INTERPOL

For official use only

Bioterrorism Incident Pre-Planning & Response Guide

2nd Edition – 2010
INTERPOL Bioterrorism Prevention Programme

ACKNOWLEDGMENTS

ICPO-INTERPOL gratefully acknowledges the technical advice and contributions provided for this guide by experts from the following agencies:

- Australian Chemical, Biological, Radiological and Nuclear Data Centre, Australian Federal Police
- New South Wales Police Force, Forensic Science Services Branch, Australia
- Robert Koch Institute, Germany
- United Kingdom Metropolitan Police Service
- United Kingdom Centre for the Protection of National Infrastructure
- United States Centers for Disease Control and Prevention
- United States Federal Bureau of Investigation
- United States Sandia National Laboratories International Biological Threat Reduction
- World Health Organization

Table of contents

Foreword

The threat of bioterrorism is real and one that we, at INTERPOL, take seriously. The damage caused by a biological attack could reach an untold magnitude, causing wide-scale illness and death, and instilling fear and panic in whole populations.

Terrorists continue to attempt to build up their capacity to produce and deploy bio-weapons. The risk is evolving with the rise of the Internet and the increasing availability of data on obtaining materials and assembling weapons. Clearly, the need for structured prevention and response strategies – for the law enforcement community and beyond – is more critical than ever.

In response to these growing threats, we launched the INTERPOL Bioterrorism Prevention Programme six years ago as the world's first global resource for the exchange of information and expertise in this area.

This Bioterrorism Incident Pre-Planning and Response Guide is a key output of the Programme. Now in its second edition, this comprehensive Guide covers topics as diverse as legislation and media management, and contains expanded information on how to conduct a forensic investigation in a bioterrorism-related case. In addition to our resource centre, data-sharing systems and the production of this Guide, INTERPOL delivers hands-on training sessions for investigators and first responders.

In the event our worst fears are ever realized, law enforcement could not, and should not, shoulder the response alone. A comprehensive approach would need to be co-ordinated among numerous bodies and agencies, including customs, border control, public health professionals, the military, intelligence services and environmental

management. I therefore urge all of you to work with us in putting in place the inter-agency procedures and practices that are necessary to effectively respond to a bioterrorist attack and, more importantly, to prevent any such attacks in the first place.

This manual is the product of contributions from experts from numerous countries and fields and from other international organizations. Not only would I like to thank everyone who was involved in the production of this Guide, but I would also like to applaud the spirit of international and cross-sector co-operation which has helped make this detailed reference manual such a valuable resource. Finally, without the generous support of the Sloan Foundation, none of our work in this important area would be possible.

Ronald K. Noble
INTERPOL Secretary General

I. INTRODUCTION

1. Who should read this guide?

This guide is intended primarily for law enforcement and other entities which can play a role in bioterrorism preparedness and response, and which possess a limited-to-basic knowledge base of CBRNE (chemical-biological-radiological-nuclear-explosives) matters.

The guide serves as a reference document and can be used as a menu of options, in combination with other relevant documents and/or policies used in a national and international setting.

2. What is CBRNE and how does bioterrorism fit in?

CBRNE is the common abbreviation for "**Chemical, Biological, Radiological, Nuclear and Explosives**". Although the potential presence of explosives, chemicals or radiological agents cannot be ruled out as part of routine CBRNE threat investigations, **this guide does not contain specific information regarding chemical, radiological, nuclear or explosives incidents.** However, it is important to look at bioterrorism in the framework of the possible threats that occur within the CBRNE spectrum. Many countries have general contingency planning for CBRNE incidents and have specific protocols in place to deal with each element of this spectrum. It is important to stress that a bioterrorist attack cannot be dealt with using an all-hazards approach. Bioterrorism has special, unique aspects which must be carefully considered when planning any preventive or response strategy.

3. What is bioterrorism?

It is helpful to define bioterrorism in order to be able to identify appropriate measures and planning. A suggested definition of bioterrorism is:

> "Bioterrorism refers to the intentional release of biological agents or toxins for the purpose of harming or killing humans, animals or plants with the intent to intimidate or coerce a government or civilian population to further political or social objectives."

Biohazard packaging. © INTERPOL

4. Why is bioterrorism a challenge for the law enforcement community?

Recent trends in terrorist attacks indicate that terrorists often favour mass-casualty incidents. The relative ease of acquisition of biological agents and their effectiveness as a weapon to instil fear make their use a natural evolution of terrorism. There have been numerous historical events involving the use or threatened use of toxins and pathogens. In recent times, a number of individuals and terrorist organizations have expressed interest in, or attempted to acquire, biological pathogens and toxins.

Bioterrorism poses many challenges for the law enforcement community. There is potential for terrorists to select agents that can be manipulated and dispersed to affect either a single person or up to hundreds or thousands of individuals. The impact of this form of terror may span jurisdictions or nations, requiring co-ordinated communication and investigative efforts across national borders. A large portion of the public could feel that they or their families have been exposed and forcefully demand health care and medications, thus requiring law enforcement to position themselves at hospitals, medical clinics and pharmacies. Quarantine enforcement would likely become a responsibility of law enforcement services as well.

The development of the bio-sciences is continuing daily and brings immense positive social, economic and health benefits to our society. However, their development may also provide terrorists with the opportunity to seek to misuse them. This is a challenge for law enforcement (and the scientific community) and is often referred to as the "dual use" dilemma.

Planning for the health care of law enforcement officers and their families must be given high priority within the overall law enforcement strategy.

Bioterrorism is different from many other types of terrorist act. Traditionally, law enforcement agencies plan and exercise extensively for responses to "overt" acts of terrorism such as bombings, hostage-takings and assassinations. While acts of bioterrorism may be overt, enabling law enforcement to respond traditionally, unique challenges arise when individuals or groups use biological agents covertly. Because biological agents are not generally detected by the senses, and the time from exposure to onset of illness may vary from days to a few weeks, perpetrators may be attracted to this form of crime as they have plenty of time to flee the "scene".

Covert incidents will be detected primarily by medical and public health authorities. Law enforcement services cannot deal with instances of bioterrorism on their own. It is crucial that agreements be put in place and regularly exercised between law enforcement and partner agencies outlining their respective or co-operative roles in dealing with a biological attack. For example, the ability to share information legally between law enforcement agencies and the health community is a key aspect of preparation and contingency planning. *(For the definition of covert and overt attacks please refer to Chapter II.5., page 43)*.

Law enforcement officers who respond to a potential bioterrorism event must do so within the limitations of their training, support network and equipment. Personal safety is a primary concern.

Hospital entrance. © Shutterstock

5. What makes bioterrorism a threat?

The actual threat of bioterrorism is present, but few countries have assessed the threat as being high. In case of an attack, the consequences will be significant.

Bioterrorism has become one of the major challenges of the 21st century, even though biological warfare itself is as old as the human race. Historically, there have been many attempts to initiate the spread of infectious diseases: micro-organisms or toxins of micro-organisms were used as weapons unleashed on select groups of people such as the armed forces (for instance, in the Middle Ages, the bodies of plague victims would be thrown over city walls to discourage advancing enemy armies). However, only recently has this become a threat to civilian populations. Bioterrorism may be aimed at a civilian target, and biological weapons may be spread or biological agents deliberately released in a number of ways.

The initiators of biological attacks may be from a variety of backgrounds. They range from States, terrorist groups supported by the State, transnational organizations, independent political or religious sects (e.g. the Rajneeshee group in Oregon, United States of America), to terrorist groups or individuals (sometimes called "lone wolves").

Bioterrorism is especially threatening precisely due to its clandestine nature. Even if this kind of terrorism is not easily visible, it can be devastating in nature and difficult to cope with for a variety of reasons. Most significantly, terrorist groups rarely claim responsibility for these acts, as is the case with other types of attack.

The impact on a large population from a biological contagious agent would be devastating. © Shutterstock

Thus, if the attack is covert, it may take a while before it is detected. A large number of sick people with similar symptoms and/or the presence of an unusual infection may indicate that a bio-weapon has been used.

The effects of the attack will be visible on a number of levels:

- **Physical** - actual diseases
- **Psychological** - fear, mass panic
- **Economic** - travel restrictions, business shut-down
- **Environmental** – visible on humans, animals, plants.

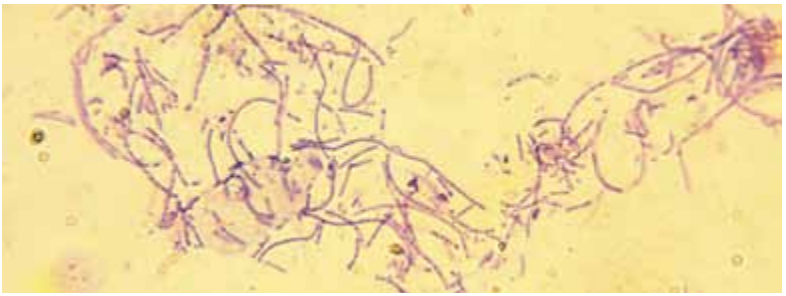
6. What are biological agents?

Biological agents include pathogens, pests and toxins that can be used for legitimate or illegitimate purposes. Pathogens are disease-causing organisms, including bacteria, viruses and fungi. Pests can include insects, worms and plants. Toxins are poisonous substances produced by living organisms.

Biological agents have different properties, depending on the characteristics of each agent. It is important to be able to understand these differences when responding to a bioterrorism incident. Agents can be grouped into the following clusters.

BACTERIA

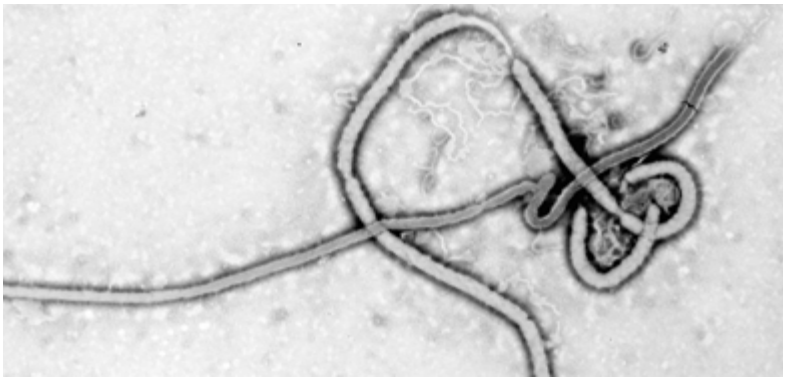
Bacteria are single-celled organisms and their many types can be found everywhere in nature; however, only certain types are pathogenic. Bacteria can infect almost any multi-cellular organism, including humans, animals, plants and insects. Some bacteria can spread from host to host and cause contagious diseases, while others are non-contagious. Certain bacteria require a host cell to replicate, whereas others can replicate outside a host. During times of stress such as low nutrient availability and drought, some bacteria can form a dormant, non-replicating spore that can survive in the environment for extended periods of time (months or years).



Bacillus anthracis, the bacteria responsible for anthrax. © Shutterstock

VIRUSES

Viruses are infectious micro-organisms that are unable to replicate outside a host cell. Different viruses can infect humans, animals, plants and bacteria. They usually target specific species but certain viruses can also be transferred between different species. Viruses can spread from host to host and can cause contagious diseases.



Ebola virus.

TOXINS

Biological toxins are poisonous substances produced by living organisms, including plants, animals or micro-organisms. Toxins cannot spread between organisms and do not cause contagious disease.

Due to the different properties of bacteria, viruses and toxins, they may act differently if intentionally released. Diseases caused by bacteria and viruses have incubation periods: this is the period before disease symptoms appear. During this time, the small numbers of the organism that initially infect the host multiply to larger numbers that cause the pathogenic effect on the host. The incubation period can range from a few days to several weeks. Toxins do not replicate; there is therefore no incubation period and symptoms can appear within hours to days.

There are different treatments for bacteria, viruses and toxins. Bacterial infections can be treated with specific antibiotic therapy; however, some bacteria have developed antibiotic resistance. Prophylactic vaccines are available for several bacterial diseases. Viruses are not susceptible to antibiotic treatment. There are antiviral therapies that can be used to treat some viral infections and vaccines are available for prophylactic use against some viruses. Antibiotics and antivirals are not effective against toxins. Some antitoxins and vaccines are available for specific toxins. Supportive therapy is treatment that is used to treat the symptoms of the disease rather than the agents themselves; such therapy can be used in addition to specific treatment or if there is no treatment available.

Castor beans, which can be used to make ricin. © Australian Federal Police

Castor bean seeds. © Australian Federal Police

BOX 01

EXAMPLES OF BIOLOGICAL AGENTS

Bacterial agents (disease)

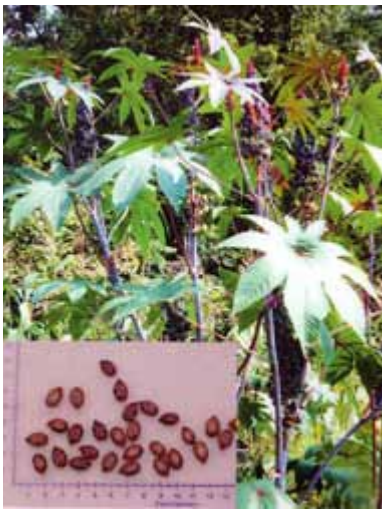
- *Bacillus anthracis* (anthrax)
- *Yersinia pestis* (plague)
- *Francisella tularensis* (tularemia)

Viral agents (disease)

- Foot-and-mouth disease virus (foot-and-mouth disease)
- *Variola major* virus (smallpox)
- Marburg virus and Ebola virus (hemorrhagic fever)

Toxins (source)

- Botulinum Toxin (from *Clostridium botulinum*)
- Ricin (from castor beans)



Castor bean plant.
© FBI and NCTC-USA

Wool containing *Bacillus anthracis*.
© Robert Koch Institute

Biological agents can be used to target humans, animals or crops (this last use is known as agroterrorism). The agents can be used in large-scale or small-scale attacks to kill or incapacitate, or in assassinations.
Biological agents can enter the body by various modes, depending on the agent's properties:

- **Inhalation** – entry into the lungs. Inhalation is often considered the most desired route for a bioterrorist attack. For an agent to enter the body through inhalation, it would have to be released by aerosolization.

