its properties with regards to virulence, viability, etc.,

○*in vitro*:

• Including development in the presence of immunity (modifications to circumvent); and

• Routes of infection.

• EoP, or Ease of Production, where end result is usable quantities of agent suitable for weaponization or use.

• EoH, or Ease of Handling, describing how easily the agent can be handled from acquisition and production through dissemination.

• Morbidity expectations.

• Mortality expectations (in the absence of countermeasures).

• TTE, or Time To Effect, denoting probability of a release causing effects within a desired and predictable time-frame.

• RoE, or Reliability of Effect, including environmental survivability during dissemination.

• Possibility of genetic or other modification.

5.6.3 The dummies

Two categories of actors will be described and represented by dummies in this document: the state and non-state actors. The non-state actor is assumed to operate without dependable state support.

(i) The state actor

The dummy used to exemplify a state actor has the following characteristics:

• A burgeoning biotechnological industrial base, with established production of fermentation-based and gene modified products.

• A scientific base for the biotechnology industry in the country and an active R&D establishment working in the fields of microbiology and molecular genetics, and with at least one Biosafety Level (BSL)-3Ag facility with access

to laboratory animals, available with the necessary security arrangements in place to be able to conduct agent tests clandestinely.

• A military or military controlled scientific establishment working in parallel with, and drawing knowledge and experience from, the civil science and R&D establishment.

• A civil and military medical service able to afford what the regime deems to be sufficient protection of the country's population and armed forces in case a biological warfare agent is used in conflict.

• An intention, i.e. the intent to be able to deploy a Biological Weapon (BW) in order to start, maintain or influence a conflict and cause casualties that would decisively alter the paradigm of such conflict. This intent could be driven by an aspiration to have and be able to use a weapon of mass destruction that is less visible in development than a chemical or nuclear weapon would be, and possibly as a response to a perceived adversary's capabilities.

The development of a biological weapons programme would in the early stages be impossible to distinguish from medical (including veterinary medical) and environmental research; indeed, much of the relevant and necessary information could be derived from completely open and legal microbiological, infectious disease and environmental research. Only in the later stages, where agent survivability and large-scale dissemination needs to be tested, will accidents or observations give indications of the activity. This might be in the shape of a non- transparent pathogen testing programme, unusual vaccine or biological countermeasures development, the establishment of "false-flag" bio-containment or BSL-3, BSL-3Ag+ or preferably -4 facilities, or the appearance of small outbreaks or clusters of unusual disease.

(ii) The non-state actor

The non-state actor would typically be a belligerent group driven by radical ideas, by definition independent of any government, willing to use violence or death as a tool and willing to extend the use of this tool to include deliberate introduction of dangerous pathogens into society. Most such groups would be considered terrorists, but could be deniably supported by some states. If such a group obtains a safe haven in any country for the purposes of establishing headquarters and, in this case, an R&D base, they would after about a year move into a third category, the state-supported actors with capabilities that will lie between the non-state actors and states with a bio-weapons programme. This third category will not be discussed further in this document, but will be classed in the state category.

In our context, a non-state actor has restricted overt access to technology and scientific institutions. The ability to communicate without being compromised is also limited, as is the ability to travel. The actor will have limited scientific and technological capabilities quantitatively or qualitatively, and will also be constrained in time when they are a known threat: counter-terrorism has a high priority. This again restricts the freedom of choice in targeting, means and scope of an attack.

There are many definitions of terrorism[18], but the most comprehensive and easily understandable one[19] we have found defines five necessary elements:

- Terror is a method and not an ideology in itself[20]. Terror is in other words a tool.
- Terror contains the threat of systematic and directed violence.
- Terror is usually directed against civil society, it is apparently indiscriminate and its targets often of symbolic value.

The fear derived as a consequence of the first three elements, and which makes tactical success possible, is the precondition for the fifth element: A strategic goal, which is political.

From this one may also draw the conclusion that a non-state actor using a BTA need not cause overly many casualties, but must give the impression that they can and will. The non-state actor will have an intention to cause terror by the deliberate use of biological agents causing disease and death against their targets.

5.6.4 Dissemination

Based on the requirements for the precise and predictable effect of weapons use from state actors and the need for spectacular attributability from the non-state actor, a requirement will usually be that the effects of an attack occur as simultaneously and within as defined a time-frame as possible. Besides demonstrating that this is an intended event and maximising injury, it will also minimise the ability of health services to respond sufficiently. A comparison of some possible dissemination routes is given below with regard to timing and efficiency. Terminology has been garnered from Sackett *et al.* for the phasing[21].

---

[18] Terrorism is defined by the U.S. Department of Defense as “the unlawful use of – or threatened use of – force or violence against individuals or property to coerce or intimidate governments or societies, often to achieve political, religious, or ideological objectives.” www.pbs.org/wgbh/pages/frontline/teach/alqaeda/glossary.html downloaded 11 September 2007. The main challenge faced when trying to define terrorism, and which tends to defy lawmakers, is that acts of terror encompass several different criminal acts that are part of the phenomenon, and are difficult to use to formulate an exclusive, formal definition. Terror may be explained analytically, or definitely defined

[19] Jansen PT. The effect and effectiveness of counter-terrorism methods used by Israel, 1993 – 2006; PhD-thesis in international relations, University of St. Andrews, Scotland, 2007.

[20] Rote Arme Fraktion is an example where violence (Urban guerrilla warfare) was a goal in itself as it countered (Max Webers observation on) “... das Gewaltmonopol des Staates…”. (Max Weber: “Politics as a Vocation”, closely followed by Thomas Hobbes in “The Leviathan” where he describes the necessity of an instrument of violence to retain power).

[21] Sackett DL, Haynes RB, Guyatt GH and Tugwell P. Clinical Epidemiology – a basic science for clinical medicine 2nd ed; ISBN 0-316-76599-6; ch 5 s155 ff. 1991

Dissemination via	Period of Infection	Prodromal Phase	Acute Disease	End-State
Surfaces	Days	1 – 10 days	6 – 20 days	Uncertain
Foods	Days – Weeks	Days – Weeks	Days – Weeks	Uncertain
Water	Days	1 – 10 days	6 – 20 days	Uncertain
Aerosol	Minutes	1 – 5 days	3 – 8 days	4 – 14 days

Table 5.6-1: Effect of Dissemination of Something like Anthrax on Disease Development – Time-Scale

Notes:

- *Contaminating surfaces will certainly cause infection, but within an undefined time-frame and dependent on agent survivability. Contagion will thus be distributed over days depending on contact time and amount, received dose will vary, and disease will occur over a longer time axis that does not give a clear indication of an attack. Gastrointestinal and cutaneous infection is achieved, with an uncertain outcome with respect to the number of dead and sick.*

- *Foodstuffs may be infected intentionally, and will give a long-lasting, low-dosage exposure dependant on when and how the relevant food is consumed. It will complicate identification, but also weaken the claim and effects of a biological attack. Gastrointestinal infections will result, but with even less certain outcome than after surface contamination.*

- *Contaminating water-supplies, while doable may give the same effects as contaminating surfaces. Tap water is difficult to contaminate due to disinfectants and dilution, but local sources or piping areas may be efficiently utilised. The impact will be very variable, depending on water use in the target.*

- *Infection from inhaled air containing an aerosol gives an immediate dose and an acceptable probability of massive, simultaneous contagion in the target. Disease progression will be similar in all affected, and the probability of the desired effect being reached high.*

5.6.5 The risk posed by the agents

When evaluating the risk posed by the different agents in these actor-scenario settings, absolute numbers are very complex to find or even estimate. What will be covered is the relative risk represented within the group of agents chosen, based on an evaluation of the different factors related to the agents. Thus, an easily identifiable and accessible, suitably pathogenic agent that is stable in culture and has a good shelf-life may have a higher relative risk than one which is more difficult to culture and identify, even though the latter may have higher pathogenicity. As these factors are to a large extent decided by access to knowledge, technical expertise and equipment they will be weighted differently between the non-state and state dummy when estimating the technical probability of use.

