COMMISSION OF THE EUROPEAN COMMUNITIES

Brussels, 24.6.2009
SEC(2009) 874

COMMISSION STAFF WORKING DOCUMENT

Bridging Security and Health: Towards the identification of good practices in the response to CBRN incidents and the security of CBR substances

{COM(2009) 273 final}

COMMISSION STAFF WORKING DOCUMENT

Bridging Security and Health: Towards the identification of good practices in the response to CBRN incidents and the security of CBR substances[1]

Introduction

This Commission staff working document "Bridging security and health: Towards the identification of good practices in the response to Chemical, Biological, Radiological, Nuclear (CBRN) incidents and the security of CBR substances" focuses on the cooperation between public health and Law Enforcement authorities at national level, between Member States and at EU level. The Commission provides with this document a compilation of identified good practices which aims at helping Member States to improve their national structures, raise awareness and enhance European cooperation and coordination.

This document has been developed on the basis of the results of training programmes and joint train-the-trainer events between Public Health and Law Enforcement services organised by the Commission together with Europol and the European Centre for Disease Prevention and Control (ECDC) in March 2004 and June 2007.

These training events, which mixed case-studies based on based on lessons learned from real events and technical presentations, brought together Law Enforcement and Public Health officials to foster an improved understanding of the investigative goals and methods specific to each discipline. These trainings also aimed at strengthening interdisciplinary collaborative effectiveness in response to future deliberate contaminations with biological or chemical agents. The training increased participants' familiarity with their law enforcement and public health counterparts in their home jurisdictions. It became clear that preparedness in the Member States requires attention to specific situations for each service involved, such as: conducting epidemiological investigations and public health responses in the setting of a crime scene; meshing criminal investigative procedures with epidemiological, laboratorial, and other scientific procedures in such settings; joint media communications from law enforcement and public health operations.

Between February and May 2008, three further regional workshops were organised with a limited number of EU and national experts together with Member States representatives from Law Enforcement and Public Health. They met in Slovenia, Portugal and Luxembourg to respond the request of the participants of the previous training events for more guidance on establishing an improved collaboration between law enforcement and public health at national level. The outcome of these workshops, where participants further shared their experience considering their own systems and mechanisms in the light of experience of other Member States, is the fundament of the present document.

This Commission staff working document is part of the CBRN package adopted by the Commission on 17th June 2009. This paper should be seen as separate from the CBRN Action

[1] This Commission Staff Working Document accompanies the Communication on "Strengthening Chemical, Biological, Radiological and Nuclear Security in the European Union", adopted on 24th June 2009.

Plan and focuses solely on the possible cooperation between public health services and law enforcements agencies in the specific event of a CBRN incident. However, this document is not a manual on how to develop this collaboration and does not provide policy recommendations or actions which should be implemented by Member States in a given time frame – it only offers best practices as source of inspiration. In as far as the workshops have led to policy recommendations these have been included in the EU CBRN Action Plan.

This document provides a list of topics in a chronological response order, not in a priority order. Relevant good practices in the field were identified and examples of how the issues raised could be dealt with at national level are provided. In addition, each chapter contains a checklist of key questions tailored to public health and law enforcement authorities in order to assist them in identifying gaps and needs in their national preparedness plans. Further references are included to provide more detailed information on the single topics dealt with.

The list of topics and issues covered by this document is not intended to be exhaustive. The paper particularly does not intend to and cannot derogate from the applicable legislation for public health professionals or law enforcement agencies in the European Union, or replace existing recommendations and practices which have been developed in specific sectors (e.g. the security issues of nuclear substances are not addressed) or by international organisations (e.g. international guidance agreed at the IAEA). Member States are invited to use this document as a starting point to apply and further develop good practices in the collaboration between public health and law enforcement authorities and to improve their national preparedness plans accordingly.

Any new measure or action, particularly in the field of information exchange, must respect fundamental rights and observe the principles recognised in particular by the Charter of Fundamental Rights of the European Union and the Convention for the Protection of Human Rights and Fundamental Freedoms, notably the right to private life and the right to protection of personal data.

The protection of personal data, in particular relating to a person's health and medical data, is of key importance to a person's enjoyment of his or her fundamental right to respect for private and family life and to the protection of his or her personal data as guaranteed by Article 8 of the European Convention of Human Rights, Article 8 of the EU Charter of Fundamental Rights and the legal provisions on the protection of personal data under European Community and European Union law[2]. Respecting the confidentiality of health data is a vital principle in the legal systems of all Member States in the European Union. It is crucial not only to respect the sense of privacy of a patient but also to preserve his or her confidence in the medical profession and in the health services in general.

Therefore, in the framework of a possible cooperation between public health services and law enforcements agencies in the specific event of an CBRN incident, anonymous or

[2] See, in particular, Article 8 and 13 of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23.11.1995, p. 31); Article 10 of Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (OJ L 8, 12.1.2001, p. 1); Article 6 of Council Framework Decision 2008/977/JHA of 27 November 2008, on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (OJ L 350, 30.12.2008, p. 60).

pseudonymous data must be used, whenever possible. In case the processing of personal data relating to health is necessary in a specific case, Member States must afford appropriate safeguards laid down by law to prevent any such communication or disclosure of personal health data as may be inconsistent with the guarantees under EU law.