- **Ingestion** – from food or water which contaminates the gastrointestinal tract.

- **Absorption** – intact skin acts as a barrier to infection. Micro-organisms can enter through cuts or abrasions, or through the mucus membranes, such as the eyes.

- **Injection** – through hypodermic syringe or projectile.

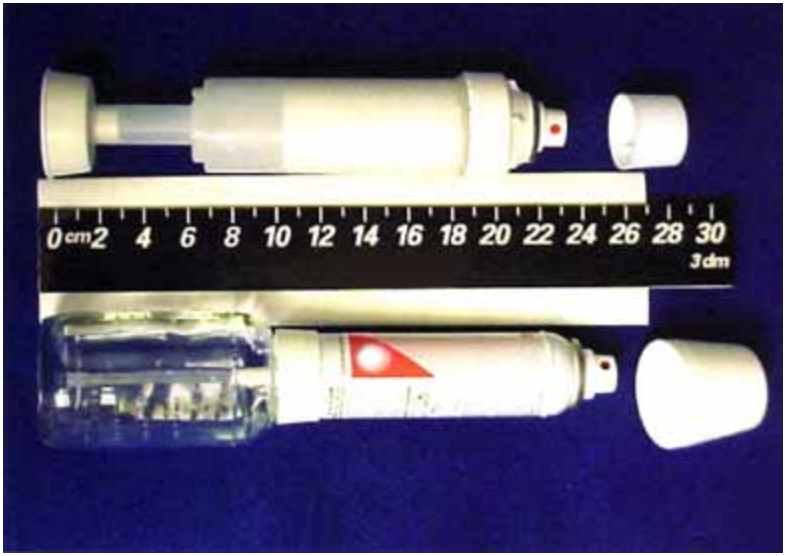
If the biological agent is contagious, it can then spread from person to person.

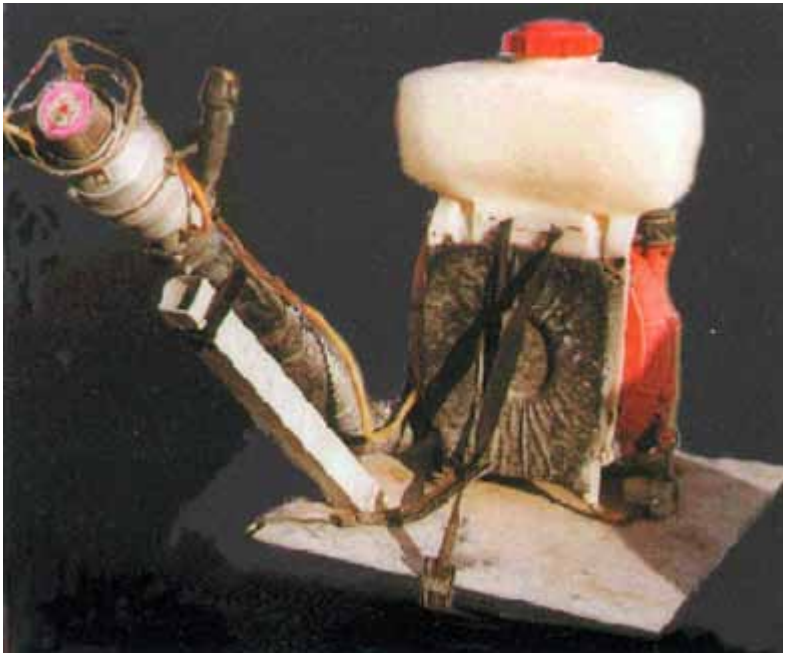
BOX 02

SUMMARY

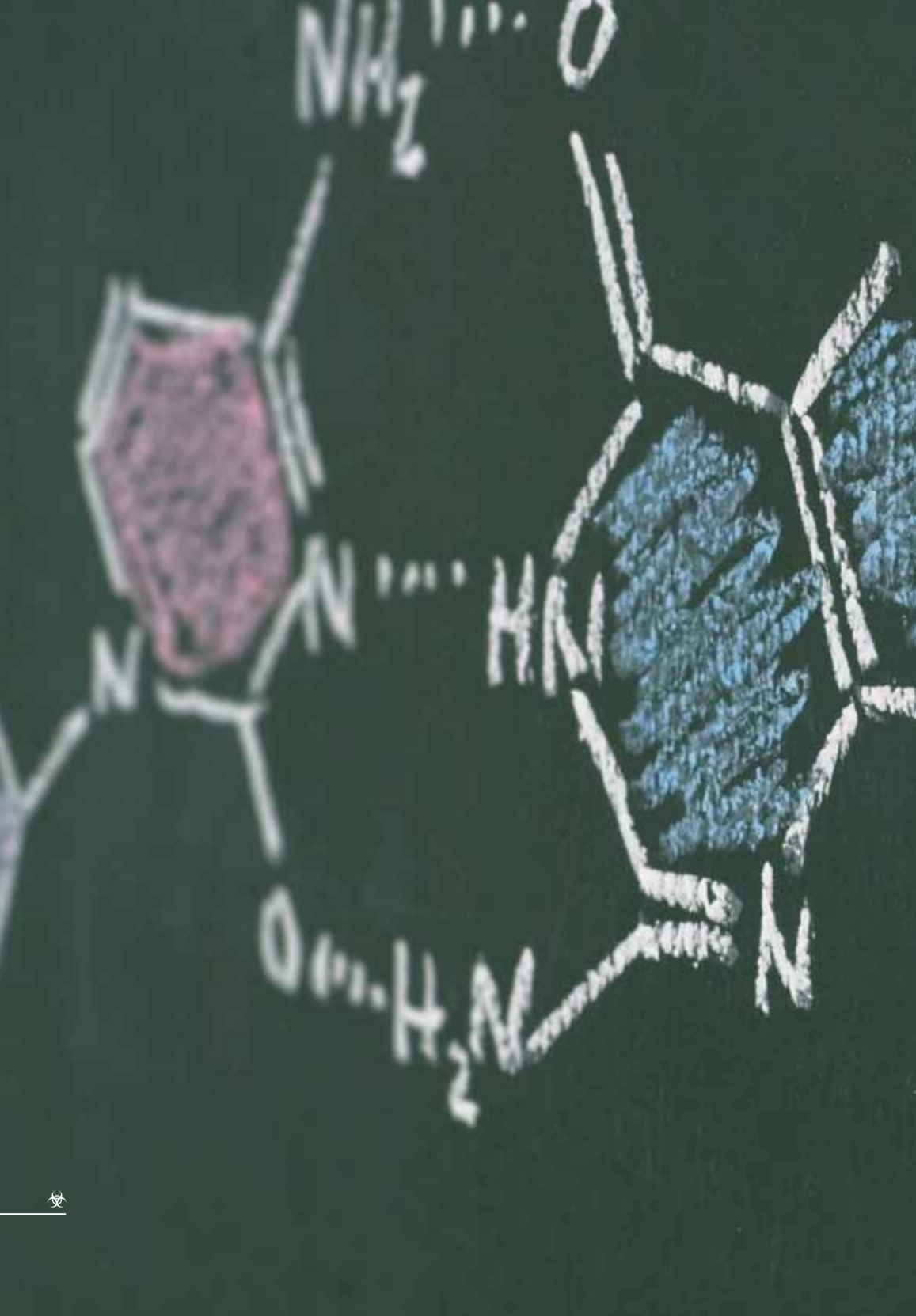
ROUTES OF EXPOSURE

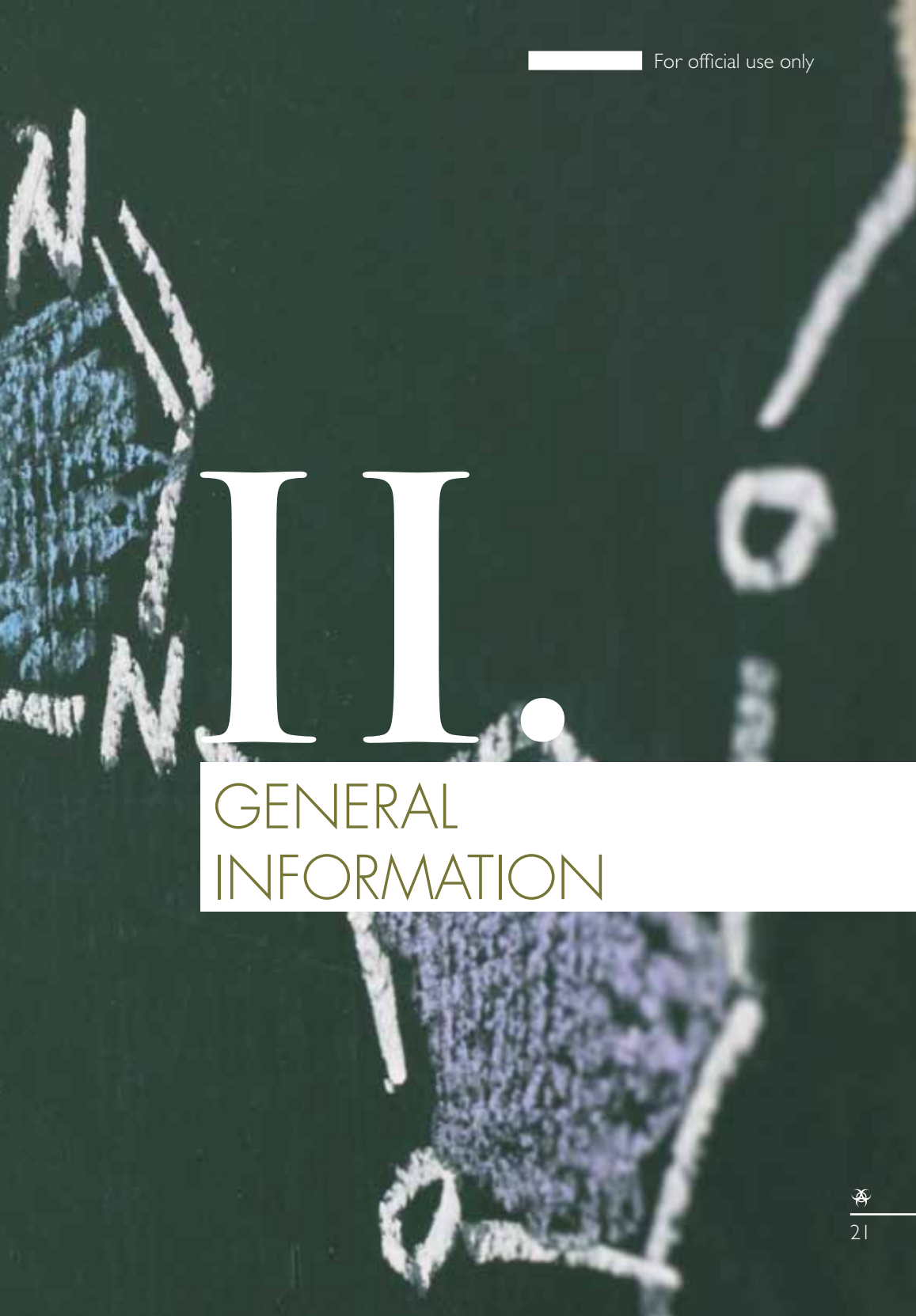
1. Inhalation
2. Ingestion
3. Absorption
4. Injection





Modes of dissemination. © FBI and NCTC-USA


NH2
O
N
N
H
N
O
H2N
N



II.

GENERAL INFORMATION

1. Bioterrorism as part of CBRNE

This guide is intended to provide information relating to a biological incident, i.e. how to prevent such incidents and how to respond to them. It is essential, in all cases, to rule out the presence of chemical, radiological and/or nuclear hazards before considering your response to a biological incident. The spectrum "Chemical, Biological, Radiological and Nuclear" (CBRN) sometimes includes the additional component, "Explosives", to make the abbreviation CBRNE. Many incidents or attacks involve a single element of the spectrum, and since explosives are still widely and preferentially used in terrorist attacks, their presence too should be ruled out before further steps are taken.

Chemical incidents are more likely to be immediately apparent, because of what can be either seen or smelled. Biological agents are difficult to detect at first, unless you have additional information, such as a specific threat that mentions a particular agent. Radiological incidents cannot be seen or smelled, but radiation can be detected by using readily available detection equipment.

CHEMICAL INCIDENTS

Chemical substances are everywhere in nature and are used in almost all natural and man-made processes. Examples include Toxic Industrial Chemicals (TICs), like ammonia and chlorine, as well as dangerous household chemicals such as bleaches and pesticides. Such chemicals may appear as a gas, a liquid or in powder/granular form.

Chemicals that could be used for terrorist purposes also include chemical warfare agents such as mustard gas or sarin.

It is possible to acquire equipment that can be used to detect chemicals. Such equipment must be used in accordance with the manufacturer's instructions and be regularly tested. Those using the equipment will need special training in its use and certification to that effect. Usually, chemical detectors will only detect what they have been programmed to detect.

BOX 03

SOME CHARACTERISTICS OF CHEMICAL AGENTS

- Exposure is usually by skin contact, inhalation or ingestion
- Onset of symptoms can be almost immediate in some cases
- Victims may exhibit symptoms such as coughing or convulsions, or complain of burning skin
- With some very toxic chemicals, death will be almost immediate
- There may be a visible cloud or plume of gas
- An unusual and/or pungent smell may be apparent
- Dead vegetation or animals may be present

Toxic chemicals sign.

Respirators. © Sandia National Laboratories International Biological Threat Reduction

BIOLOGICAL INCIDENTS

While the other elements of the CBRNE spectrum have certain obvious characteristics making detection possible, biological agents require a different approach concerning their detection, analysis and response. The working definition of biological incidents used by the United Nations Office of Disarmament Affairs (UNODA) is: "incidents in which a biological agent harms or threatens to harm humans, livestock or agricultural or economic assets."