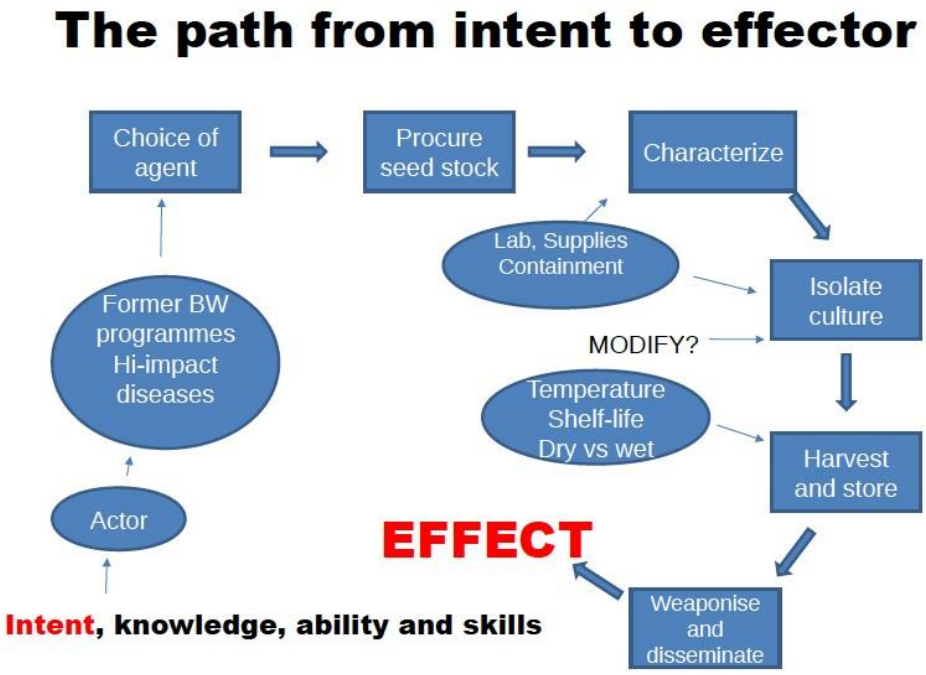


Figure 7: Overview of the process of creating a biological weapon.

5.6.6 The actor

We are facing two potential groups of actors: the state-supported, or national who bases their effects on political and military power, and the non-state actor basing their effects on terrorism.

In both cases the four factors – intent, knowledge, ability and skills[22] – are decisive, as are the differences in constraints: few constraints need bother the state actor provided there is an intent, while the non-state actor, operating outside the law and norms of society, is at least constrained in time, knowledge, ability, skills and, not least, security.

[22] Intent is described earlier, and is the basis for any assessment or evaluation of threat. An actor must have the intent of using biological agents to cause harm. Knowledge cover the whole aspect of tacit and intangible knowledge necessary to run the process of producing a biological agent in such a form as to be usable to fulfil an intent. Ability covers accessibility to facilities and equipment that makes the process achievable, skills are those necessary to exploit these abilities.

Figure 8: Actor constraints

We have developed a matrix to describe some of these constraints as they influence agent production, and to all intents and purposes the level we should be considering when assessing the dummy non-state actor is 2, the state actor somewhere between 3 and 4.

It is important to bear in mind that the principal quantitative difference between these two groups is caused by the unequal constraints of resources, supplies, containment and storage facilities, delivery vehicles, time, knowledge and skills.

Level	Agents	Competence	Facilities
0	Contamination with faecal matter or similar	No scientific background necessary	None necessary
1	Agents in impure culture	Basic microbiology	Simple lab
2	Pure, identified agents	+Technical skills and diagnostic knowledge	Containment corresponding to « almost BSL-3 »
3	Stabilized agents	+Supporting group, lab animal facilities	BSL3, lab animal facility + production
4	3 + delivery means	+Multi-disciplinary group with weaponization capability	As 3, plus BSL3Ag+ or BSL4 and test sites

Table 5.6-2: Competence and facility requirements.

Level 4 needs resources that transnational groups with state support and “safe haven” might have available; these would then be considered outside the non-state actor group, more similar to states.

At Level 0, the actor is seen capable of using pollutants directly to contaminate the environment. There is no demand on scientific competence or need for facilities to accomplish this; faecal matter polluting a well is a sufficient example.

At Level 1, agents, only probably identifiable, would be cultivated in impure cultures and with questionable, if any, effectiveness. At Level 2, isolated and identified strains would be developed and used, at Level 3 we would find stabilized and confirmed agents and at Level 4 the biological warfare agents.

5.6.7 Identifying and choosing agents

Identifying and choosing biological agents for development into effectors is crucial to any success, and is the first test of the capability of the actor.

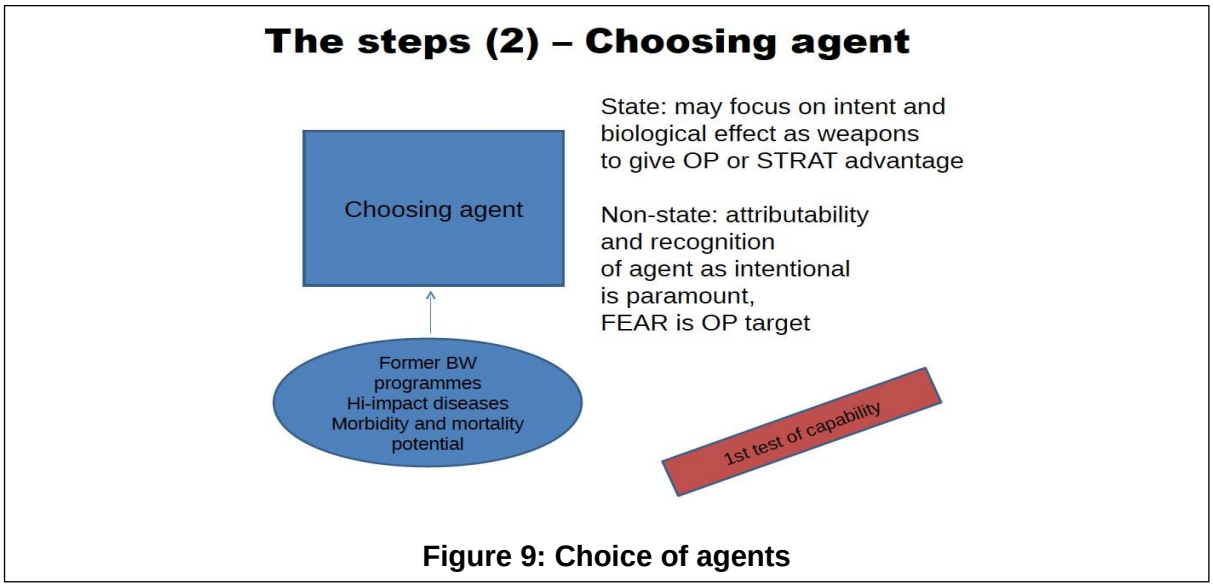


Figure 9: Choice of agents

A state actor needs a weapon with defined and predictable effects in order to use it as part of a campaign plan and be able to exploit the results. It needs an agent that gives an operational or strategic advantage: the effect must be large enough to achieve this and at the same time be a deterrent. Based on the knowledge base represented by the state's collective R&D resources, a state may choose a suitable effector, with a focus on properties that work towards an operational or strategic advantage.

A non-state actor does not need the same quantitative EFFECTS; they need to create fear or a state of terror. The agent must be recognisable as DANGEROUS, but as mentioned earlier attributability is crucial, it must be apparent that the event is intentional.

Our group, RTG/HFM-186, has gone through the first stage one would see in any kind of programme, be it defensive or offensive, involving biological agents in a threat scenario. This involves the use of skills, abilities and knowledge to identify and evaluate agents as threats. Any choice of agents will always be debatable, some will have a preference for one while excluding another, others would like to include many more, some would even deny the possibility of any agent having a belligerent potential. The mix of expertise in different fields associated with defence against biological weapons has, however, led us to a consensus list containing 15 agents, of which three are toxins. A state would probably be able to ID and choose any 14 of our 15 agents, *Variola major* (smallpox) being a special case, as knowledge, skills and abilities are

not serious constraints. Non-state actors would be restricted in choices due to these constraints, and would probably choose agents based on prior knowledge of effects and high accessibility. This knowledge would be acquired by studying former BW programmes, high-impact diseases and the morbidity and mortality potential of accessible agents.

Most of the agents listed will be familiar to anyone interested in this aspect of microbiology, and based on an evaluation of virulence, pathogenicity, stability, availability, ease of production and dissemination, possibilities of modification, and knowledge of the potential the different agents have to cause harm when used belligerently, we ended up with this choice:

1) *Variola major* (smallpox);
2) *Bacillus anthracis* (including MDR) (anthrax);
3) *Yersinia pestis* (plague);
4) *Francisella tularensis* (tularemia);
5) Filovirus Ebola;
6) Filovirus Marburg (viral hemorrhagic fevers);
7) *Clostridium botulinum* toxin (botulism);
8) Alphaviruses (VEE, EEE, WEE) (viral encephalitis);
9) *Brucella* species (brucellosis);
10) *Burkholderia mallei* (glanders);
11) *Burkholderia pseudomallei* (melioidosis);
12) *Coxiella burnetii* (Q-fever);
13) Staphylococcal enterotoxins;
14) *Rickettsia prowazekii* (typhus fever); and
15) Ricin toxin.