The examples in the box below demonstrate why the use of biological agents can be so difficult to detect and different from detecting chemical and radiological agents.

BOX 04

SOME CHARACTERISTICS OF BIOLOGICAL AGENTS

- There is usually no taste or odour
- They are invisible to the naked eye
- Microscopic amounts may cause infection
- Symptoms of infection may be delayed by hours (toxin), days, or possibly weeks
- Some infections can be transmitted from person to person
- People may be exhibiting similar symptoms at an increasing rate until the first cases are diagnosed
- Many agents are sensitive to environmental conditions (weather, sunlight or air pollution) but some may survive in the environment for a long time (e.g. spores causing anthrax)

Biological substance. © iStockphoto

RADIOLOGICAL INCIDENTS

Radioactive materials come in a wide range of physical forms and are commonly used for many industrial, research and medical procedures. The presence of radiation may not be immediately apparent and symptoms may develop over a long period of time, depending on the "dose rate" and duration of exposure. Radiological sources include, but are not limited to, specific isotopes of caesium, uranium, cobalt, iridium and iodine.

Instruments for detecting radiation are used to recognize and identify radioactive materials. All detectors have their specific capabilities: for example, certain detectors are capable of detecting only the presence of certain types of radiation, while others are able to provide isotope identification. In all cases, equipment must be used in accordance with the manufacturer's instructions and undergo regular testing, and those using the equipment will need special training in its use and certification to that effect.

BOX 05

EXAMPLES OF RADIOACTIVE MATERIAL CHARACTERISTICS

- Odourless and tasteless
- Can be in the form of powders, ceramics, metallic pellets/wires, liquids or gases
- Substance will emit radiation (alpha or beta particles, X-rays, gamma rays or neutrons)
- Radiation type will determine how far the radiation will penetrate, i.e. gamma rays and neutrons are highly penetrating while alpha and beta particles travel only short distances
- Symptoms of exposure may include reddening of the skin or burns, nausea, vomiting, diarrhoea, fatigue and headaches
- Levels of radiation can be detected and measured with the use of specialist equipment such as handheld survey instruments (e.g. Geiger counters, ionization chambers), personal dosimeters or Radiation Portal Monitors.

Radiation hazardous material. © Shutterstock

NUCLEAR INCIDENTS

Nuclear weapons utilize the energy produced by the splitting or fusion of atomic nuclei to generate tremendous explosive force, heat, radiation and other harmful effects. The design and production of nuclear weapons are usually State-controlled, and are challenging even at national level. The manufacture of nuclear weapons requires enormous efforts in development and production, and is technologically and financially demanding. In addition, the acquisition or production of components and materials required to create a nuclear weapon is extremely difficult, not least of which being the production of highly enriched uranium (HEU), or weapons-grade plutonium.

These difficulties make nuclear weapons the least likely form of weapon to be used by terrorists. However, these weapons are unique in terms of their extreme explosive energy and their ability to generate and deliver significant doses of ionizing radiation and to contaminate a wide area. This latter capability has both short- and long-term effects that can inflict mass casualties. A nuclear incident could also include attacks to nuclear facilities where highly radioactive material is stored.

Nuclear explosion. © Shutterstock

EXPLOSIVES INCIDENTS

Explosives are most likely to be used in conventional terrorist attacks (single or multiple attack modes) which have an immediate effect, resulting in damage to infrastructure and/or casualties. Different types of explosives can be used in an attack, ranging from commercially available explosives to military or homemade explosives. These can be used in devices such as: an improvised explosive device (IED) e.g. a parcel- or suitcase-bomb; a vehicle-borne improvised explosive device (VBIED) such as a car bomb; a large-vehicle-borne improvised explosive device (LVBIED); or a person-borne improvised explosive device (PBIED) e.g. rucksack bomb or suicide vest being carried or worn by a suicide bomber. The combination of explosives with other materials (CB or R) is possible, but the heat and blast effects of the explosives may negate some chemicals and biological agents depending on the quantities involved, configuration and agent types, but will not destroy any radioactive materials.

Please note: This guide does not give specific information about types of attack where chemical, biological or radiological material are used. This is because predicting such incidents could lead to responders "expecting" certain situations, rather than being alert to all possibilities.

A terrorist fabricating an explosive device. © Shutterstock

2. Acquisition of biological agents

A successful bioterrorist attack involves planning for the effective acquisition, production and dissemination of the biological agent(s). Each part of this process can present a challenge to the perpetrators' knowledge and capabilities.

BOX 06

FACTORS AFFECTING SELECTION AND ACQUISITION OF AGENTS

- Ease of acquisition/production
- Technical skill/education of the terrorist organization
- Ease of delivery/dissemination
- How resistant the agent is to environmental conditions
- Whether the intention is to incapacitate or kill
- Whether the agent is contagious
- Potential risk to the terrorists themselves

The availability of and access to the desired agent, associated production equipment and methodology to be used will influence the choice of agent. It is important to remember that there are legitimate reasons for the acquisition of biological agents and associated production equipment, which can make detection of illegitimate activity difficult (the "dual-use" aspect referred to earlier).

A significant challenge for the terrorist is the acquisition of the biological agent of choice. Depending on the terrorists' intentions and capabilities, they may consider a range of sources for acquiring their agent of choice.

BOX 07

EXAMPLES OF MEANS OF AGENT ACQUISITION

- Fraudulent acquisition from a commercial supplier
- Diversion of transported material
- Stolen from legitimate holding:
    - Microbiology/pathology laboratory
    - University research laboratory or biotech
    - Veterinarian laboratory
      by:
    - Coercion of employees
    - Trusted insider (a disgruntled employee, one motivated by personal gain or the desire to commit a terrorist act)
    - Breach of laboratory security
- Nature/Environment
    - Infected animal
    - Agent reservoirs (i.e. soil, insects, etc.)
    - Clinical sample (human or animal)
- Self-propagation or natural growth of plants (plant toxins)

Clostridium vial. © Robert Koch Institute

3. Production and dissemination of biological agents

The methods of producing many biological agents are openly available in scientific literature, terrorist manuals and extremist literature. However, scientific and/or technical knowledge is usually required to comprehend these methods.

The different properties and growth conditions of bacteria, viruses, fungi, toxins, pests, etc. means that there are a variety of methods for isolation, culturing, purification and dissemination of biological agents. This also means that different levels of technical skills and specialized equipment are required to produce and disseminate particular biological agents.

Pests or plant-toxin acquisition and isolation may require improvised equipment and some technical skill. Bacterial culture will require some specialized equipment and technical skill. Viruses can be grown in cell culture, which will require specialized equipment and a higher degree of technical skill. Alternatively, in the absence of specialized equipment, animals (for example rodents) can be used to culture some pathogens, or eggs can be used to grow some agents.

Dissemination or dispersal system. © Shutterstock

Certain biological agents may require the addition of flow agents that assist with dispersal. These additives may have specific properties which may provide vital evidentiary value for any subsequent forensic investigation. Biological agents may be disseminated in a liquid, powder, gel or slurry. The smaller the particle, the greater the risk it possesses as an aerosol for inhalation.

MEANS OF AGENT DISSEMINATION

Biological agents can be disseminated in a number of ways. Law enforcement agencies may detect biological agent dissemination through reports of unusual behaviour or the discovery of unexpected devices or odours.

Dissemination devices. © Australian Federal Police

Air conditioning system. © Shutterstock

BOX 08

EXAMPLES OF DISSEMINATION TECHNIQUES

- Dispersal systems for inhalation exposure
- Mail/packages
- Commercially available spray devices
- Crop dusters
- Fire extinguishers
- Air-conditioning systems
- Smoke generators
- Cooling fans/mist generators

- Food and water contamination
- Individual consumption items
- Food chain contamination

- Injection
- Contaminated needles
- Projectiles
- Contaminated shrapnel
- Direct contact by infected persons/animals

- Military munitions

BOX 09

EXAMPLES OF BIOLOGICAL AGENT DISSEMINATION INDICATORS

- Presence of suspicious liquids or powders
- Sick or dying animals or persons
- Unscheduled/unusual spraying activity
- Unusual odours
- Purified biological agents are odourless, but unpurified products may have distinct odours characteristic of rotting meat or fermentation.
- The smells of growth media may be interpreted as musty, yeasty or like rotten meat
- Presence of dissemination devices (see box above)
- Reports of tampering with food, water supply or air distribution systems
- Receipt of a written, electronic or verbal threat or claim of responsibility

A victim is hospitalized. © Shutterstock

4. Intelligence indicators for bioterrorism

After gaining an understanding of the acquisition, production and dissemination of biological agents, it is important for law enforcement and partner agencies to know when a potential bioterrorist attack is imminent.

Each stage of the process – to plan, acquire and/or produce, deploy and disseminate the agent – may leave intelligence indicators that could lead to disruption of the event. It is important to stress the fact that the examples below do not constitute a check-list and that, for each of these indicators, information should be analysed, checked and acted upon on a case-by-case basis.

BOX 10

EXAMPLES OF INTELLIGENCE FINDINGS POTENTIALLY INDICATING AN INTEREST IN BIOTERRORISM

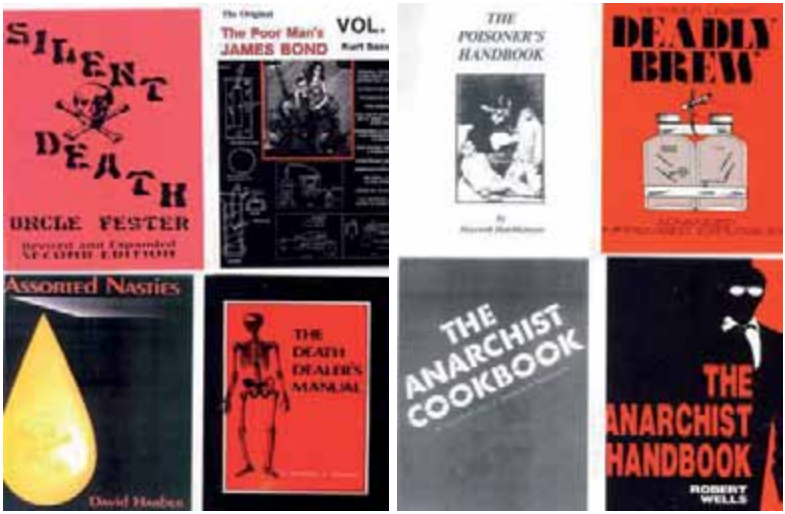
- Efforts to recruit individuals with education or experience in microbiology, medicine or engineering from universities/hospitals/ laboratories
- Connections of terrorists to biological laboratories
- Unusual or suspicious interest in laboratories holding biological agents
- Unjustified travel to disease-endemic areas, particularly during outbreaks
- Fraudulent acquisition of biological agents from commercial suppliers
- Diversion of biological agents from transported material
- Loss or theft of biological agent from legitimate holding (e.g. laboratory)

BOX 10

continued

- Suspicious behaviour in a laboratory
- Purchase of plants or seeds known to be sources of toxins
- Theft or acquisition of laboratory equipment
- Suspicious behaviour in disease-endemic areas, such as trapping of sick or dying animals or taking samples of soil without a legitimate reason
- Modification of premises (e.g. taped windows, modification of ventilation systems)
- Possession of protective clothing, respirators or masks
- Unusual or suspicious purchase/possession of:
    - vaccines and antibiotics
    - antiseptics, bleach or other anti-microbial substances, cleaning supplies
    - laboratory animals
- Interest in dissemination devices or recovery of such devices
- Small scale "trial" attack
- Unusual or suspicious clusters of dead animals
- Presentation of people with atypical symptoms or clusters of people with unusual symptoms at health-care facilities
- Interest in extremist literature (e.g. "Silent Death"[1])
- Recovery of periodicals, instruction manuals or web resources providing biological-agent production recipes

[1] Silent Death, by Steve Preisler, 1997



Examples of extremist literature, periodicals and instruction manuals providing biological-agent production recipes. © FBI and NCTC-USA

Castor bean pulp

Ricin extraction

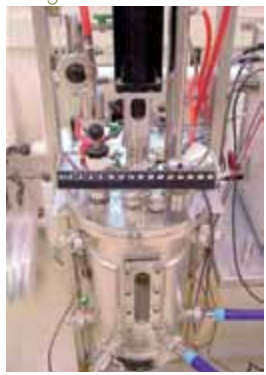
Castor beans

Meat broth

Examples of plants or seeds known to be sources of toxins. © FBI and NCTC-USA

Examples of laboratory equipment. © FBI, NCTC-USA and Sandia National Laboratories International Biological Threat Reduction

Bioreactor



Fermenter

High-speed centrifuge

Autoclave

Autoclave

Centrifuge

Incubator

Glove box

Biosafety cabinet

Lyophilizer

Sampling equipment

Incubator shaker

Bench top fermenter

Vacuum pump

Vacuum pump

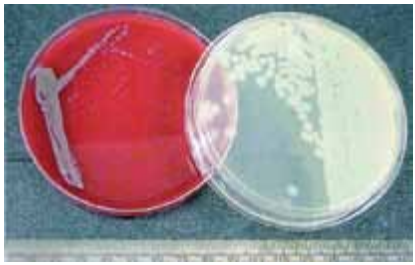
Examples of laboratory equipment (continued). © FBI and NCTC-USA

Glassware

Growth media

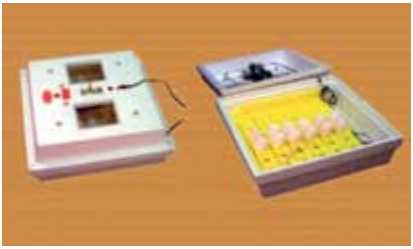
Vaccine vial

Agent containers



Agar plate

Mortar & pestle



Egg incubator

Biohazard signs

Milling device

Vacuum filtration

Microscope

Biohazard signs

Examples of dissemination devices. © FBI and NCTC-USA

Example of anti-microbial substances. © FBI and NCTC-USA

Examples of protective clothing. © Australian Federal Police

5. Different types of attacks - overt and covert

It is extremely important for law enforcement to understand the different dimensions of overt and covert attacks in the development of all bioterrorism response protocols.

OVERT ATTACK

An overt attack is an event clearly recognizable by law enforcement or other responders. Awareness of the attack will be evidenced by:

- reception of a specific threat, warning or intelligence
- discovery of a means of dispersal or other signature activities/ apparatus, or
- discovery of questionable or suspect materials.

To mitigate the health consequences of the attack, law enforcement must inform public health and medical authorities of the event. The means of contact should be pre-established and exercised, practised and tested beforehand in order to avoid delay or inefficient information exchange.

Suspicious bag abandoned in a public space. © Shutterstock

The consequence of failing to have an established information-exchange protocol between law enforcement and public health for overt attacks is the potential for delays in public health and medical responses. There is also the possibility of attacks occurring prior to the detection of the overt event, and these prior attacks would be discovered only upon review of medical and public health information.

COVERT ATTACK

Terrorists are likely to use biological agents in a covert attack. A covert attack will have the following characteristics:

- no announced threat or warning;
- a carefully disguised dispersal device or method;
- and no physical indication of the agent being spread.

In these situations, victims are unaware that they have been exposed, and law enforcement is not aware that a crime has taken place. There will not be a defined crime scene until after there has been a medical diagnosis, environmental detection and/or a public health investigation. The terrorist is likely to prefer such a scenario as victims will not seek the necessary medical treatment until they experience symptoms, thus causing a delayed recognition by health and law enforcement officials. In the case of some agents, a delay in initiating treatment may lead to an increase in the number of deaths.

A law enforcement investigation will not be initiated until notification by public health officials, probably after they have detected an unusual disease pattern by means of a health-surveillance system, or following the diagnosis of an unusual disease by the health-care community. Since the law enforcement services must rely on early detection and notification by public health and medical authorities, it is recommended that these agencies consider creating notification protocols and conduct pre-event training.

Laboratory flasks. © Robert Koch Institute

BOX 11

EXAMPLES OF DISEASE PATTERNS THAT MAY INDICATE BIOTERRORISM

- A sudden increase in patients with similar symptoms
- A high mortality rate among victims having common home or work locations and activities
- Disease concurrent with illness in the susceptible animal population
- A disease that is not normally seen in that specific geographical location or at that specific time of year
- The diagnosis of a disease with potential for use in a bioterrorist case.

6. Personal Protective Equipment

Personal protective equipment, also called PPE, is a "must" for any intervention in a contaminated or suspected contaminated environment. There are different levels of protection, ranging from A to D.

LEVEL A

Offers the highest level of respiratory and dermal protection by combining an encapsulating, gas-tight suit with built-in bootees and gloves, and self-contained breathing apparatus (SCBA). This is used in "immediately dangerous to life and health" (IDLH) environments where chemicals are toxic by dermal absorption and inhalation.

Not used in biological responses.

Personal protective equipment (PPE) Level A. © FBI

LEVEL B

Offers the highest level of respiratory protection (SCBA) and a splash-protective suit (not gas-tight) which may or may not be fully encapsulating, and chemical-resistant gloves and boots that may or may not be built into the suit.

Used in biological responses.

PPE Level B. © FBI

LEVEL C

Offers a lower level of respiratory protection and some suits may offer limited splash protection. Suits may include hooded coveralls with built-in booties. The level C ensemble will include the suit, gloves, foot coverings, and a full-face respirator or powered air-purifying respirator (PAPR) with high-efficiency particulate air (HEPA) filters.

Used in biological responses.

PPE Level C. © FBI

A PAPR, in combination with protective suits with an integrated respirator hood, offer maximum comfort for both wearing and using:

- Continuous airflow insides the suit minimizes heat stress
- No airway resistance
- Fast deployment
- Also designed for users with beards and/or goggles
- Additional safety by means of positive pressure inside the suit
- No difficulties with face seal
- Requires less training and practice.

Ideal for managing most biological incidents

Example of PAPR with an integrated respirator hood.
© Robert Koch Institute

LEVEL D

Offers the lowest level of protection, includes wearing of normal work clothing, safety glasses, hard hat and steel-toe shoes. Such equipment is not used in a biological response, and should be used only in cases when the atmosphere does not contain any hazards.

FACTORS TO CONSIDER WHEN WEARING PPE

The wearing of any level of PPE imposes a number of limitations on responders. Law enforcement officers should train often to understand the impact of wearing PPE on operational duties.

PPE. © Robert Koch Institute

BOX 12

USE OF PPE - LIMITS TO OPERATIONAL CAPABILITIES

- Restricted mobility and dexterity
- Difficulty in communicating
- Reduced vision
- Heat stress
- Increased weight - Level A can weigh as much as 20-25kg
- Psychological stress:
    - Claustrophobia
    - Threatening appearance to victims
- SCBA tank provides limited supply of air

Regular training is mandatory when using PPE!

III.

PREPAREDNESS FOR BIOTERRORISM

1. Prevention and preparedness

It is universally agreed that terrorists must be prevented from acquiring biological agents. Measures taken to enhance prevention can be established at the international level with various initiatives which are also reflected and integrated in the national measures taken. Prevention measures and policy can be taken forward to make it more challenging for perpetrators to initiate a bioterrorist attack. In addition to these, other elements in a prevention strategy should include more general security measures to make it more difficult to obtain biological agents and to encourage non-proliferation.

One of the key elements of preparedness is legislation, which includes the rule of law and policing powers to be able to detect, respond and pursue a bioterrorist act. Law enforcement and other agencies should seek to establish and maintain inter-agency arrangements and co-ordination mechanisms. There is a need for unprecedented collaboration as these partner agencies are often different from those which the police usually work with, like the public health community, scientists, and laboratories. Medical staff may speak different languages (figuratively speaking), use different approaches to cases or incidents and also have, in an ideal situation, an early-warning mechanism in place to detect and communicate outbreaks of diseases.

In order to build a strategy for prevention, the following strands must be developed:

- Legislation
- Partnerships, including inter-agency arrangements and co-ordination mechanisms
- Laboratory safety and security.

2. Legislation

In order to best prevent bioterrorism incidents, it is essential that accurate, appropriate and updated legislation reflecting current 'best practice' be developed to enable law enforcement and health officials to have the means to intervene and react.

Legislation is what will give legitimacy to law enforcement and public health actions before, during and after a bioterrorism incident.

National legislation needs to be comprehensive in order to avoid any gaps and to effectively criminalize activities involving the misuse of biological agents.

DUAL USE

A very important aspect to consider when dealing with biological agents is the fact that biological agents can be, and are, used for legitimate means (pharmaceuticals and research, vaccine production, development of cosmetics, etc.). Unfortunately, they can also be misused for bioterrorism purposes. This is known as the dual use of biological agents.

Dual use is something which must be considered when enacting bioterrorism legislation, as there needs to be a clearly defined balance between what is prohibited and what is authorized. Although the use of biological agents cannot be prohibited, they need to be clearly regulated in order to avoid criminal use.

LEGITIMATE USE VS. CRIMINAL USE

National legislation often makes a clear distinction between biological agents and bio-weapons. The distinction lies in the fact that the first category is intended for peaceful purposes and the second for harmful and criminal purposes. To be more precise, a bio-weapon is a biological warfare agent combined with an application tool.

Making these distinctions clear in legislation from the onset will make it easier to distinguish between what is allowed and what needs to be strictly prohibited.

In addition, national laws should not only indicate a general prohibition of bio-weapons. They need to include specific aspects of prohibition, such as the prohibition to develop, produce, possess or stockpile bio-weapons.

Biological packaging. © Robert Koch Institute

Although the legitimate use of biological agents needs to be preserved, it nonetheless needs to be regulated in order to avoid accidents and the possibility that people with bad intentions will be in a position to acquire, develop or use biological agents.

A secure entrance. © INTERPOL

Precise legislation regulating the transport and transfer of biological agents needs to be developed. Import, export and inventory controls and regulated procedures also need to be included in legislation. The physical protection of material and facilities should also be seriously considered in national laws. Bio-security guidelines need to be developed: these serve to secure the premises where biological agents can be found, including the personnel who will be working in those premises. Such guidelines can include basic systems such as secure badging systems including biometric identification for personnel, state-of-the-art alarm systems, etc.

INTER-AGENCY CO-OPERATION

Legislation needs to include features that can facilitate inter-agency co-operation, in order for law enforcement and public health officials to be able to develop common contingency plans, share information lawfully, and perform joint investigations and joint interviews. Such features may take the form of co-operation agreements between administrations or memoranda of understanding, for example.

BOX 13

ASPECTS TO CONSIDER WHEN DEVELOPING NATIONAL LEGISLATION

- Working with biological agents
- Securing biological agents
- Developing biological agents
- Acquiring biological agents
- Possessing biological agents
- Transferring biological agents
- Transporting biological agents.

INTERNATIONAL REFERENCES AND MECHANISMS

Several international instruments have been developed to attempt to control the development and use of biological weapons.

These instruments can and should be used for reference when developing and enacting national legislation.

These international references are for example:

- Geneva Protocol of 1925 (covering the prohibited use of biological agents)
- Biological Weapons Convention of 1972
- International Health Regulations, revised in 2005.

Member countries seeking assistance in the development of new legislation can consult the following organizations *(for contact information, please consult the useful links page at the end of this guide):*

World Health Organization – The World Health Organization (WHO), based in Geneva, Switzerland, is the directing and co-ordinating authority for health within the United Nations system. It is responsible for providing leadership on global health matters, shaping the health-research agenda, setting norms and standards, articulating evidence-based policy options, providing technical support to countries and monitoring and assessing health trends. In addition to its many primary tasks concerning international health matters, the WHO is also mandated to propose conventions, agreements and regulations, and make recommendations on such matters. One of the major achievements deriving from the WHO's mandate are the International Health Regulations.
(More information is available on the website: http://www.who.int)

United Nations: Resolution 1540 (2004) adopted by the Security Council at its 4956th meeting, which urges member countries to take necessary measures to adopt laws which *"...prohibit any non-State actor to manufacture, acquire, possess, develop, transport, transfer or use nuclear, chemical or biological weapons and their means of delivery, in particular for terrorist purposes, as well as attempts to engage in any of the foregoing activities, participate in them as an accomplice, assist or finance them"*.

The resolution also mentions that States shall: *"...take and enforce effective measures to establish domestic controls to prevent the proliferation of nuclear, chemical, or biological weapons and their means of delivery, including by establishing appropriate controls over related materials and to this end shall:*

(a) Develop and maintain appropriate effective measures to account for and secure such items in production, use, storage or transport;

(b) Develop and maintain appropriate effective physical protection measures;

(c) Develop and maintain appropriate effective border controls and law enforcement efforts to detect, deter, prevent and combat, including through international cooperation when necessary, the illicit trafficking and brokering in such items in accordance with their national legal authorities and legislation and consistent with international law".

(For a complete text of the Resolution 1540, please visit the United Nations website at: http://www.un.org/docs/sc/unsc_resolutions04.html)

Biological Weapons Convention Implementation Support Unit, based in Geneva, Switzerland. The Unit takes care of administrative support to the BWC; serves as an information exchange point between member states and with international and professional organizations; administers exchanges of information under the Convention (including the confidence-building measures, national implementation database, and Compendiums and National Approaches); supports member states in their effort to implement the convention; and assists member states in their efforts to expand the membership of treaty. *(For a complete overview of this unit, please visit the website: http://www.unog.ch)*

United Nations Office of Disarmament Affairs (UNODA) is based in the UN Headquarters located in New York, United States. The Office promotes the goal of nuclear disarmament and non-proliferation and the strengthening of the disarmament regimes in respect to other weapons of mass destruction, chemical and biological weapons. It also promotes disarmament efforts in the area of conventional weapons, especially land mines and small arms, which are the weapons of choice in contemporary conflicts.

UNODA provides substantive and organizational support for norm-setting in the area of disarmament through the work of the General Assembly and its First Committee, the Disarmament Commission, the Conference on Disarmament and other bodies. It fosters disarmament measures, through dialogue, transparency and confidence building on military matters, and encourages regional disarmament efforts.

UNODA is providing support to the Secretary-General's mechanism for investigation of alleged use of chemical, biological and toxin weapons. It works with Member States to update the roster of experts and laboratories whose services would be available to carry out investigative activities as well as to update the technical guidelines and procedures for timely and efficient investigations.

UNODA organizes specialized training courses for experts from the roster to enable them to undertake UN fact-finding missions in particular in cases of alleged use of biological weapons.

(For more information, please visit the website: http://www.un.org/disarmament/)

The United Nations Interregional Crime and Justice Research Institute – UNICRI – was created in 1968 to assist intergovernmental, governmental and non-governmental organizations in formulating and implementing improved policies in the field of crime prevention and criminal justice. In a rapidly changing world, UNICRI's major goals today are advancing security, serving justice and building peace. UNICRI sees itself as "the first response broker". It has become known for its dynamic, fresh and innovative approach in applied research.

UNICRI's activities tackle major concerns in the field of crime prevention and criminal justice, such as corruption, security governance and counter-terrorism, organized crime (in particular, trafficking of persons as well as illicit drugs and arms). The Security Governance/Counter-Terrorism Laboratory is an information-gathering centre, that tests ideas to find proactive solutions to the many global security issues. The Laboratory works

to strengthen security through the management of new ideas in the field of counter-terrorism; abiding by a creative multi-level and intersectorial approach. Through brokerage action the Lab provides fresh ideas and innovative solutions to policy-makers, helping tackle issues affecting the international, regional and local spheres.