Some of these will be familiar from former, discarded weapons programmes; the reason for this being, of course, that behind the selection of agents chosen for development in the former arsenals of some Nations lay a great deal of science and knowledge of effects that is difficult to bypass. The others may be seen as what we regard as the most potential of the representatives of new or emerging disease-causing agents. With the exception of *Variola major*, they are all zoonotic with animals as their main host.

Further challenges are provided by the continuous emergence of these kinds of agents, and as science advances, so does the ability to use and change these agents into new agents of war or terrorism. A special concern is the synthesis of highly pathogenic microorganisms, either unintentionally as seen with mouse ectromelia virus[23] in 001 or intentionally. These concerns must be covered elsewhere.

[23] http://jvi.asm.org/content/75/3/1205.abstract. (accessed 12 Jan 2011)

5.6.8 Procuring seed stock

Finding the right pathogen sub-strain to work with is a crucial success criterion in any kind of offensive programme.

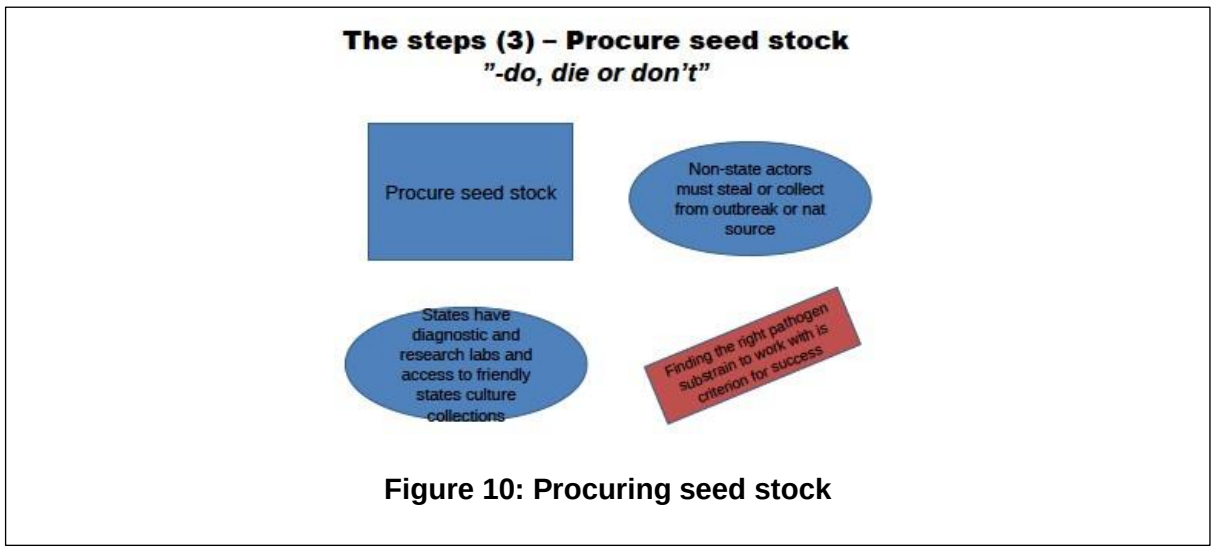


Figure 10: Procuring seed stock

This is the "do, die or don't" of a programme. Again, non-state actors are hampered by lack of the access states have to diagnostic laboratories, research labs and culture collections in their own or friendly Nations. They are reduced to stealing from laboratories or collecting from outbreaks, a complicating uncertainty factor as regards the effectiveness of the agent. States will succeed if they put their minds to it; non-states may have to go for the tried and tested agents. This is an important limiter for the non-states, and is where they and states part ways with regards to technical probability, and thus risk.

5.6.9 Characterisation

The actor further needs to characterise agents with regard to virulence and pathogenicity and stability of properties during further work and development. This may be one of the points where the Aum Shinrikyo group failed; they produced an ample load of anthrax spores only to experience the embarrassment of them being a vaccine strain.

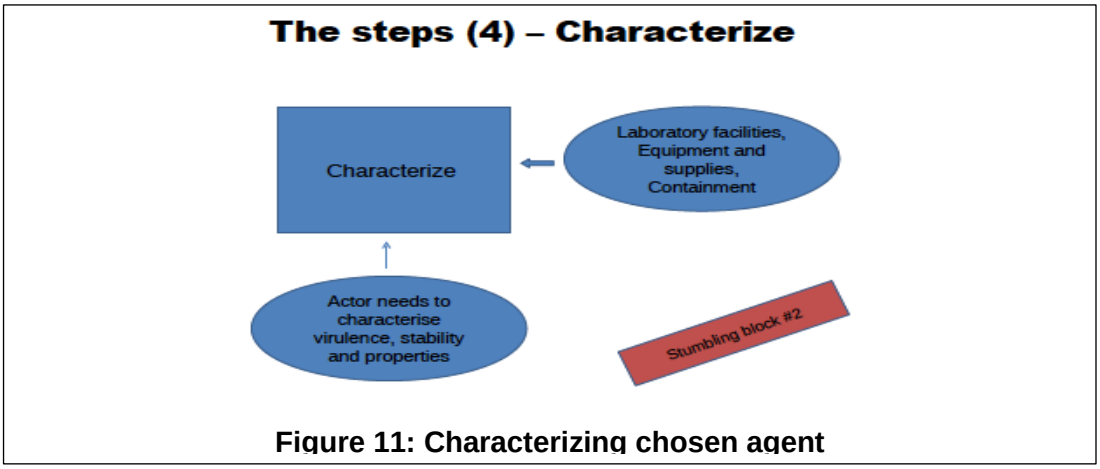


Figure 11: Characterizing chosen agent

Where the state actor will work towards optimization of the chosen strain, the non-state actor's efforts may be hampered by lack of access to really virulent strains, and the lack of ability, time and resources to modify the available strains. In our spore dissemination experiments at the FFI we have assumed an inhalational LD 90 of around 25000 spores, which may be in the region expected from modestly virulent wild-types of *B anthracis*. This gives a 40 cu m effective aerosol using COTS equipment[24]. Finding a better sub-strain, say with an LD 90 of 5000 would increase the effective cloud by a factor of 5 – 8.

However, 25000 is assessed to be good enough for a non-state actor if the intent is to produce mass fear rather than mass casualties.

5.6.10 Isolate, culture and confirm properties

At this step the actor needs to find the actual individual colonies they are using for their effector, the actual seed- stock, and properties like stability of virulence and viability must be re-determined. At this stage the qualitative and quantitative aspects of the final effector are to a very great degree determined. We have assessed the 15 agents the RTG/HFM-186 has chosen, and each stage and step is assigned a numeric value describing how dangerous or suitable an agent is at that step. The numbers from 1 through 9 are negotiable but based on what we could find from textbooks, practical and clinical experience and discussions with colleagues and others. The number 4 denotes neutral, less is difficult or unsuitable, more is easier or suited.

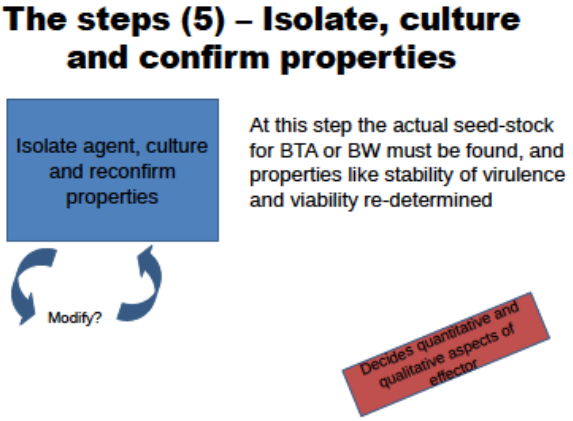


Figure 12: Determining agent properties

[24] FFI (Norwegian Defence Research Establishment) aerosol experiments. Diverse internal reports 2006-2011

GENERIC THREAT ASSESSMENT AND RELATIVE RISK: BIOLOGICAL THREAT AGENTS AND WEAPONS

Table 5.6-3: Evaluation of Agent Properties as Biological Threat Agents (Aerosol Release).

Agent	Avail	ID	Culture	Isolation	Virulence	Stability	EoH	Morb	Mort	TTE	RoE	Modifiable
B. anthracis	9	7	9	6	7	8	7 /3*	9	8	8	7	Y
Botulinum toxin	5	3	7	3	9	5	6	9	7	9	4	–
Y. pestis	5	6	8	6	7	4	4	7	8	9	5	Y
Variola major	1	2	1	1	9	6	6	9	7	6	6	– (?)
F. tularensis	7	5	6	5	6	7	7 /3*	9	5	5	6	?
Ebola VHF	3	4	3	3	4	5	2	7	7	5	2	?
Marburg VHF	2	4	3	3	5	5	4	7	7	6	4	?
B. mallei	3	6	3	4	8	7	4	8	8	4	5	?
B. pseudomallei	6	4	6	4	8	8	4	7	7	4	5	?
C. burnetii	7	4	5	5	6	7	6	6	5	4	5	?
Staph enterotoxin	7	6	7	7	8	8	6	8	5	9	9	Y
R. prowazekii	5	N/A	N/A	N/A	8	N/A	5	9	7	7	6	?
Alphaviruses**	6	4	5	5	8	7	3	8	6	6	7	Y
Ricin toxin	9	5	6	6	8	6	4	8	8	7	5	?
Brucella spp	8	6	4	6	7	7	5	7	5	4	5	?