The Knowledge Management System on the prevention of illicit trafficking of CBRN material – currently developed through two regional initiatives in South-East Europe and the Caucasus (KMS 1) and North Africa and the Middle East (KMS 2) – is designed to assist states in establishing clear channels of communication, improving information sharing on CBRN incidents, and accessing information that helps strengthen capabilities in terms of effective border control, law enforcement operations, national export controls and trans-shipment controls. Rather than focusing on CBRN substances, this project focuses on the modalities through which CBRN materials may be illegally transferred or acquired. KMS applies a CBRN comprehensive approach unifying strategic knowledge and expertise drawn from the different CBRN areas. By collecting and comparing all data on illicit CBRN trafficking at the national and regional levels, KMS increases opportunities to identify trends in trafficking, predict the location of future incidents and assess existing vulnerabilities and risks.

(For more information: http://www.unicri.it and http://lab.unicri.it)

On INTERPOL's website *(https://www.interpol.int)* there are various links to other international and national organizations which can provide useful information on bio-preparedness in general.

3. The need for partnerships

Law enforcement has specific goals: the prevention and investigating of crime and maintaining law and public order. In the prevention of the specific crime of bioterrorism, law enforcement should reach out to those agencies and partners that also have a responsibility in preparedness and prevention.

Public health and medical health, fire-fighters, civil protection and other agencies involved often use different vocabulary and specialist terminology, as well as having different standard operating procedures. A "case" means one thing for medical staff and something quite different for police officers.

Collaboration needs to be established beforehand and should be not based solely on personal relationships, but on a network of relationships between responsible agencies at different levels. When tackling bioterrorism, various agencies are involved, as bioterrorism touches upon different competencies: counterterrorism, health protection, consequence management, laboratory security, scientific and academic research. "To prevent and to prepare" means that in order to have effective collaboration, co-operation agreements should be put in place beforehand. This collaboration includes not only public agencies (international and national), but also public-private partnerships. The following agencies, bodies or entities could be involved in this collaboration:

BOX 14

POSSIBLE COLLABORATION IN PREVENTING AND PREPARING FOR A BIOTERRORISM INCIDENT [2]

INTERNATIONAL LEVEL

- United Nations
- World Health Organization
- INTERPOL
- EUROPOL
- Regional organizations or inter-State co-operative bodies.

NATIONAL LEVEL

- Law enforcement - including customs, police, prosecutors dealing with bioterrorism or general CBRNE (chemical, biological, radiological, nuclear, explosives) incidents
- Health protection agencies
- Military
- National fire services
- Civil protection
- Laboratories (forensic, reference laboratories and laboratories specialized in CBRN materials)
- Scientific community, research facilities, academic world
- Policy makers in CBRN response and resilience
- National co-ordination agencies (e.g. consequence management)
- Agencies responsible for threat assessment
- Environmental agencies
- Transporters of CBRN materials.

[2] Roles and responsibilities may vary between the agencies mentioned according to national, regional and international arrangements.

BOX 14

continued

LOCAL LEVEL

- Local agencies of law enforcement
- Local health facilities
- Fire service
- Local government.

From the early-detection phase to the recovery phase, various agencies have to collaborate in order to protect against, prevent and pursue a bioterrorist incident.

For law enforcement, the most important tools are agreements with the medical and public health communities that include:

- **An early-warning system** whereby law enforcement is informed of any emerging suspicious health issues;
- A **means for disclosure** of information, accommodating **patient privacy and confidentiality** issues;
- Collection and handling of **evidence**;
- Selection of compatible **personal protective equipment**; and
- Co-operation with other **national/international health and law enforcement organizations.**

Not all law enforcement agencies have the resources and skills in-house to deal with such an urgent matter as a bioterrorist attack and will need to seek out partnerships with other entities. This could include protocols on providing protective equipment, assistance in forensics, transport of pathogens or any other assistance that could be part of the preparedness plans. The type of partnership would depend on the national and regional capability, as well as the structural and legal constraints of each country. Countries need to be aware of the possibilities for co-operation and support from regional and international bodies; partnerships between countries could also be envisaged. International organizations such as the World Health Organization, INTERPOL and the UN offer services and support to their member countries.

(For more information about these services, please consult the appropriate agencies whose website addresses are listed on page 134 of this guide.)

4. Joint law enforcement and public health operations and investigations

A strong working relationship between law enforcement and public health is essential to respond effectively to both covert and overt acts of bioterrorism. The interaction between law enforcement and public health may take place in a variety of ways, ranging from informal relationships where agencies exchange subject matter expertise, to having both agencies working together to conduct a joint interview of a patient who may be the victim of a bioterrorism event.

THE BENEFITS OF ESTABLISHING PARTNERSHIPS WITH PUBLIC HEALTH AUTHORITIES

Public health agencies are responsible for protecting the health of the public. They do this by implementing disease-control measures to prevent the spread of disease and investigating the causes of disease outbreaks. Public health practitioners have specialized expertise in investigating disease outbreaks, which can prove highly valuable to law enforcement during a bioterrorism investigation. Additionally, in many cases a public health practitioner during their disease investigation (epidemiological investigation) will ask many of the same questions as law enforcement: for example, how did this person become sick, where did they travel to, who did they have contact with, and how long have they been sick?

BOX 15

PUBLIC HEALTH – SKILLS AND KNOWLEDGE

Public health professionals including but not limited to:

- Medical specialists
- Epidemiologists
- Trained outbreak investigators
- Laboratory specialists.

With knowledge about:

- Potential bioterrorism agents, the diseases they cause, diagnosis and treatment
- Diseases that are commonly seen in a geographic region
- Infection-prevention and worker-safety measures
- Health-related risk communication
- Which laboratories can conduct testing to confirm the presence of biological agents.

And relationships and links to:

- Hospitals, clinics and physicians
- Laboratories with capability to test for biological threat agents.

BOX 16

COMPARISON OF PUBLIC HEALTH AND LAW ENFORCEMENT GOALS

LAW ENFORCEMENT	PUBLIC HEALTH
▪ Protect health and safety of public ▪ Determine cause of bioterrorism attack ▪ Stop further crimes ▪ Apprehend and convict criminals.	▪ Protect health and safety of public ▪ Determine cause of bioterrorism outbreak ▪ Stop further cases of disease and outbreaks ▪ Build science base for future prevention.

As can be seen from the above, while law enforcement and public health have some different goals, both are interested above all in determining the cause of the outbreak (or the crime) in the interests of protecting the health and safety of the public.

Laboratory worker. © Robert Koch Institute

JOINT NOTIFICATION PROCEDURES

It is essential to establish communication mechanisms between law enforcement and public health. These mechanisms and the criteria used to prompt information exchange should be developed with consideration for pertinent laws and regulations protecting both sensitive law enforcement data and confidential medical information. Effective information exchange requires that law enforcement and public health personnel be familiar with one another and know which people in each agency should receive the information.

Definitive criteria for public health notification of law enforcement are difficult because almost all biological agents mimic other diseases in their early stages. However, there are a number of specific situations in which information should be shared between public health, medical and law enforcement authorities to detect and manage a bioterrorism event.

BOX 17

TRIGGERS FOR LAW ENFORCEMENT TO SHARE INFORMATION

- Any intelligence or indication that any group or individual is unlawfully in possession of biological agents.
- Seizure of processing equipment, dissemination devices, literature or related items that could be used in the production or use of biological agents.
- Any assessment that indicates a credible biological threat may exist in the area:
  - Credible threats to events and venues in the area
  - Credible threats to segments of the population.

BOX 18

TRIGGERS FOR MEDICAL AND PUBLIC HEALTH TO SHARE INFORMATION

- Any indication that a disease outbreak could be caused by an intentional act.
- Laboratory results that indicate the identification of a potential biological terrorism agent e.g.:
  - Inhalational anthrax
  - Pneumonic plague
  - Ricin
  - Smallpox.
- Large number of individuals reporting unexplained similar symptoms.
- Unexplained deaths.
- Unusual disease presentation such as:
  - Anthrax (inhalation)
  - Plague (pneumonic).
- Any disease with an unusual geographic or seasonal distribution such as:
  - Ebola haemorrhagic fever without exposure to endemic areas
  - Flu-like illness in summer.

CONDUCTING A THREAT ASSESSMENT

At a time when many countries must deal with terrorism effectively, law enforcement agencies are constantly responding to new threats. With finite resources, it is essential that law enforcement agencies develop procedures to evaluate the credibility of these threats, so that resources may be prioritized in accordance with the threat level. A formalized threat assessment, which draws upon the technical expertise of various law enforcement disciplines and other agency experts, assists in evaluating a threat, determining

if it is credible, and identifying what resources are needed to conduct a criminal investigation, mitigate the threat, and preserve evidence in a contaminated environment.

When information regarding a threat is received, a threat assessment should be initiated. This may happen on-scene or through a co-ordinated conference call by telephone or any other communication method. Assessment participants are chosen in a tailored response to the threat to provide input in specific areas of expertise. Law enforcement may consider drawing expertise from public health, medical authorities, emergency management personnel and fire department personnel, to name just a few.

A recommended approach that may be taken by law enforcement is to divide the threat assessment process into three prongs. Firstly, law enforcement should evaluate the operational practicality of the threat: does the operation that is used to carry out the threat seem practical? Would the operation work? Secondly, assess the technical feasibility of the threat: does the threat require technical expertise and, if so, are those involved technically competent? Lastly, if information is known regarding the perpetrator, does this person display the behavioural resolve to carry out the operation? While not definitive, affirmative responses to these questions may suggest a threat is credible and that an immediate law enforcement response and follow-up actions are urgently required.

JOINT INVESTIGATIONS OR OPERATIONS

Once information regarding a potential threat, outbreak or incident has been shared, law enforcement and public health agencies may be responsible for independent roles and responsibilities in the resulting investigation. Co-ordination of law enforcement and public health activities is therefore essential. It is recommended that joint operations and investigations be pre-planned and exercised. Agencies can consider assigning liaison contacts to respective partner agencies in order to ensure

investigative information is shared. Additionally, in the early stages of a covert bioterrorism attack, it may be beneficial to consider conducting joint interviews.

JOINT INTERVIEWS

A joint interview draws on the strengths of having a multidisciplinary interview team. In a joint interview, a law enforcement officer and a public health official both take part in a single interview of a victim. This allows both parties to obtain the same information and minimizes potential duplication of effort and possible collection of contradictory information. It is essential, of course, for the parties involved in the interview to plan their approach and questioning before conducting the interview. When evaluating the potential to conduct joint interviews, those responsible must be sure to review current regulations, rules and laws to ensure that law enforcement may be present during a patient's interview. Some countries allow the exchange of sensitive medical information in certain circumstances, while others do not.

BOX 19

SUMMARY

ADVANTAGES OF JOINT INTERVIEWS

- Minimize the collection and documentation of conflicting information
- Simultaneous access to information
- Opportunity to address misunderstandings
- Multi-disciplinary interview perspective.

JOINT TRAINING

It is highly recommended that law enforcement and public health officials establish protocols to conduct joint training, notifications, threat assessment, and/or interviews. These protocols should be included in bioterrorism-specific training and exercises to ensure that these procedures will be beneficial during an actual response.

Joint training. © INTERPOL

5. Securing the agents

In addition to the development of response protocols, law enforcement should take a leading role in promoting a programme of prevention. Because dangerous biological pathogens are stored in many legitimate laboratory facilities, a first step in prevention may be to review and improve security at these facilities. Systems – similar to the requirements for other critical infrastructures – should be put in place to require the mandatory reporting of accidents, theft, loss, or release of biological agents. In order to ensure a level of information exchange between relevant actors, a clearly established notification mechanism is called for which would allow anyone to inform the relevant authorities about the loss or theft of high-risk biological material, or about a suspicious transaction. As a minimum requirement, facility security managers should have the necessary contact details of the appropriate local law enforcement authorities.

Other considerations that may serve as a deterrent to the misappropriation of biological agents could include adding restrictions to the purchase of dual-use laboratory equipment (making it mandatory for individuals to provide documentation of legitimate use), and adding regulations on the purchase and transportation of biological agents. The creation of outreach programmes that increase the level of bioterrorism awareness and information exchange between law enforcement, industry and the scientific community will facilitate the reporting of suspicious activities and may have an added deterrent value as well.

Biohazard signs. © FBI

6. Bio-safety and bio-security

Bio-safety and bio-security measures serve to prevent the risks linked with the use and stockpiling of biological agents. As law enforcement needs to develop a working relationship with the scientific community and laboratories, it is important to understand the definition and scope of these terms. After assessing the risks related to certain hazardous agents, it is important for law enforcement to follow up on these security measures.

Note: The term "biohazard" and its associated symbol is generally used as a warning, so that those potentially exposed to the substances will know to take precautions.

The biohazard sign can appear in different colours and forms. © Shutterstock

BOX 20

DEFINITION

LABORATORY BIO-SAFETY AND BIO-SECURITY

BIO-SAFETY

- A set of preventive measures designed to reduce the risk of accidental exposure to or release of a biological hazard
- Goal: reduce risk of accidental exposure to or release of potentially hazardous agents

BIO-SECURITY

- A set of preventive measures designed to reduce the risk of theft of biological material
- Goal: protect biological agents from theft and malicious use

COMMON STRATEGY

- Implement graded levels of protection based on a risk assessment
  - Methods of implementation must be carefully considered
- Bio-security and bio-safety should be integrated systems that avoid compromising necessary infectious-disease research and diagnostics

BOX 21A

ACTION

LABORATORY BIO-SAFETY RISK ASSESSMENT

Assess the biological material

- Contagious; potential impact of disease
- Routes of exposure
- Host range
- Type of material
  - Clinical sample
  - Pure culture
- Environmental stability

Assess what is being done with the material

- Diagnostics
- Procedures that may generate aerosols

Consider PPE

- Respirators
- Gloves

Law enforcement should understand similar concepts when handling potentially contaminated crime scenes

- Contaminated evidence
- Collection procedures that generate aerosols
- PPE

BOX 21B

ACTION

LABORATORY BIO-SECURITY RISK ASSESSMENT

Assess the biological agent

- Determine if the material could be attractive for misuse
- Evaluate potential adversaries that could be interested in the agent

Evaluate potential scenarios

- Consider specific scenarios resulting in access to the material
- Identify how the scenarios could occur
- Evaluate the potential consequences associated with the scenarios

Evaluate threat environment

- Criminal activity
- Extremist activity
- Terrorist activity

POTENTIAL ROLE OF LAW ENFORCEMENT

Law enforcement may have an important role to play in ensuring that bio-security measures and protocols are applied and respected. These are some examples of how police and other agencies can contribute to bio-security in general:

Police intervention. © Robert Koch Institute

BOX 22

ROLE OF LAW ENFORCEMENT IN BIO-SECURITY

Physical security and access control

- Attempted unauthorized access
- Suspicious person
- Theft of keys
- Attempted subversion of the security system
- Security breach

BOX 22
continued

Personnel security
- Background investigation
- Fraudulent application information or credentials

Transportation security
- Package theft
- Theft of carrier vehicle

Information security
- Theft, loss or compromise of information:
  - Laboratory notebook
  - Experimental procedures or data
  - Security access codes
- Suspicious requests for information

Material control and accountability
- Investigate theft or loss
  - biological agents, equipment, information
- Investigate potential compromise of security system

Additional
- Assess the threat environment
  - Local and regional criminal activity
  - Local and regional terrorist activity

IV.

OPERATIONAL RESPONSE TO BIOTERRORISM

1. Incident response checklist

Once an investigation is launched, the response relating to the crime scene should be structured. To this end, a checklist is a useful tool. The overall principles of incident response provide methods to identify vulnerabilities and to take appropriate countermeasures to prevent and mitigate failure risks for an organization. The main priorities in a biological incident are:

- Preservation of life
- Safety of personnel involved
- Investigation
- Intelligence to prevent further attacks
- Public reassurance and return to normality.

BOX 23

ACTION

INCIDENT-RESPONSE CHECKLIST FOR THE CRIME SCENE PHASE

- Evaluate the current on-scene situation and conduct a threat assessment
- Notify other appropriate agencies if threat is determined as credible
- Establish Incident Command
- Establish a secure perimeter or cordon
- Establish safe base of operations considering:
  - Explosive devices
  - Hazardous materials
  - Meteorological and topographic conditions.
- Gather information regarding the incident/ threat/suspect substance (hazard and risk assessment) – eliminate explosive, radiological and chemical hazards
- Determine the level of response required

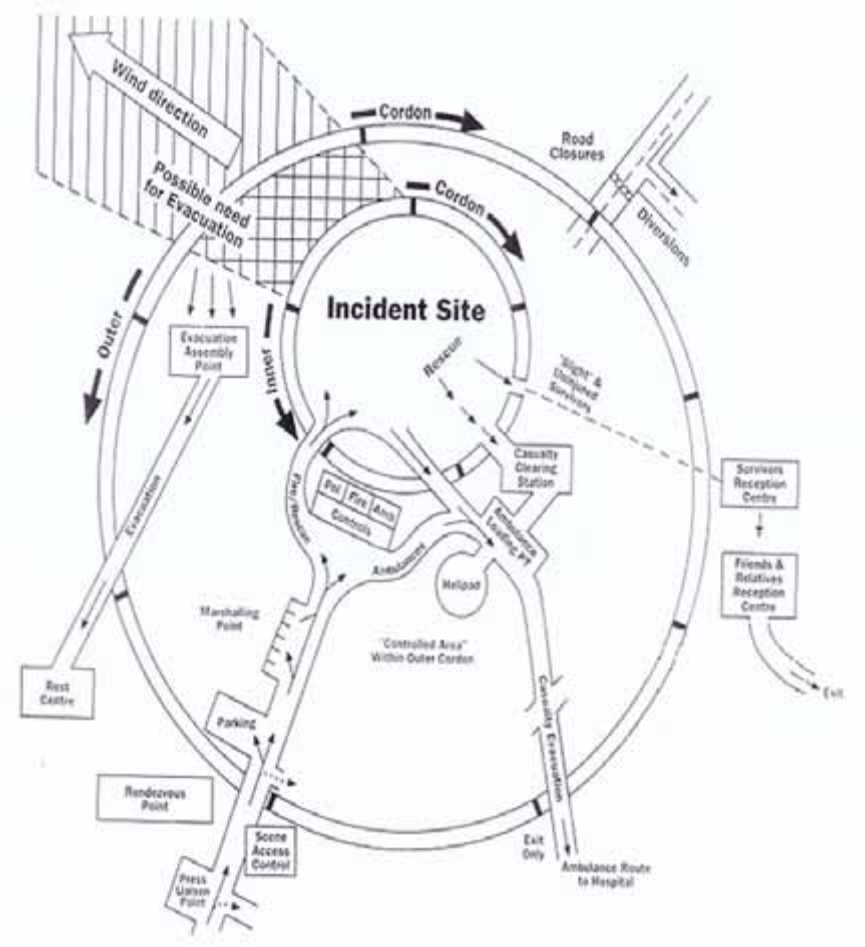
BOX 23
continued

- Identify hot, warm and cold zones
- Develop and implement a site safety plan
- Ensure hazard containment
- Ensure no responders enter contaminated area without proper PPE
- Establish access-control point – establish a single point of entry into the zone and a control entry board to ensure complete knowledge of personnel on the site at any given time
- Brief personnel about on-site safety
- Collect contact details and identification information from victims
- Identify and interview witnesses
- Bear in mind the risk of perpetrators still being present on scene
- Designate health and laboratory liaisons
- Establish personnel and evidence decontamination corridor
- Determine if additional resources and actions are required
- Develop an evidence recovery plan
- Co-ordinate with receiving laboratory decontamination corridor
- Establish personnel and evidence decontamination
- Implement evidence recovery plan
- Conduct full handover briefing for the agency responsible for remediation and site clean-up
- Notify domestic and international partner agencies

Onsite briefing. © Robert Koch Institute

The approach to use is similar to that of Consequence Management, which should include the following aspects:

- Command and control – multi-agency response
- Site security
- Survivor reception
- Hospital procedures
- Disaster victim recovery and identification – mortuary process
- Joint police-health media strategy
- Public reassurance
- Decontamination
- Return to normality.



Conceptual model illustrating incident site management.
© Metropolitan Police Service UK

2. Conducting an on-scene threat assessment

When law enforcement services arrive at the scene, information must be collected as quickly and efficiently as possible. Information gathered prior to arrival is often incomplete or, in many cases, contains errors or misstatements. Law enforcement may collect information by conducting interviews of victims or witnesses, reviewing images from the security (video tapes), or examining evidence.

After gathering the initial facts regarding the situation, law enforcement should initiate a threat assessment to determine the scope of the threat and whether the threat is credible (this is sometimes also referred to as a "risk assessment"). If the threat is deemed to be credible, a law enforcement investigation should be opened and planning should begin on how to collect evidence in a contaminated environment.

Note: Consult appropriate authorities to determine safety or Personal Protective Equipment needs prior to handling potentially exposed victims or evidence.

NOTIFY APPROPRIATE AGENCIES IF THREAT IS CREDIBLE

If the threat is credible, law enforcement should ensure that the appropriate authorities are notified immediately. Countries may have different mechanisms to ensure such notification, but it is recommended that procedures be developed especially between law enforcement and public health services to ensure direct communication with public health authorities when a credible bioterrorism threat exists. Public health can assist law enforcement in a variety of ways, as mentioned previously, and may begin recommending disease-control measures in order to protect the

public. Other agencies that may be notified by law enforcement include: hazardous materials specialists who have been trained to collect contaminated evidence; fire department personnel who can provide decontamination support; and the appropriate biological-agent laboratory that can conduct tests to confirm the presence of the agent.

3. Hazard and risk assessment

HAZARD CONTROL ZONES

Ensuring the safety of responders within any potentially contaminated environment includes the appropriate selection and use of **Personal Protective Equipment**, adherence to strict **contamination-control measures**, and the presence of **on-site medical personnel**.

Once it has been determined that there are no explosive hazards, a hazard and risk assessment should be conducted after considering the following criteria:

- Types of hazards
- Responder tasks
- Environmental conditions.

Conducting a hazard and risk assessment is a continuous process. The level of PPE can be adjusted according to the level of risk. The purpose of establishing hazard-control zones (commonly called hot, warm and cold zones) is to avoid unnecessary exposure. It includes access control and setting up decontamination procedures for personnel, equipment and evidence. Decontamination is a critical component of these procedures and must be in place before any responder enters the contaminated area.

BOX 24

ACTION

COMPONENTS OF A BIOLOGICAL-HAZARD ASSESSMENT

- Establish a safe base of operations: uphill and upwind safe area
- Assess explosive hazards
- Assess chemical hazards
- Assess radiological hazards
- Gather all relevant information:
  - Explosions
  - Victims' symptoms
  - Time from exposure to onset of symptoms
  - Smells
  - Observable agents/materials, devices, containers or debris
- Model potential downwind risk and hazard area
- Determine potential victims at risk:
  - Consider evacuation
  - Consider medical intervention
  - Consider shelter on site
- Develop an Incident Action Plan which will include:
  - Operational objectives
  - Site safety plan
  - Evidence recovery plan
- Select the appropriate level of PPE
- Identify or utilize available detection and monitoring equipment
- Determine evidence-recovery equipment and teams
- Ensure that the scene is photographed or filmed prior to being disturbed
- Screen evidence for radiological and chemical hazards and collect samples for lab analysis
- Co-ordinate sample preparation with receiving laboratory

4. Safety for personnel by training, protective gear and decontamination

In order to ensure personal safety for law enforcement and support agencies at a contaminated crime scene, training, equipment and support must be provided to the officers.

TRAINING

Training in the recognition of potential incidents and hazards, the use of personal protective and detection and monitoring equipment, incident mitigation tools and methods, and inter-agency concepts of operations, is critical for the success of the response.

PERSONAL PROTECTIVE EQUIPMENT (PPE)

There are several levels of PPE. Each level provides some type of dermal and respiratory protection (see Chapter II.6 for more information). The selection of PPE is determined by conducting a hazard and risk assessment which includes, but is not limited to, identifying potential CBRN threats, oxygen levels, and tasks to be conducted.

DECONTAMINATION SUPPORT

Law enforcement operations within a contaminated crime scene must be supported by a decontamination corridor to safely move responders, equipment and evidence out of the scene.

Decontamination tent. © INTERPOL

MEDICAL COUNTER-MEASURES

Medical staff must be on the scene to care for responders. Medical monitoring must be provided for all personnel entering and exiting the scene. Of particular importance is the ability to deal with heat-stress injuries as well as provide prophylactic treatment for responders against accidental exposure to the agent. Depending on the agent, it may be necessary for medical personnel to administer antibiotics or vaccines to responders and to continue medical monitoring for a prescribed period after the event.

Decontamination tent. © INTERPOL

Medicines. © Shutterstock

5. Containment

The purpose of containment is to reduce the risk to the public and responders, as well as to preserve evidence. Because a terrorist may target an open-air event or an event within a structure, containment strategies must be developed for each type of scenario. Evacuation of potential victims should take place first before containment. As soon as possible after victims are removed, a containment strategy should be employed.

BOX 25

ACTION

INDOOR ATTACKS MAY BE CONTAINED BY

- Turning off ventilation systems
- Closing doors and windows
- Shutting down elevators
- Restricting air flow by sealing ducts, windows, doors
    - Use tape, sheet plastic or expanding foams

Ventilator. © Shutterstock

BOX 26

ACTION

OUTDOOR ATTACKS MAY BE CONTAINED BY

- Physically covering the device or dispersed substance
- Lightly spraying the visible dispersed materials with water and bleach mixtures and employing other available commercial systems for agent containment

BOX 27

ACTION

DECONTAMINATION PROCEDURES SHOULD AS A MINIMUM PROCEED AS FOLLOWS

1. Rinse outer garments through the application of a light spray of soap and water.
2. Disrobe the responder following Standard Operating Procedures (SOP).
3. Thoroughly decontaminate equipment and the first container/bag that contains the evidence (double bag procedure) removed from the scene.
4. Dispose of contaminated waste as hazardous waste.
5. Rule out potential remnant contamination.

While decontamination procedures should be also put in place for members of the public affected, it is important for the safety and well-being of the staff involved that appropriate decontamination procedures be put in place for those who have been in contact with the agent or who have been deployed in an operational mission in the hot zone.

Doffing PPE with assistance. © Robert Koch Institute

6. Evidence recovery

The collection of contaminated evidence may be conducted under either covert or overt situations depending on each country's legislation.

Specially trained and equipped crime-scene personnel may recover and/or interpret evidence within the crime scene and from victims.

Evidence removed from the site must be handled and packaged in a way that:

- Maintains sample integrity
- Ensures chain of custody, and
- Ensures the sample is from the original source and is free from contamination.

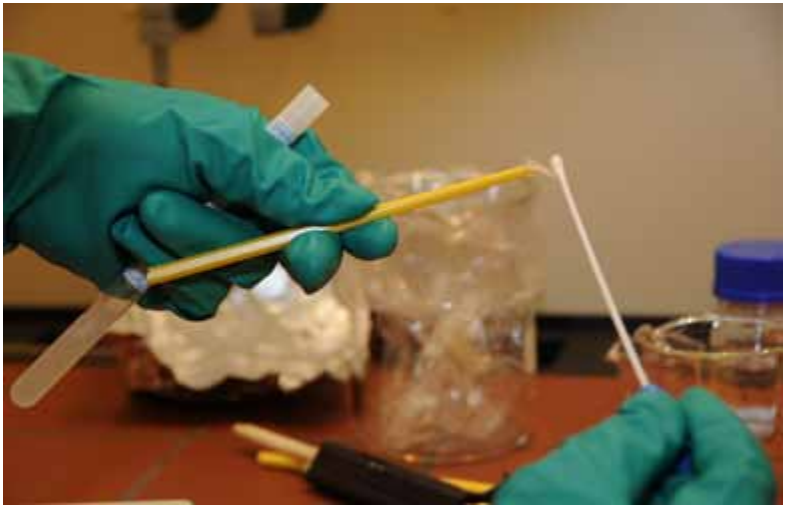
This phase is undertaken only if the environment is safe to work in; personal and public safety is the primary concern.