** As wet or (dry) agent formulation.*

*** VEE, WEE, EEE / Viral encephalitis.*

Explanatory notes: *Effect/suitability is described by numbers 1 to 9, where 1 denotes very difficult/inefficient or unsuited, 9 denotes very easy/highly effective or suited. 4 is neutral. The reference point here is an experienced laboratory-trained microbiologist, an un-schooled person would probably not manage to handle anything rated 4 or less;* ***Availability*** *denotes how easily obtainable the agent is from environmental or laboratory samples or actual cases;* ***ID*** *describes how easily the agent is definitely identified;* ***culture*** *is a description of skills and conditions necessary to culture or produce the agent;* ***isolation*** *is how easily the agent is isolated from a mixed culture;* ***virulence*** *describes the ability of the agent to cause disease when the optimal sub-strain is chosen;* ***stability*** *expresses how well the agent retains its properties with regards to virulence, viability, etc., when cultured in vitro;* ***EoP*** *is "ease of production" throughout the production process resulting in usable quantities of weapons grade agent;* ***EoH*** *or "Ease of Handling" describes the ease with which the agent can be safely handled without loss of properties from production to dissemination;* ***morbidity*** *denotes relative morbidity;* ***mortality*** *denotes relative mortality in the absence of countermeasures;* ***TTE*** *is "Time To Effect" and denotes probability of significant effect within a given time-frame;* ***RoE*** *is "Reliability of Effect" and denotes the probability of a release causing the desired disease-effects, given the constraints imposed by EoH. Finally, modifiable denotes possibility of modifying agent.*

The perceived, public effect is presumed high for all these agents. All values given are estimates based on textbooks, reference texts, practical and clinical experience and discussions with colleagues and others, and are negotiable.

Special note on estimated virulence of VHF: *It has a low value because of very complicated infectious routes both from clinical cases and the environment that are difficult to exploit when used as a biological threat weapon.*

5.6.11 Harvest and store

At this step in the process most of the focus is on viability, and how long the effector retains its properties during production and storage. This needs to be tested and determined. Storage usually degrades the agent unless special precautions are taken, both by autolytic and extraneous influences, but for our generic non-state actor this would be a very short phase, and would represent yet another constraint in that the time from production to use would have to be short. This has an important influence on planning and targeting.

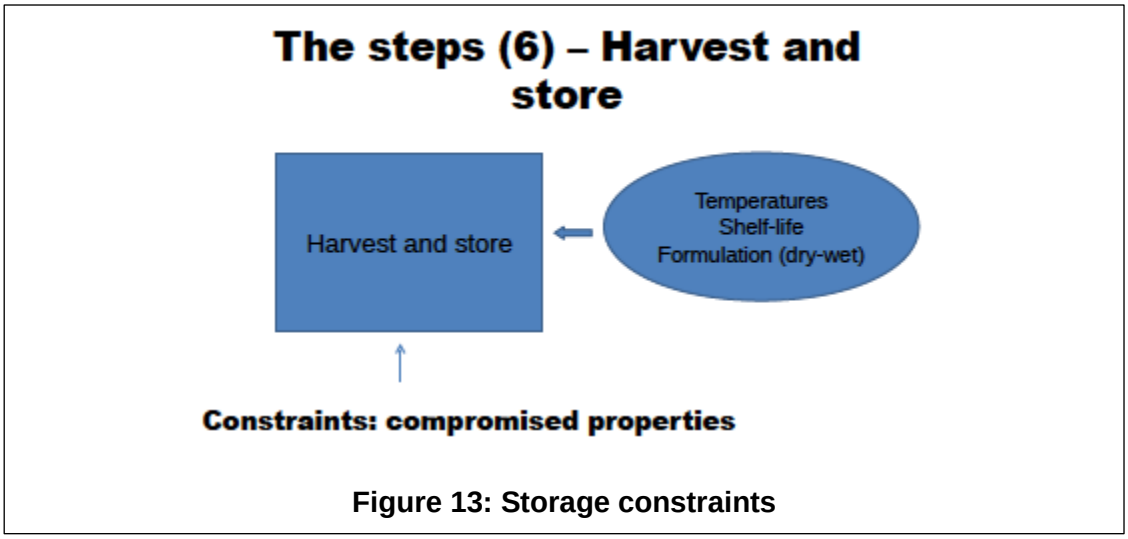


Figure 13: Storage constraints

5.6.12 Weaponization

The next step is the weaponization process. For a state this is a complex process, and continued testing and QA is mandatory, especially with regard to how well the effector retains desired properties in relation to shelf-life and dissemination. This decides the operational efficiency and impact of the effector. During this process protection of the agent from environmental contamination, and also protecting the handlers, is important, and influences the operational impact (RoE). For a non-state actor it is another, crucial constraint, even though the weaponization process itself can be simplified.

Figure 14: Impacting factors on weaponisation

5.6.13 Dissemination and effect

Given targeting within operational constraints, the effect will then be decided by the dissemination method and the quantity and qualities of the agent.

Figure 15: Effect in target

5.6.14 Technical probability – non-state

A non-state actor will experience constraints in time, technology and security that are assessed to lead them to emphasise availability and factors related to finding the effector they want (ID, culturability, isolation, etc.). EoP (Ease of Production) and mortality will also be deciding criteria, and using the table these have been summed to express a technical probability factor. Any agent with a score lower than 4, i.e. neutral, for at least one of these parameters has been relegated to "lower risk". This is based on the thesis that obtaining a result sufficient to provoke attributable fear is the deciding factor in effector production.

The first figure is the sum of Availability+ID+culture+isolation, the added figure is EoP+Mort:

B. anthracis	31 + (7+8)
Staph E tox	27 + (5+5)
R. prowazekii	? but several parameters assessed as below 4; relegated
Ricin	26 + (7+8)
Alphaviruses	20 + (6+6)
Botulinum toxin	Several parameters below,incl EoP; relegated
Variola major	Assessed as very low probability; relegated
F. tularensis	23 + (5+5)
Y. pestis	25 + (5+8)
B. mallei	3 on availability and culture; relegated
B. pseudomallei	0 + (4+7)
Marburg VHF	Several parameters below 4; relegated
Brucella spp	EoP is assessed as 3;relegated
C.burnettii	21 + (4+5)
Ebola VHF	Several parameters below 4; relegated

This leaves eight agents, ranked as follows, followed by estimated effect/consequence (0 – 9) based on probable effector efficiency after successful release (average of TTE (Time To Effect) and RoE (Reliability of Effect):

B. anthracis	31 + (7+8)	est effect:	7.5	HIGH TP (Technical probability)
Ricin	26 + (7+8)	do	6	HIGH TP
Y. pestis	25 + (5+8)	do	7	HIGH TP
Staph Etox	27 + (5+5)	do	9	HIGH TP
F. tularensis	23 + (5+5)	do	5.5	MEDIUM TP
Alphaviruses	20 + (6+6)	do	6.5	MEDIUM TP
B. pseudom	20 + (4+7)	do	4.5	MEDIUM TP
C. burnettii	21 + (4+5)	do	4.5	MEDIUM TP

All these agents have sufficient morbidity or mortality, and though differing in assessed consequence will all satisfy a non-state actor's requirement for an effector.

5.6.15 Technical probability – state

As mentioned, a state actor will focus on the efficiency and reliability of their effectors in a weapons system. This technical probability, given the intent to use, represents the probability of use defined at the start of the document.

Based on the previously shown table, and working out the sums of factors TTE, RoE, morbidity, mortality, and adjusting for availability, we get a list ranking the agents as follows:

B. anthracis	40 (9)	
Staph Etox	39 (7)	
R. prowazekii	36 (5)?	
Ricin	34 (9)	
Alphaviruses	34 (6)	
Botulinum toxin	34 (5)	
Variola major	34 (1)	availability restricts choice until GT is efficient
F. tularensis	32 (7)	
Y. pestis	32 (5)	
B. mallei	32 (3)	
B. pseudomallei	31 (6)	
Marburg VHF	29 (2)	
Brucella spp	28 (8)	
C. burnetii	27 (7)	
Ebola VHF	26 (3)	

Given this ranking we get three obvious sets of agents:

Staphylococcal Enterotoxin, Ricin and Botulinum toxin all come out as high risk in that order.