BOX 28

ACTION

COMPONENTS OF EVIDENCE RECOVERY

- Scene assessment and hazard identification
- Recording of the scene using photography/video
- Collection of suspicious substances for further testing
- Collection of contaminated items for forensic examination
- Interaction between law enforcement and public health specialists or equivalent.



Sampling. © Robert Koch Institute

6.1 Sample collection at a contaminated crime scene

Biological substances are hard to detect and have limited immediate effects. Therefore, unknown substances need to be tested for the presence of other hazards, such as toxic chemical and radiological materials. Please refer to specific guidelines for such testing.

The sample collection procedures that follow are to be employed during an investigation where it is suspected that the substance is of a biological nature.

Collection of biological evidence should be performed by specially trained personnel following specific procedures that are established and co-ordinated with the receiving analytical laboratory.

CRIME SCENE SAMPLING TEAM

The composition of the sampling team will vary according to country-specific legislation and incident-specific requirements. As a general rule, the crime scene sampling team should consist of at least three operators: two individuals for sample collection (assistant and sampler) and one as a note-taker/photographer.
What are their roles?

1. Assistant - Ensures containers are pre-labelled with identifying numbers; opens packaging; hands items to the sample collector for each task.

2. Sampler - Receives items from assistant; collects sample and seals packaging; places in evidence bag; avoids touching other items.

3. Note-taker/photographer - Photographs items at the scene. Records information about the sample description and location of collection.

Notetaker. © Robert Koch Institute

CONTROL SAMPLES

Control samples may be required as evidence during court proceedings to indicate that collection vessels and samples are free from environmental contamination.
Whenever possible, prepare control samples for each type of environmental sample taken at a sampling site. For example, if collecting a soil or water sample from a contaminated site, also collect a sample of soil from an area not covered by the investigation but similar to the site being investigated, and label it as a "control sample".

Blank samples are used to prove the sterility of the collection equipment. Blank samples of collection media and utensils are prepared and packaged in the same manner as the actual samples, although they are not subjected to a contaminated surface or substance. The blank and control items should preferably be from the same batch or equipment number as the items used during the actual sampling. Control samples and blank samples are prepared away from the contaminated site and stored for future cross-referencing should they be required.

Control samples. © Robert Koch Institute

GENERAL OPERATIONS

Prior to entering a contaminated crime scene, ensure that the following have been prepared or conducted.

Site Safety Plan - to identify environmental, structural and other risks and plan for reducing or eliminating these risks. Seek expert advice where required.

Sampling Plan - to identify the order and priority of samples to be collected, based on information/intelligence from the scene, witnesses and investigators. The sampling plan will also assist in determining the type of equipment and other resources required.

Remember that all equipment that enters the contaminated crime scene or incident site needs to exit through decontamination and will become wet.

BOX 29

ACTION

PRE ENTRY PREPARATION

- Conduct site safety briefing
- Prepare a sampling plan
- Contact appropriate receiving laboratories
- Identify necessary equipment, try to use as much disposable equipment/tools as possible
- Separate equipment for each sampling task into itemized packages/kits, for example:
  - Liquid
  - Powder
  - Documents
  - Microscope slides.
- Label containers for each of the collection items
- Check the prepared sampling kits against the sampling plan
- Organize spare equipment
- Prepare control samples and blanks (refer to the "Control samples" section above)
- Prepare other necessary equipment before entry:
  - basket, bucket or plastic bag for carrying sampling equipment
  - sample equipment/kits
  - plastic sheets for the floor
  - cameras/video equipment (waterproof housing)
  - radio (waterproof or wrapped in plastic)
  - waterproof note pad and pens.
- Consider possible deployment of onsite detection equipment (rapid test kits, portable PCR-analyser)

BOX 30

ACTION

EVIDENCE COLLECTION GUIDE

- Identify each team member and their role: sampler, assistant, note-taker/photographer.
- Enter the scene, and identify and establish a "clean" working area.
- Photograph the scene.
- Place plastic sheeting or other barrier onto the clean area and place all equipment in this area.
- Mark sample areas or items to be collected with an indicator tag; photograph and record them.
- Sample collector and assistant can begin to collect items according to the sampling plan.
- Sample collector should wear multiple pairs of gloves, changing outer gloves between each sample.
- At no time should the innermost gloves be removed in the contaminated area.
- Sampling gloves and tools (such as pipettes) must be used only once for each sample or sampling area and then placed into the hazardous-waste bag or container.
- The Assistant labels all primary (inner) and secondary (outer) sample containers with their identifying information.
- The Sampler collects the sample and transfers it to the appropriate collection tube/jar. This inner tube is then placed in outer tube (the secondary container).
- The Note-taker/Photographer is to record the date, sample identifier and a description of the sample, and document all photographs taken.
- Place packaged sample into a labelled plastic zip-lock bag or other protective bag and move onto the next task.

BOX 30 continued

- Ensure that these potentially hazardous materials are transported in a clean and secure container that complies with national and/or international requirements.

6.2 Examples of sample collection

BIOLOGICAL LIQUIDS

Biological liquids such as liquid media or culture broth can be packaged safely in sterile plastic tubes. The aim of packaging the samples is to preserve the sample and to create a safe transportation vessel.

BOX 31

ACTION

BIOLOGICAL LIQUID SAMPLING PROTOCOL

- Label the centrifuge tubes with identifying numbers
- Use a disposable pipette to transfer 1-3 ml of the liquid to the sterile centrifuge tube and seal the lid
- Seal this container with Parafilm, wax paper, or similar product
- Transfer this centrifuge tube (inner) into another sterile plastic container (outer tube)
- Seal the outer plastic container with evidence tape.

A sterile plastic tube with liquid sample inside.

VISIBLE POWDERS

Biological powders may be found in a number of different forms, colours and textures. Powders should be collected carefully as the creation of aerosols can be hazardous. Respiratory protection should be worn when entering a scene containing dry powders for collection.

Sterile scoop with inner tube, sample over-packed in a 50 ml centrifuge.

BOX 32

ACTION

BIOLOGICAL POWDER SAMPLING PROTOCOL

- Label the tubes with the identifying numbers
- Use a sterile disposable scoop or spatula
- Collect a small amount of powder: sweep away from your body
- Transfer a small quantity to a sterile centrifuge/plastic tube
- Seal the tube with Parafilm or wax paper
- Over-pack this inner tube inside a 50 ml centrifuge/plastic tube, and seal it with evidence tape
- Place the outer tube in a zip-lock bag or plastic container for transport.

6.3 Trace collection

The recovery of trace biological material may include powders, liquids or other material. The collection of trace material should be conducted while preserving other critical evidence such as latent prints and DNA.

To increase the likelihood of recovering trace biological evidence, consider sampling from horizontal surfaces and protected areas such as drawers, heating or air-conditioning vents, cracks and seams in tables or work surfaces.

BOX 33

ACTION

TRACE SAMPLING PROTOCOL

- Remove swab/applicator from the packaging
- Moisten the tip with sterile water to increase its collection capability
- Use it dry if protecting other critical evidence such as latent fingerprints or DNA
- Wipe the swab/surface of applicator, over an area using the entire padded area
- Roll the swab/applicator over approximately a 10 x 10 cm area
- Place the swab/applicator into a labelled 50 ml sterile plastic tube
- Break the swab/applicator handle.
- Seal the tube with Parafilm and evidence tape
- Over-pack the tube inside a plastic container or plastic bag.

Trace collection, swabs and foam-tipped applicator as options.

6.4 General evidence collection

The collection of any item from a suspected biological incident requires appropriate collection and packaging to ensure the protection of critical evidence and eliminate the risk of contamination spread. As a rule, all items must be collected and over-packed in two layers then placed into a clean plastic drum for transport through decontamination.

Items of interest could include:

- Microscope slides
- Agar/culture plates
- Documents
- Glassware
- Electronic devices, such as mobile phones.

Glassware. © Australian Federal Police

BOX 34

ACTION

AGAR/CULTURE PLATE

- Seal the culture plate with Parafilm
- Cover the edge with evidence tape, sign and date it
- Place the plate into a clean plastic bag
- Place in a small plastic drum
- Store at refrigerated temperature.

Examples of general evidence packaging: culture plate sealed with Parafilm and evidence tape.

BOX 35

ACTION

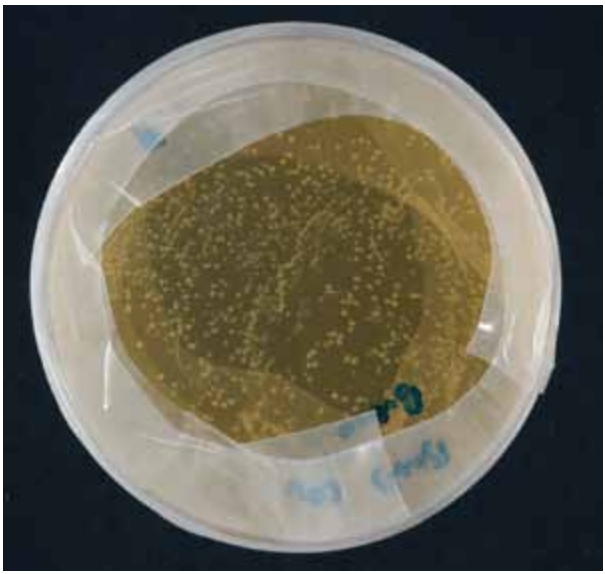
MICROSCOPE SLIDE

- Place the microscope slide into a 50 ml centrifuge tube
- Place Parafilm over the lid
- Over-pack tube into a plastic zip-lock bag
- Place bag into a clean plastic drum for transport.

Examples of small drums. © Robert Koch Institute

6.5 Evidence Integrity

Sample and evidence integrity refers to the item remaining whole, complete and not tampered with. It can be improved through correct use of packaging, labelling and tamperproof seals. The integrity of the sample is important for presenting such evidence in court.



Tamperproof seal. © Robert Koch Institute

6.6 Laboratory chain of custody

All samples collected from a crime scene and/or transferred between law enforcement and public health laboratories require a record of the chain of custody. This refers to documentation giving information about the collection, transfer, analysis and disposal of the item. It should include the signature of each person handling the sample and the date of each transfer.

Laboratory. © Robert Koch Institute

6.7 Evidence preservation

To preserve a sample is to protect it from destruction or degradation. We want to preserve the biological sample, but it may also be important to preserve critical forensic evidence such as fingerprints and DNA.

Biological samples are sensitive to heat and sunlight and may degrade. They should be taken to the receiving laboratory as soon as possible. If necessary, make an effort to keep samples in a cool or shaded area.

When considering storage temperatures consider this rule:

- If it is cold, keep it cold (do not freeze).
- If it is warm, make it cold.
- If it is frozen, keep it frozen.

Incubator.

Samples.

6.8 Laboratory co-ordination

Identify the appropriate public health or specialist laboratory required for sample analysis. Contact the lab prior to transport and discuss the samples to be analysed. Seek advice from the receiving laboratory on sample collection, packaging and screening where necessary.

7. Forensic microbiology and investigation

Forensic science is, in brief, the application of science in the investigation of legal matters. Scientific knowledge and technology varies among disciplines, yet ultimately, this science has the potential to provide the information necessary to determine who committed a given crime.

As with all major crime investigation, the collection and analysis of traditional forensic evidence such as fingerprints, hairs, fibres and DNA can be valuable in the process of first identifying and later prosecuting the offender.

An act of bioterrorism or crime involving the use of a biological agent brings with it a new branch of forensic science – forensic microbiology – that seeks to identify signature traits and markers related to the biological agent used, as well the application of traditional forensic science to items contaminated with a viable biological agent.

Forensic microbiology is a scientific discipline dedicated to analysing evidence from a bioterrorism act or crime, or the inadvertent release of micro-organisms/toxins, for the purposes of attribution.

Attribution does not refer to the identification of the pathogenic organism alone but, more importantly, to the persons who committed the crime. In addition to the collection of traditional forensic evidence, investigators may need to consider analysing the specific make-up of the agent in question (e.g. the strain or species type). This knowledge might reveal manufacturing traits (e.g. remnants of culture media), weaponization traits (e.g. flow agents and additives) or geographic information that might, in turn, help to narrow the field of suspects.

Such testing will be limited to specialists' laboratories that may not be available within your own country. Law enforcement and public health authorities should seek out those laboratories capable of conducting such testing.

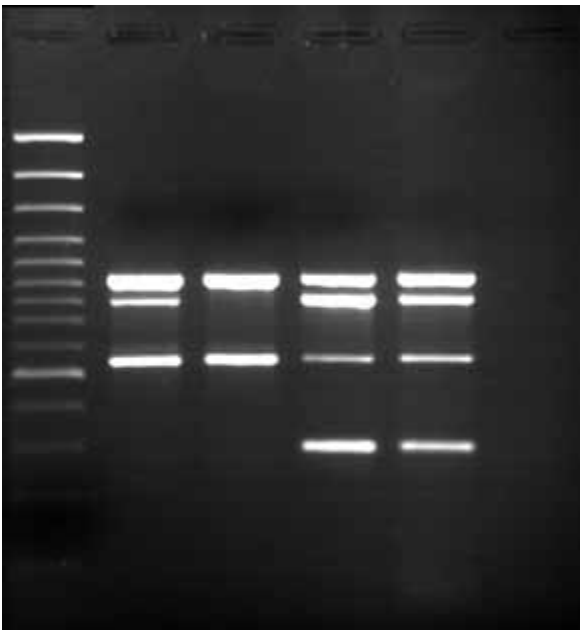
TRADITIONAL FORENSIC EVIDENCE

The collection of both physical and trace evidence is vital both to the investigation and to the ultimate prosecution of the offender. This evidence may be collected from the scene, a person or an item of interest connected to the crime. It may be visible to the naked eye, e.g.: shoe marks, tool marks, firearms and blood. It may also be evidence requiring further enhancement, such as latent marks and trace DNA.

Trained forensic officers collect such evidence as part of a criminal investigation in accordance with local protocols.

It is also important to note that the collection of traditional forensic evidence may be difficult as items of interest may be contaminated and successful decontamination may not be possible without destroying critical evidence. Forensic police may be required to adapt to the challenges presented by a contaminated crime scene.

For example: It is advised that wherever possible, the collection of traditional forensic evidence, such as latent fingerprints and their development, be conducted on the scene and recorded using digital imaging with waterproof housing.



DNA banding of plague. © Robert Koch Institute

8. Site release

Site release will be done once the competent authority has taken a decision based on the risk assessment and completion of the clean-up process.

After completion of all law enforcement-related operations, clean-up of the incident area can begin. The restoration of an area contaminated with a biological agent requires specialized personnel, equipment and expertise. The clean-up process will depend on the type of biological agent and the resources available to effectively destroy the organism, therefore enabling the site to be returned to the owner. This may take time, especially since some agents are resistant and can remain in the environment for a long time.

Police tape. © Photosdisc

V.

MEDIA MANAGEMENT

Media Management

Terrorists' main goal is to provoke a crisis in society. Thus, an important channel that helps terrorists achieve their aims is the media: newspapers, radio, television and the Internet.
The very role of the media, which is to provide news to the public at large, makes them an obvious target, as was seen in the case of the anthrax letters of 2001 in the United States. Attackers see targeting the media as a way of ensuring more visibility for their actions.

Media outlets themselves should investigate their vulnerability to a bioterrorist attack and how to respond to it, preferably by liaising with the agencies responsible for co-ordinating both prevention of and the response to any incident.

The media can play both a positive and negative role at all stages of the bioterrorist "attack", from early detection to the aftermath

Gathered press. © Istockphoto

and recovery phase. Media management should therefore be part of the overall preparedness strategy, as newsworthiness practically guarantees that any bioterrorist-related incident or attack will receive comprehensive media coverage.

The main elements that prompt demand for news coverage are all present in a bioterrorist attack: panic, the human factor, the possibility of consequences on a global scale, and the non-conventional and thus unexpected method of attack. It is also the nature – and indeed the aim – of terrorist organizations to achieve such media coverage in order to show their actions to the public.

In the case of bioterrorism, it would take only a small attack to spark a situation of general panic. If left to themselves, media outlets would likely release different threatening images and worst-case scenarios, which in turn would drive a large part of the population to seek information from the governmental agencies responsible for bio-preparedness. The effects of a bioterrorist scare would be immense, as a comprehensive effort would be needed to successfully reassure the population.
In the case of a bioterrorist attack, it is also likely that, in the initial stages, the media would spread messages that could have an impact on investigations or an operational response. If governmental agencies do not respond quickly enough, the media may, in their hunger for information, seek out self-proclaimed experts. These "experts" may provide false information and thus spread destructive messages, which in turn would cause further misinformation or even panic.

THE MEDIA AS A POSITIVE FACTOR IN CRISIS MANAGEMENT

Communication with the public should be part of the risk- and communication-management procedures. And far from being shunned, media involvement should be ensured from the very outset.

In order to harness the full power of the media, the following guidelines could be followed at different stages of a bioterrorist crisis.

BEFORE AN ATTACK

Law enforcement and public health agencies should have a flexible emergency communications plan already in place. This plan would give guidelines on how to proceed in the event of a bioterrorist crisis.

At this planning stage, personal contact could be established with the media to ensure that a good working relationship, based on trust, existed. Co-operation would then be much easier if a real crisis occurred. This "institutionalization" of media relations should be part of a corporate media strategy, whereby the procedures and modalities for working with the media are known by all staff members. Precise communication strategies involving biological incidents could easily be integrated with existing emergency planning and would involve all relevant agencies.

It is also recommended that specialist training sessions specifically cover media management, as it will be of vital importance to have procedures ready to put in place when confronted with a threatened or real attack. Additionally, it is highly recommended that the relevant organizations already develop awareness and crisis communication strategies for people living close to facilities storing high-risk biological agents and toxins.

Television coverage. © iStockphoto

DURING A BIOTERRORIST ATTACK

Early involvement – From the very outset, the media should be involved as a responsible and helpful partner in spreading the message about how to counteract the threat. To this end, the public health and law enforcement agencies should join forces and appoint a common spokesperson/PR team. In the event of a crisis or bioterrorist attack, this media and press relations officer (or unit) should immediately take action. Early announcements are crucial, even if the information is incomplete and provisional.

In the early stages of an attack, announcements should be specified as being "temporary" or "based on available information" to avoid retracting statements, which would undermine the public's trust. The media should be informed as soon as possible about the nature of the attack, and they should be given – in clear and understandable language – any scientifically based information on the substance used in the attack and possible dangers.

Co-operation and consistency – The response from the governmental agencies in charge of media management should be co-ordinated in order to present a unified, clear and understandable message to the general public. To this end, common actions such as holding a press conference and issuing regular joint press releases should be envisaged.

The agencies must agree beforehand on the kind of information that is to be shared. They should take into account the type of information that can be given to the public without hampering or influencing the law enforcement investigation or the health response or any other response in the management of the incident. It is important to bear in mind that the message must be consistent in order to be credible.

Methods of reaching at-risk public – The method of spreading the message will vary, depending on cultural differences, the targeted social group, etc. Advice to the public on how to act should be short, simple and easy to follow. Local television and radio stations could be approached in order to spread a message that is both reassuring and informative to the public, explaining how the public could act in a certain situation to stop the spread of the disease.

A broad media plan should be envisaged in order to determine the most appropriate media tool (Internet, television, radio, newspapers) to get the message across to the public most at risk.
The government could also set up a hotline to have an expert give information to interested persons. Private telephone numbers could be given in a crisis, since normal channels of communication with health and law enforcement agencies (via public telephone numbers or contact addresses) are likely to be overloaded with requests about the situation from the general public or the media.

Contact point – A special communications centre should be installed off-location. It is not advised to let officers in the field communicate directly with the press as this might influence or block the operations. However, interaction with the media should take place close to the location of the event, not in an office, to make sure the central communications point remains the main source of information for the public.

BOX 36

SUMMARY

MEDIA MANAGEMENT - THE BASICS ON APPROACHING THE MEDIA:

- Have a communication cell appointed to liaise with the media (if possible already before any incident occurs);
- Reach out early to the press to prevent rumours and misinformation;
- Make sure there is one consistent, reassuring, yet honest message agreed upon beforehand with all relevant agencies concerned;
- Match the communication method to the targeted at-risk population;
- Have a permanent presence and be available to answer questions close to the scene;
- Provide regular updates.

VI.

APPENDICES

1. Glossary of biological terms

Aerosol	A fine suspension of particles or fine liquid droplets suspended in the air.
Agar	Polysaccharide extract of red algae used as a solidifying agent in various microbiological media. May be a dry powder or a gel at room temperature.
Anthrax	A serious disease caused by *Bacillus anthracis*, a bacterium that forms spores. There are three modes of anthrax infection: skin, lungs and digestive system. The bacteria are found in the soil and infect grazing animals.
Antibiotic	A substance that inhibits the growth of, or kills, micro-organisms.
Antiserum	The liquid part of blood containing antibodies, which react against disease-causing agents such as those used in bio-weapons (BW).
Aseptic techniques	Precautionary measures taken in the field and the laboratory to prevent the contamination of equipment, people, animals or plants by extraneous materials or other micro-organisms.
Bacteria	Single-celled organisms that multiply by cell division and that can cause disease in humans, plants or animals.

Botulinum toxin	Toxin made by the bacteria *Clostridium botulinum*. This toxin causes botulism, a muscle-paralysing disease. Exposure can be by inhalation, ingestion or injection of the toxin. It is not transmitted from person to person.
Causative agent	The organism or toxin that is responsible for causing a specific disease or harmful effect.
Contagious	Capable of being transmitted from one person to another, one animal to another and between people and animals.
Culture	A population of micro-organisms grown in a medium. The medium may be liquid or solid.
Culturing	The process of growing bacteria in a prepared medium (e.g., a liquid or solid).
Decontamination	The process of making people, objects or areas safe by absorbing, destroying, neutralizing, making harmless or removing the hazardous material.
Dual-use agent	Agents with legitimate use that could be exploited or used maliciously.
Fungi	Any of a group of organisms mainly characterized by the absence of chlorophyll, the green compound found in other plants. Fungi range from microscopic single-celled plants (such as moulds and mildews) to large plants (such as mushrooms).
Genetic engineering	The techniques involved in altering the characteristics of an organism by inserting genes into its genetic material.

Hazard assessment	Evaluating and ranking potential hazards by their estimated frequency and intensity, and determining a margin of safety. Risk analysis is based on hazard assessment.
Host	An organism, animal or plant that acts as the habitat for the growth of another organism.
Infectious agents	Biological agents capable of causing disease in a susceptible host.
Infectivity	(1) The ability of an organism to spread. (2) The number of organisms required to cause an infection in secondary hosts. (3) The capability of an organism to spread out from the site of infection and cause disease in the host organism.
Line-source delivery system	A delivery system in which the biological agent is dispersed from a moving ground or air vehicle in a line perpendicular to the direction of the prevailing wind. (See also "point-source delivery system")
Medical monitoring	Assessment of individuals' health and well-being by competent medical personnel.
Micro-organism	Any organism, such as bacteria, viruses and some fungi that can be seen only with a microscope.
Mycotoxin	A toxin produced by specific fungi.
Organism	Any individual living thing, whether animal or plant, fungus, virus or protistan.
Pathogen	Any organism capable of causing disease in humans, animals, plants and micro-organisms.

Pathogenic agents	Biological agents capable of causing disease.
Plague	A disease caused by *Yersinia pestis*, a bacterium found in rodents and their fleas in many areas of the world. There are two main forms of plague: pneumonic (lung infection) and bubonic (infection of the lymph glands). The pneumonic plague variety can be spread from person to person.
Point-source delivery system	A delivery system in which the biological agent is dispersed from a stationary position. Under the same conditions, this delivery method results in coverage over a smaller area than with the line-source system. (See also "line-source delivery system")
Ricin	A toxin that can be made from castor beans. Intoxication may be via inhalation, ingestion or injection of the toxin. Castor bean plants are grown all over the world and are used to make castor oil. Ricin intoxication cannot be transmitted from person to person.
Risk assessment	The process to determine risk-management priorities by evaluating and comparing the level of risk against predetermined standards and other criteria. It describes the context within which the problem is located, identifies gaps in knowledge and measures likelihood and impact.
Route of exposure (entry)	The path by which a person comes into contact with an agent or organism; for example, through breathing, ingestion or skin contact.

Smallpox	A disease caused by the virus *Variola major* and *Variola minor*. It is a serious contagious disease in humans. At present, smallpox has been eradicated in the world population.
Spore	A reproductive form some micro-organisms can take to become resistant to environmental conditions, such as extreme heat or cold, while in a "resting stage".
Threat assessment	Strategic-intelligence products that provide analysis of the capabilities, intentions, vulnerabilities and limitations of groups posing a crime or security threat. Their outlook is generally long term and future oriented.
Toxicity	A measure of the harmful effect produced by a given amount of a toxin on a living organism. The relative toxicity of an agent can be expressed in milligrams of toxin needed per kilogram of body weight to kill animals.
Toxins	Poisonous substances produced by living organisms.
Tularemia	A disease caused by the bacterium *Francisella tularensis*. It is highly infectious, with a small number of bacteria needed to cause disease; it is not transmitted from person to person. Tularemia is typically found in animals and is most prevalent in rodents.
Vaccine	A preparation of killed or weakened micro-organism products used to artificially induce immunity against a disease.

Vector	An agent, such as an insect or rat, capable of transferring a pathogen from one organism to another.
Venom	A poison produced in the glands of some animals, for example, snakes, scorpions or bees.
Virus	An infectious micro-organism that exists as a particle. Particle sizes range from 20 to 400 nm. Viruses are not capable of reproducing independently outside a host cell.

2. Useful links

INTERNATIONAL ORGANIZATIONS

World Health Organization:

- http://www.who.int

United Nations:

- **Biological Weapons Convention Implementation Support Unit:** http://www.unog.ch/bwc/isu/
- **United Nations Office of Disarmement Affairs:** http://www.un.org/disarmament/

NATIONAL INITIATIVES AND LINKS

Canada:

- **Link to the CBRN training of the RMCP:** http://www.rcmp-grc.gc.ca/fsis-ssji/firs-srij/cbrn-eng.htm
- **General website:** http://www.rcmp-grc.gc.ca/secur/index-eng.htm

United States:

- **United States Centers for Disease Control:** http://www.cdc.gov
- **Sandia National Laboratories:** http://www.sandia.gov , http://www.biosecurity.sandia.gov
- **WMD Unit of the Federal Bureau of Investigation:** http://www.fbi.gov/hq/nsb/wmd/wmd_home.htm

Germany:

- **Robert Koch Institute:** http://www.rki.de

United Kingdom:

- **Home Office:**
  http://security.homeoffice.gov.uk/cbrn-resilience/equipping-emergency-services/

Australia:

- **Australian Federal Police CBRN Data Centre:**
  http://www.afp.gov.au/what-we-do/operational-support/australian-chemical-biological-radiological-and-nuclear-data-centre.aspx

For more links to useful websites, please consult the Bioterrorism website on the INTERPOL site:
http://www.interpol.int/Public/BioTerrorism/default.asp

3. National details on bio-preparedness

Please write down any national details on bio-preparedness to complete this guide.

INTERPOL

For official use only

INTERPOL General Secretariat
Bioterrorism Prevention Programme

200 Quai Charles de Gaulle
69006 LYON – FRANCE

Telephone: +33 4 72 44 70 00
Fax: +33 4 72 44 71 36

http://www.interpol.int/Public/contact.asp

or contact your
INTERPOL National Central Bureau