The remaining agents are assessed to have an availability that precludes them having a higher relative risk than the others.

Comparing the ranking of bacterial, viral and toxin agents with one another is difficult, but generally the technology for mass-producing bacterial agents is more widely known, which may give bacteria and bacterial toxins an advantage.

The possibility of modifying strains to give higher virulence, or transferring plasmids or other genetic elements to change the basic properties of some agents complicates the picture, and must be borne in mind in any evaluation or assessment of biological agent use. The progress in biotechnology will certainly have an impact on the availability of some agents, some of which may be usable in attacks. The fact that some research groups have managed to produce or modify some agents does not, however, mean that these technologies are widely available for immediate use: the work done to achieve these steps is time and resource demanding and is not assessed to be widely available to biological agent producers for some years.

5.6.16 Interplay between targeting, agent choice and intent

> *"Why would Saddam Hussein want to produce aflatoxins as bioweapons? They don't give effects until several years after use, and then as liver cancers…"*
> *ANON*

Ideally an actor would focus on targeting in order to obtain an objective:

- What is to be achieved?
- When must it be achieved?
- What effect is necessary in the target (effect constraints, both upper and lower)?
- Which effector will be suitable to achieve this?

In a conventional setting this is done using the familiar and tested resources available to the war fighter, within overall political and technical constraints imposed on the operation. A terrorist will use guns, flammables and explosives, states will utilise military might (or at least threaten to use it). At a strategic level, the same reasoning is used when developing new weapon systems and types. This would also be valid when states develop unconventional weapons such as those based on a biological effector. In a conflict where biological weapons or terrorism agents are first used, the actual effects will be largely unexplored and add to the complexities in planning and execution. Targeting in the case of non-state actors may visibly be dependent on agent choice which again will influence and modify the objectives that can be reached.

This will impact states less than it will non-state actors due to the difference in resource and time availability. In the interplay between targeting, agent choice and intent the results may appear very uncertain and difficult to envisage both for attacker and defender. In the case of a non-state actor this may be assumed to reinforce their leaning towards agents that are “tried and tested”, and restricts their choice. This will limit their arsenal to threat agents that are seen as easier to produce and procure, and that may not need much testing due to good documentation. This will also simplify defensive preparations in society, with the possibility of giving priority to the most probable threats.

The state actor poses a significantly more complex threat with regard to detection and countermeasures, given a less limited choice of agents with the possibility of modifying or altering them. Technical considerations will, however, probably play an important part here as well, and will, combined with effective and reliable intelligence, make countermeasure prioritization possible.

5.6.17 A final word on consequences

The Health Services in most countries are very capable, but operate at a level that handles day-to-day situations more or less easily, with (possibly) some extra capacity available during the influenza season and the like. Additionally, the health services can usually be mobilised through emergency re-prioritization to provide an emergency capacity in addition to this.

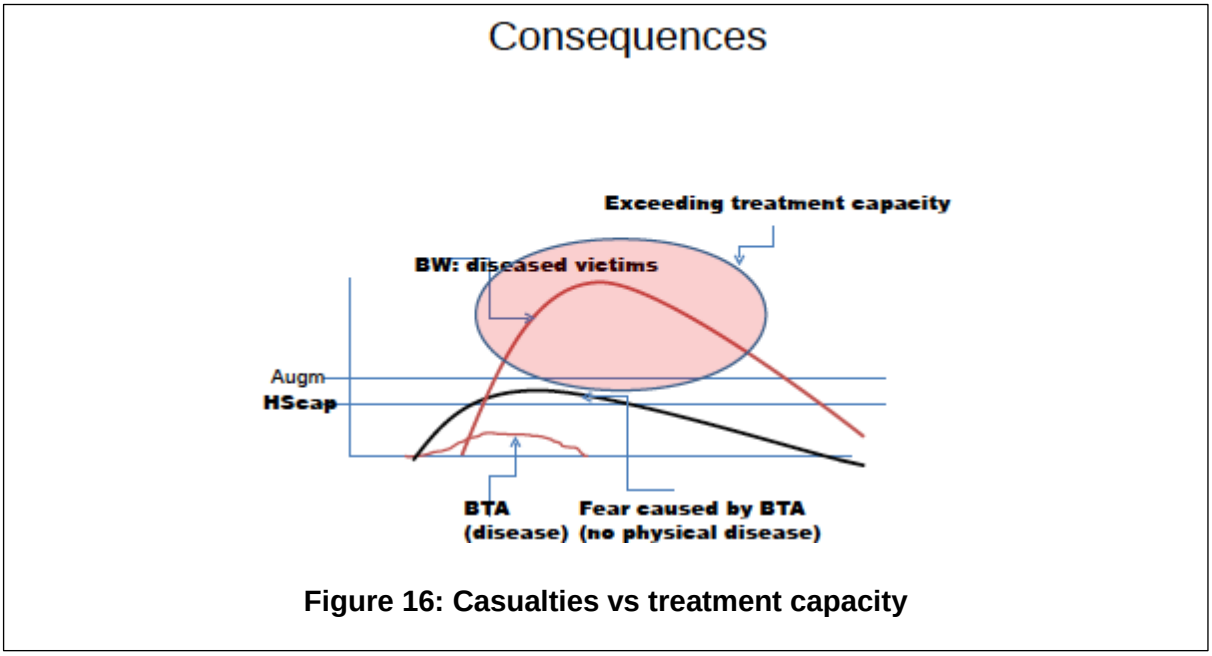


Figure 16: Casualties vs treatment capacity

A non-state actor will rarely, based on the studies we have done at the FFI, be able to cause significant NUMBERS of disease casualties (enough to overwhelm the emergency services) when using BTAs, though the capacity of the primary health services may be overwhelmed due to high numbers of worriers. The primary effect

will be intentionally caused disease striking at will and making individuals targets of a population.

A state attack using biological weapons might leave a very high number of diseased victims, enough to overwhelm the treatment and logistics capacities of any health systems. In practice this will leave a sizeable part of the affected population without necessary access to medical assistance, and leave to the aggressor, through their choice of agent, to decide who lives and dies. The goal of all countermeasures work should be to prevent this from happening.

HScap: Health services medical emergency treatment capacity in a non-epidemic situation. Augm: Capacity following re-prioritization.

The coloured oval denotes the group of casualties outside any possible treatment capacity when you have a time- compressed, enormous number of acutely ill, infectious-disease victims, the kind of consequences a BW attack might entail.

INTENTIONALLY BLANK

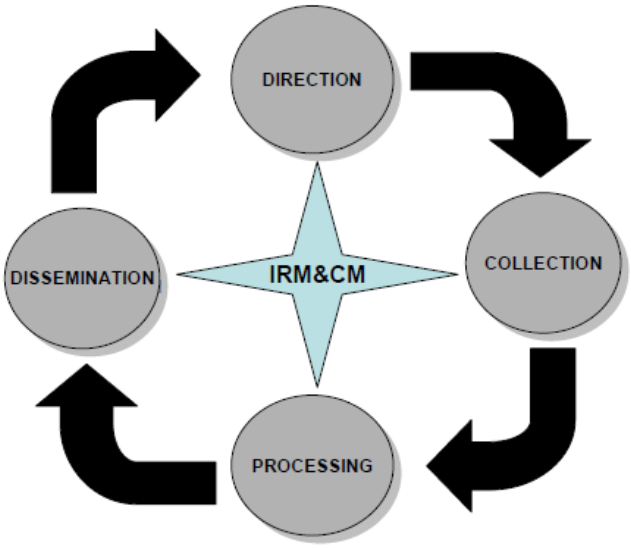
CHAPTER 6 MEDINTEL CYCLE

6.1. THE MEDINTEL CYCLE

The medintel cycle alternatively can:

- contribute to the overall intelligence cycle when medintel assessments are just a subset of the JIPOE;
- represent a stand-alone cycle when only medintel assessments are needed.

As the general intelligence cycle, *medintel cycle is the sequence of activities whereby raw information is obtained, assembled, converted into medical intelligence products and made available for users*.



Even though a medintel organization – according to different national approaches – can reside either in the Intel domain, as well as in the medical domain, the medintel cycle is a methodological approach valuable in both cases.

The cycle consists of 4 core stages, coordinated by a central hub process:

6.2. DIRECTION

Direction encompasses:

- determination of collection requirements,
- defining the collection plan,
- issuing of tasks and requests to collection disciplines, assets and agencies,
- maintenance of a continuous check on the productivity of such capabilities.

Direction is the key to the intelligence process.

6.3. COLLECTION.

Collection is the exploitation of sources by collection agencies/ disciplines / units and the delivery of the information obtained to the appropriate processing unit for use in the production of intelligence.

During the collection phase, the appropriate **JISR assets**, sources and agencies are tasked to collect information.

It encompasses three different phases:

- *screening (collection),*

- *filtering,*
- *validation.*

6.4. PROCESSING.

Processing is defined as the conversion of information into intelligence through collation, evaluation, analysis, integration and interpretation.

Processing is iterative and may generate further requirements for collection before dissemination of the medintel products.

Processing is almost totally based on human judgment, informed by subject-matter expertise and good competency-based networking, representing a critical point in the medical intelligence cycle.

It may be started and fed by the use of **Critical Indicators**.

It is made up of the following 5 steps:

- Collation,
- Evaluation,
- Analysis,
- Integration.

6.5. DISSEMINATION.

Dissemination is defined as the timely conveyance of medintel assessments, in an appropriate form and by any suitable means, to all those who need it.

It must meet security requirements and encompasses a due mechanism for feedback from stakeholders

6.6. MEDINTEL REQUIREMENT MANAGEMENT AND COLLECTION MANAGEMENT (IRM&CM).

It is the hub of the medintel cycle, coordinating the core four stages and ensuring intelligence requirements (IR) are satisfied and the intelligence assets available are focused and prioritized.

It permits best use of collection capabilities.

CHAPTER 7 PITFALLS AND FLAWS IN THE MEDINTEL PROCESS

7.1. INTRODUCTION

Due to the fact that medical intelligence largely is a human process, there is a certain risk that due to this human factor, the result of the medintel may be negatively influenced. These influences can be procedural, perceptional or due to lack of experience. As a rule of thumb, a pitfall or flaw will have bigger consequences when it happens early in the medintel cycle and should be prevented as much as possible.

7.2. PITFALLS AND FLAWS IN THE DIRECTION PHASE

7.2.1 Commander and staff

Medintel products may be partly or on the whole unsatisfactory to support the decision making process when the Information Requirements have not been properly issued by the Commander/staff (or by the Internal Medintel Direction, when proactively engaged) when assessed or selected in relation to the mission.

7.2.2 Direction

Delays or misconception in the prioritization process of Information Requirements during the medintel direction can lead to useless assessments.

To avoid this, the Commanders intent should be clearly understood, next to his critical Intelligence Requirements. When in doubt it is best to ask for additional clarification

7.3. PITFALLS AND FLAWS IN THE COLLECTION PHASE

Errors in the Collection phase may be quantitative (insufficient) or qualitative (inconclusive) or both and can derive from errors in:

1. developing the ICP by the CCIRM,
2. linked to misuse in Indicators,
3. from inaccurate knowledge of information background,
4. mistakes in Indicators exploitation,
5. poor refinement of the ICP,
6. inadequate/improper tasking of collection assets,
7. ineffective work done by the single assets/capabilities.

All these factors of influence can be mitigated with a thoroughly designed ICP. In general, long-term strategic assessments will have time to develop such a thorough plan, whilst at the tactical level time can be extremely limited. Awareness of information gaps is then essential in providing good medintel products.

Information and intelligence can suffer from:

1. misinformation: spread of unintentionally false information, facts, opinions;

disinformation, involving spread of intentionally false information, inaccurate information deliberately spread, such as denial or deception, due to intentional misleading censorship, concealment, manipulation, distortion or falsification of evidence by an adversary, and needs to be accurately evaluated by taking into account source reliability, possible deception motivation or purposes, past patterns, conflicting data.

In order to prevent mis- and disinformation, sources should be cross-referenced with other sources. Especially in news sites, information is often copied from other news sites. Of course, this is not to be called cross-referencing, for these news sites use the same source. Proper cross-referencing comes from at least two different sources, e.g. a news site and a scientific publication or a report from a reliable organisation.

7.4. PITFALLS AND FLAWS IN THE PROCESSING PHASE

In the processing phase, all collected information is analysed and interpreted. This is the phase where pitfalls and flaws are most likely to occur due to the very nature of this phase.

Pitfalls may be linked to:

1. logical fallacies;
2. bias: an error introduced into analysis by favouring one outcome over others due to inclination of temperament or outlook;
3. prejudice: an unreasonable bias consisting in an opinion/judgement held in disregard of contradicting facts or against something without just grounds or before sufficient knowledge. Sometimes it entails collection and exploitation of improbable information/data coherent with the unreasonable model.

There may exist different types of bias or prejudices affecting the INTEL analysis and interpretation, due to different possible factors:

- cultural,
- organizational (hunting for the vertical/superordinate consent)
- institutional,
- ethnicity,
- language,
- nationality,
- political affiliation,
- religion,
- social/census/origin,
- gender,
- age,
- employment,
- institutional affiliation,
- educational,

- hindsight,
- mirror-imaging (the most common cultural pitfall: to impute own behaviours to others)

The list above shows that the background and character of the analyst can be of great influence to the final medintel product. To reduce the degree of bias, following measures can be taken:

- Critical self-awareness,
- The development of more than one hypothesis,
- The use of structured analytic techniques,
- to continue to monitor issues,
- collaboration and peer review (six thinking hats method).

Apart from any pitfalls and flaws, evidence is almost never complete in medintel assessments as they will always involve some degree of uncertainty.

As a matter of facts evidence, even when descending from correct analysis, will suffer from any degree of reliability/credibility, inconclusiveness, ambiguity, dissonance.

It is important to identify the gaps in gap and to assign a confidence level to the medintel assessments in order to better and further refine the collection plan.

Finally, it is important to think “outside the box” in order to break common thinking habits, being aware not to overdo.

7.5. PITFALLS AND FLAWS IN THE DISSEMINATION PHASE

Pitfalls may be due to inappropriate content, time, methods and route of dissemination:

1. missing or ineffective replying to the customer’s requirements;
2. delay in issuing the assessments;
3. unavailability to the proper end user.

This of course depends on a number of factors, such as:

1. Formulation of information requirements
2. development of the ICP
3. an adequate and consistent RFI development
4. adequate RFI management

INTENTIONALLY BLANK

CHAPTER 8 LESSONS LEARNED IN MEDICAL INTELLIGENCE

8.1. INTRODUCTION

Lessons Learned can be derived from any activity including the medintel discipline and the procedure can be applied in any phase of its cycle.

Lessons Learned (LL) describes activities relating to learning from experience to achieve improvements. In the medintel discipline, this means increased efficiency, and improved operational effectiveness through development of proper and timely assessment

The key factor of LL is the chance of doing things in a more easy and convenient way by using shared knowledge.

True organizational learning in medintel only takes place when driven by leaders in the Medical and in the Intel domains.

Leaders' LL guidance and engagement must be evidenced not only by words.

8.2. THE LESSONS LEARNED PROCESS

A NATO Lesson Learned results from the implementation and validation of a remedial action that produced an improved performance or increased capability.

LL is based upon three stages:

1. Lessons identification (LI): to collect learning from experiences.

2. Action: to amend existing ways of doing things based on the learning.

3. Institutionalization: Lesson sharing and, as applicable, incorporation into NATO doctrine and procedures. That means that lessons sharing have to be performed via websites, databases and for medintel organizations, via reports or newsletters.

Everyone in an organization has a responsibility for learning lessons and everyone needs to see the value of learning lessons.

8.3. PHASES OF THE LESSONS LEARNED PROCESS

Although the Lessons Learned cycle is a continuous it is not difficult to see where the cycle starts. From there the whole process will be set in motion.

8.3.1 Capturing Observations

The starting block for the process is the identification of differences between expectations and actual performance by gathering observations

Provisions should be in place for all personnel regardless of rank or branch to document observed problems, shortfalls and successes in order to report any observation by attaching their name or keeping the desired anonymity, only tracing the belonging to an appropriate branch or unit.

Post-event reports are an ideal source for observations and should become a part of the knowledge base for the next event's planners to use.

Observations concerning medintel may be peculiar to any items, products or phase/step of the medintel cycle.

Methods for collecting observations should be as simple as possible and should complement procedures for processing and sharing lessons.

They may be originated outside or inside the medintel organization.

Medintel feedback forms may represent a useful tool to capture external observations from the stakeholders.

The NATO Medintel forum on the website or on BICES may represent the proper sites where to share and manage international observations of possible common interest.

Medintel periodical staff meetings may represent the proper forum where to share internal observations.

8.3.2 Managing Observations

Observations should be reviewed as soon as possible after capture to select out unsuitable observations and allow for the capture of additional information.

From the start of the process, attach metadata to the observations. Metadata will make finding and subsequently sharing information easier.

8.3.3 Lesson Identification and Learning

In order to transition an observation into an LI, analysis of observations must be conducted to determine:

- root causes,
- remedial actions,
- the appropriate action body (internal and/or external to the medintel organization) to execute the action.

The Medintel Leader will review LIs to determine how to proceed with the LL process.

The techniques used for analysis will vary and depend on each individual LL process and roughly can rely upon a deductive or, alternatively, on an inductive-approach.

The results of analysis are to be documented LIs that are ready to be taken into the next step in the LL process.

This process can be fully performed within the medintel organization or may involve external responsibilities or commitment, as the appropriate level of leadership needs to be involved to endorse the lesson, task the Action Body and finally validate the lesson.

Additionally, the Remedial Action is a project which needs to be planned, managed, and resourced in order to be successful.

8.4. SHARING LESSONS LEARNED

Sharing knowledge improves organizational and individual performance and proper information management should help to overcome concerns regarding sharing.

Information can be shared at any time, as long as it is clear what level of quality it has, but sharing should start early in the LL process and be sustained during the entire process.

Medintel Lessons can be a valuable input not only to the medintel organization and process but also to operations and exercise planning processes, as well as to training, and therefore target audience are:

- operational and exercise planners;
- trainers.

In the medintel domain the emphasis on “responsibility-to-share” should be balanced with the security principle of “need-to-know”.

Consideration needs to be given to the *pushing* and *pulling* of information.

Pushing actively sends out new information to individuals as it becomes available.

Pulling requires individuals to regularly check to see if new information is available.

Information may be shared within the NATO medintel community via web EP’s forum, meetings and direct communications.

Medintel LL may be incorporated into NATO LL process by forwarding observations (using the ODCR form attached to the ACO 80-1 Directive) or sending LI proposals to the NATO LL organization.

In NATO, tools that support the sharing of lessons and information include databases, for example the NATO Lessons Learned Database and knowledge repositories such as wikis and blogs.

ANNEX A GLOSSARY OF ABBREVIATIONS

ACINT	Accoustic intelligence
BICES	Battlefield Intelligence Collection and Exchange System
CBRN	Chemical, biological, radiological, nuclear
CCIR	Commanders Critical Information Requirements
CCU	Coronary Care Unit
CONOPS	Concept of Operations
CPOE	Comprehensive Preparation of the Operational Environment
CT scan	Computed tomography scan
EP	Environmental Protection
FHP	Force Health Protection
ICP	Intelligence Collection Plan
ICU	Intensive Care Unit
IMINT	Imagery Intelligence
IO	international Organisation
IPB	Intelligence Preparation of the Battlefield
GIS	Geographical information Systems
GO	Government Organisation
HUMINT	Intelligence derived from human sources
KD	Knowledge Development
LI	Lessons Identified
LL	Lessons Learned
LLDb	Lessons Learned Database

Medintel	Medical Intelligence
NATO	North Atlantic Treaty Organisation
NGO	Non-Government Organisation
NMR scan	Nuclear Magnetic Resonance scan
ODCR	Observation, Discussion, Conclusion, Recommendation
OPP	Operational Planning Process
PET scan	Positron emission tomography scan
PIR	Priority Information Requirement
RFI	Request for Information
SIGINT	Signal intelligence
SME	Subject Matter Expert
TELINT	Telemetry intelligence
WMD	Weapons of Mass Destruction

ANNEX B INTELLIGENCE TERMS

Source Reliability

Ref: Annex A to STANAG 2511

Reliability of the source is designated by a letter between A and F signifying various degrees of confidence"

A. Completely reliable
B. Usually reliable
C. Fairly reliable
D. Not usually reliable
E. Unreliable
F. Reliability cannot be judged

Completely reliable (A):	Refers to a tried and trusted source which can be depended upon with confidence.
Usually reliable (B):	Refers to a source which has been successful in the past but for which there is still some element of doubt in a particular case.
Fairly reliable (C):	Refers to a source which has occasionally been used in the past and upon which some degree of confidence can be based.
Not usually reliable (D):	Refers to a source which has been used in the past but has proved more often than not unreliable.
Unreliable (E):	Refers to a source which has been used in the past and proved unworthy of any confidence.
Reliability cannot be judged (F):	Refers to a source which has not been used in the past.

Source Credibility

Ref: Annex A to STANAG 2511

"Credibility of information is designated by a numeral between 1 and 6 signifying varying degrees of confidence"

1 Confirmed by other sources
2 Probably true
3 Possibly true
4 Doubtful
5 Improbable
6 Truth cannot be judged

Confirmed by other sources: If it can be stated with certainty that the reported information originates from another source than the already existing information on the same subject, it is classified as "confirmed by other sources" and is rated "1"

Probably true: If the independence of the source of any item or information cannot be guaranteed, but if, from the quantity and quality of previous reports its likelihood is nevertheless regarded as sufficiently established, then the information should be classified as "probably true" and given a rating of "2".

Possibly true: If, despite there being insufficient conformation to establish any higher degree of likelihood, a freshly reported item of information does not conflict with the previously reported behaviour item of the target, the item may be classified as "possibly true" and given a rating of "3".

Doubtful: An item of information which tends to conflict with the previously reported or established behaviour pattern of an intelligence target should be classified as "doubtful" and given a rating of "4".

Improbable: An item of information which positively contradicts previously reported information or conflicts with the established behaviour pattern of an intelligence target in a marked degree should be classified as "improbable" and given a rating of "5".

Truth cannot be judged: Any freshly reported item of information which provides no basis for comparison with any known behaviour pattern of a target must be classified as "truth cannot be judged" and given a rating of "6". Such a rating should only be given when the accurate use of a higher rating is impossible.

Source Evaluation Rating

Ref: Annex A to STANAG 2511

Reliability and credibility, the two aspects of evaluation, must be considered independently of each other. The resultant rating will be expressed in whatever combination or letter and number is appropriate. Thus, information received from a “usually reliable” source which is assessed as “probably true” will be rated “B2”. Information from the same source of which “the truth cannot be judged” will be rated as “B6”.

Intelligence Assessments: Statements of Likeliness

Source: USA DIA

An important part of an intelligence analysis is the expression of the likeliness that the assessed event or development will or will not occur. Probabilistic language is used to express the likelihood. Most of these terms do not convey a precise numeric probability, and in common language, some are interpreted to cover a broad range of probability. They can be conceptualized as a rough hierarchy, ranging from “will not” (0 % probability) to “is certain” (100 % probability):

Probability	Verbal Expression
100 %	Will
	Is Certain Almost Certain
	Highly/Very Probable Extremely Likely Highly Likely
	Probable Likely
50 %	Even Chance
	Unlikely Low Probability Probably Not
	Very Improbable Very Unlikely
	Highly Unlikely Extremely Unlikely
	Little Prospect Remote
0 %	No prospect Will not

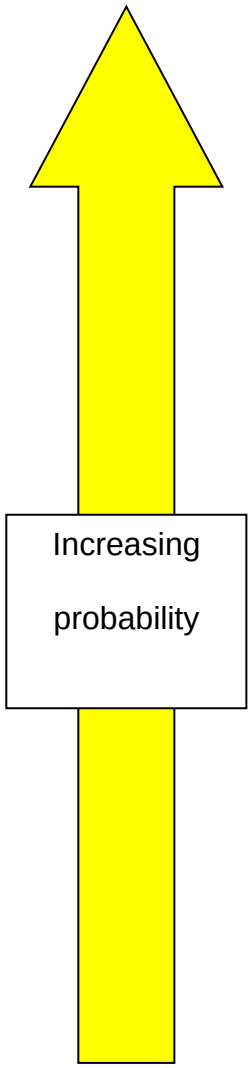


Figure 17: Expressions of Likeliness

Expressing Analytical Confidence

Source: USA DIA

Analytical confidence is not an expression of an individual's personal belief that a judgement is correct, not is it a measure of the likeliness that the event will occur in the future. Confidence in an assessment is a judgement based on three factors:

a. the strength of the knowledge base, including the quality of the sources and depth of understanding about the issue;

b. the number and importance of the assumptions used to fill the information gaps; and

c. the strength of the logic underpinning the argument, which encompasses the number and strength of analytic inferences as well as the rigor of the analytic methodology in the product.

Note: Confidence level in an intelligence assessment is a qualitative judgement that should not be confused with quantitative confidence levels in statistics and epidemiology.

	Criteria for Justification
Complete Confidence	Totally reliable and corroborated information with no assumptions and clear, undisputed reasoning.
High Confidence	Well-corroborated information from proven sources, minimal assumptions, and/or strong logical inferences.
Moderate Confidence	Partially corroborated information from good sources, several assumptions, and/or a mixture of strong and weak inferences
Low Confidence	Uncorroborated information from good or marginal sources, many assumptions, and/or mostly weak inferences.

Table 8.4-1: Confidence Levels

INTENTIONALLY BLANK

ANNEX C EXAMPLE LIST OF INFORMATION REQUIREMENTS ON ENVIRONMENTAL ISSUES

(SWE)

Issues to consider in strategic environmental and/or conflict related intelligence assessments include, but are not restricted to;

1) Environmental Key Concerns

- What are the main environmental challenges facing the region and country (e.g. climate change, deforestation, extreme weather events, industrial pollution)?
- Are there transnational environmental concerns or conflicts?

2) Environment and conflict/crime relations:

• Is there conflict or crisis in the region that are linked to environmental factors such as natural resources scarcity/abundance, environmental degradation or climate change? If so; how, and to what extent?
• Are the key natural resources scarce or in abundance or scarce?
• What foreign investments in natural resources exist, e.g. mineral resources or land?
• Is infrastructure such as oil fields or hydropower dams used as targets or sources of funding for insurgents?
• Is organized crime connected to any natural resources, .e.g. does wildlife crime or trafficking in cultural objects occurs?
• Is there transparency in governmental expenditures?
• What is the level of corruption?
• Is corruption affecting key environmental issues or natural resources management?

3) Institutional capacity and legal framework:

• What environmental legislation, multinational environmental agreements, customary laws, or sending-nation environmental regulations are applicable?
• Are there procedures for Environmental Impact Assessment (EIA) in place
• Does the receiving nation have implementation capacity for the legislation that exist?
• Does the receiving nation have environmental infrastructure such as water or waste-management facilities? If so, are they operational?
• Does the receiving nation have environmental monitoring programs of air, soil or water? If so, where and what is measured?

4) Natural resources and environmental changes:

Environmental trends:

- What is the current and predicted future state of the environment and natural resources?
- What are the main relevant ongoing processes of change?

Climate and extreme weather:

- What are the main climatic characteristics of the region?
- What are the type, magnitude, and frequency of extreme weather events?
- What are the main climate change trends and what are the predicted main concerns regarding future climate changes?

Air quality

- What are the main sources of air pollution

Water:

- What are the hydrological characteristics of the region?
- What are the total natural water withdrawal and recharge rates?

Land and soil:

- Does the region suffer from land and soil degradation?
- What is the current land uses, e.g. agriculture, industrial use?
- Are there any pollution hotspots?

Oil, minerals, and mining:

- Does commercial mining or oil extraction take place?
- Are there reserves of minerals or oil in the region that have not yet been explored?

Energy:

- What energy production and consumption patterns exist?
- What is the status of the electrical grid?

Forests:

- How much land is covered by forest?[25]
- What types of forest are there and how are the forests used?
- Does the region suffer from deforestation? If so; to what extent?

Agriculture

- What kind of agricultural activities takes place?

---

[25] the Convention on International Trade in Endangered Species of Wild Fauna and Flora, ses http://www.cites.org/

- To what extent is pesticides and other agrichemicals used

Biodiversity and wildlife:

- What is the status of the terrestrial and marine environments?
- Are there protected or endangered species in the region?
- If so, are there fauna and flora included in Appendices to the CITES convention?
- Is wildlife such as elephants, targeted andused as sources of funding for insurgents?

5) Cultural and historical resources and heritage:

- What cultural and historical sites of significance exist (e.g. UNESCO World Heritage sites, grave yards, spiritual or sacred environments)?
- What key cultural practices exist nationally, regionally, and locally?
- Is cultural or historical used as targets or sources of funding for insurgents?

6) Socioeconomic and livelihood issues:

- What main livelihoods are permanently or temporarily pursued in the region?
- What are the main socioeconomic trends and their critical characteristics?
- What demography, urbanization, and migration patterns exist?
- What sectors and areas are undergoing rapid expansion?
- What is the situation with respect to gender?
- What is the nutritional status of the population?
- How vulnerable is the area to food insecurity?

INTENTIONALLY BLANK

ANNEX D LAWS OF ARMED CONFLICT (LOAC) THE GENEVA CONVENTIONS (GC)

(CHE)

Background

The 1949 Geneva Conventions relating to the Protection of Victims of Armed Conflicts consists of four agreements:

The first Geneva Convention protects the wounded and sick soldiers on land.

The second Geneva Convention protects the wounded, sick and shipwrecked at sea.

The third Geneva Convention applies to prisoners of war (PoW).

The fourth Geneva Convention affords protection to civilians, including in occupied territories.

The 1949 Geneva Conventions (GC) are universally ratified with 194 State / Parties. The GC are supplemented by two Additional Protocols of 1977: The first Additional Protocol further develops the protection of victims of international armed conflicts. In particular, this protocol extends the same protection granted to armed forces medical personnel, to civilian medical personnel. The second Additional Protocol protects victims of non-international armed conflicts, supplementing the rudimentary protection afforded by Common Article 3 of the 1949 Conventions.

Protected personnel and cessation of protection

The Geneva Conventions and their Additional Protocols aim at protecting people who are not taking part in the hostilities (civilians, health workers and aid workers) and those who are no longer participating in the hostilities, such as wounded, sick and shipwrecked soldiers and prisoners of war. Therefore, dedicated medical personnel of the armed forces benefits from the protection afforded by the Geneva Conventions and their Additional Protocols. In particular, medical personnel and facilities of the armed forces are not to be attacked and if captured, medical personnel of the armed forces are not considered prisoners of war. However, pursuant to Geneva Conventions and their Additional Protocols, the protection ceases if the medical personnel commits acts harmful to the enemy outside their humanitarian function. In other words, medical personnel must refrain from all interference, direct or indirect, in military operations.

Medical Intelligence personnel and protection of the Geneva Convention

The work of the Medical Intelligence personnel is particularly challenging. Being a protected Medical Personnel they have to act according to the Geneva Conventions. Renouncement of the rights secured by the convention is not possible. Medical Intelligence personnel shall strictly follow the intention of the Geneva Conventions and act accordingly regardless if they wear a distinctive emblem and/or carry an ID card. However, the co-operation in the intelligence community may lead to dilemmas.

Dilemmas of the Medical Intelligence personnel regarding the Geneva Convention

While the intelligence officer may use his information to achieve the goals (e.g. defeat the enemy), the Medical Intelligence officer always has to consider if use of his information would lead to harmful acts. These situations are often not clear at first sight, e.g. Medical Intelligence staff may have information about the enemy's medical capabilities. This information can be misused to limit the enemy's capability to provide medical care to his own forces. Ethical dilemmas sometimes even go beyond the Geneva Conventions, e.g. Medical teams which treat sick and wounded enemy combatants or civilians or medical patrols may gather information by doing their duty. The Medical Intelligence staff has to consider carefully how such information should be used. Use of this information may lead to negative impact on the future work. Medical teams may no longer be allowed to treat civilians or it can even bring them in danger.

Therefore, the Medical Intelligence officer has to meet high moral and ethical standards when dealing with collection and dissemination of information.

ANNEX E GENERAL TEMPLATE BASIC MEDINTEL PRODUCT

The general template used in the medintel experiment

MEDINTEL

DTG: 261240Baug11

ANYLAND
Mission?

POC:

I. EXECUTIVE SUMMARY

I.1 Subject/Issue:
This product is tailored to a specific operational scenario. For operations with different time or space parameters or with a different operational mission, the conclusion, assessment and derived recommendations may vary.

1. Key Takeaway:	•
2. Background:	•
3. Discussion:	•

I.2 Summary conclusion / assessment of the health risk situation in the above operational scenario (paragraph format):

"SO WHAT?"

	Threat/ unmitigated risk	General recommendations:	Risk/ Mitigated risk	Specific recommendations (by FHP):
Infectious Diseases humans/animals:				
Environmental Health / CBRN:				
Medical Capabilities/ Infrastructure:				
Other health hazards:				

II. Infectious diseases

II.1. Vector insects 	SITUATION IN THEATER (legend)		THREAT ASSESSMENT (UNMITIGATED RISK)	GENERAL CONSIDERATIONS	RISK ASSESSMENT (MITIGATED RISK)	CONSIDERATIONS Specific (to be identified by FHP)
	General	Current		Exposition prophylaxis Chemoprophylaxis		

III. Environmental Health

	SITUATION IN THEATER (legend)		THREAT ASSESSMENT (UNMITIGATED RISK	GENERAL CONSIDERATIONS	RISK ASSESSMENT (MITIGATED RISK)	CONSIDERATIONS Specific (to be identified by FHP)
	General	Current				
Climate						
Air						
Soil						
Water						
Traffic						
Poisonous animals						
Hazardous facilities/objects: • Waste disposals Toxic industrial materials (TIM) • Toxic industrial chemicals (TIC) • Toxic industrial biologicals (TIB) • Toxic industrial radionuclides (TIR)						

IV. Medical capabilities & infrastructure

FACILITIES	SITUATION IN THEATER (legend)		Summary of the capability (STANAG 2481)
Nationality Name Address Contact details	Profile • Hygiene • Equipment • Specialists • Staff • Beds • Helipad • Ambulance • Blood supply • Pharmacy • Laboratory • Standards • Summary:	Evaluation	

SRD-1 TO AJMedP-3(A)(1)