SUMMARY

THREAT RECOGNITION AND ASSESSMENT

1. **Preliminary practices, criteria and conditions necessary to allow interacting between law enforcement and public health** - It is essential to establish communication mechanisms between law enforcement and public health. Most important are agreements between law enforcement and medical and public health communities that include:

   – An early notification system where law enforcement is informed of any emerging suspicious health issues by public health

   – Collection and handling of evidence

   – Co-operation with other national/international health and law enforcement organizations.

2. **Risk and threat assessment, information exchange & joint working–** taking the necessary legal framework into consideration, a strong working relationship between law enforcement, and public health and other competent authorities is essential to responding effectively to a terrorist incident or deliberate malevolent act. Both public health officials and law enforcement personnel require intelligence that helps in their tasks - the exchange of such intelligence should be set up and fully respecting the applicable legal requirements.

EU AND INTERNATIONAL FRAMEWORK

3. **Available EU and relevant international alerting and medical intelligence tools and their usage requirements** – EUROPOL is the organisation which facilitates the exchange of information and the cooperation between the competent authorities of the Member States in preventing and combating serious international organised crime and terrorism. Effective information exchange requires that law enforcement and public health personnel are familiar with one another and know which people in each agency should receive the information. Health authorities are bound to communicate to each other the appearance of public health threats.

JOINT PREVENTION

4. **Personnel security & management** - Employers have a responsibility to monitor and support staff who have access to hazardous materials, and need to ensure that employees comply with increased security measures to protect hazardous materials and information assets. This includes vetting of staff and control of visitors to sensitive sites.

5. **Facility security & management** - law enforcement competent authorities have to minimise the risk of theft, diversion, malicious use, or illicit use of CBRN agents also, to ensure compliance with security and safety measures imposed by law for CBRN agents. Because CBRN agents, especially dangerous biological pathogens, are stored in many legitimate laboratory facilities within a nation, a first step in prevention is to improve security at these facilities. In addition, legislation restricting

the purchase of dual-use laboratory equipment, and regulations on the transportation of CBRN agents is in place. Also, avoiding proliferation of potential dual-use knowledge on CBRN agents must be subject of security measures.

Safe and secure laboratories help:

- Ensure the containment of hazardous infectious substances
- Protect valuable research and commercial assets
- Minimize risk of accidental exposure or release
- Reduce the risk of crime and bioterrorism

The creation of outreach programs that increase the level of terrorism awareness and information exchange between law enforcement, industry and scientific communities will facilitate the reporting of suspicious activities.

6. **Transportation security, material control and accountability** – This is a sensitive issue, because security in this area means: monitoring of dangerous goods carried, measures to be taken in case of emergencies and exchange of information among competent authorities of the Member States concerned..

JOINT ASSESSMENT AND WORKING

7. **Joint risk and threat assessment of suspicious incidents** – it is essential to establish communication mechanisms between law enforcement and public health authorities. These mechanisms and the criteria used to prompt information exchange should be developed with consideration of pertinent laws and regulations protecting both the sensitive data of law enforcement and confidential medical information. Effective information exchange requires that law enforcement and public health personnel are familiar with one another and know which people in each agency should receive the information. It is essential to have an established information exchange protocol between law enforcement and public health authorities to avoid potential delays in responses.

JOINT RESPONSE

8. **Personal Protective Equipment (PPE) of involved staff; protecting investigators** – the level of available personal protective equipment will dictate the precise role of first responders at a suspected CBRN incident. There are a number of different forms of suitable PPE, with selection being determined by the type of the CBRN threat, work environment and type of personal decontamination facilities in operation. Respiratory protection is critical since inhalation is one of the primary routes of exposure especially for many chemical and biological agents. Prompt and thorough hazard assessment (and hazard management including the availability of decontamination facilities) is vital to ensure the safety of responders and the public. Hazard assessment involves determining the nature of the agent, the efficiency of dispersal and predicted dispersal pattern. Hazard assessment distinguishes between actual events and hoaxes.

9. **Definition and enforcement of area-security and hot/safety-zones for the purposes of an investigation** – the area in which a terrorist attack occurs should be considered as a crime scene. Law Enforcement personnel are familiar with the procedures for handling and documenting evidence. However, response personnel may be required to assist in the case where a vast quantity of evidence needs to be recovered. The location should be secured and an inner and outer cordon established, in line with applicable minimum standards. The hot zone is the innermost zone and immediately surrounds the release site, munitions or device. All personnel within the hot zone should be in appropriate Personal Protective Equipment. Appropriate barrier management has to be provided to avoid secondary contamination. Entry/exit from the hot zone is controlled at a single Entry Control Point. With regard to CBRN response a clear distinction should be made between the forensic process (collecting evidence, including analysis of samples suspected of containing agent, precursors and degradation products) having its own relatively long time-line and urgency and the immediate crisis response process which includes sampling &identification for the purpose of rapid identification of nature and severity of the incident. The latter is of crucial relevance to crisis management decision taking in the order making distinction between hoaxes and true CBRN incidents, up/down-scaling, evacuation etc. Although in part forensic methods may be shared by both processes, stakeholders and urgency are quite different.

10. **Laboratory issues: Maintenance of chain of evidence** – the chain of custody is the methodology used to track and maintain control and accountability of all evidentiary items. This includes the whole process from initial collection of the evidence to the final disposition of the specimens. Both law enforcement and public health personnel must provide accountability at each stage of collecting, handling, testing, storing, transporting the evidentiary items, and reporting any test results. Failure to properly maintain the chain of custody may prevent the evidence in question from being accepted in a court of law. It should be noted that evidence collected in a potentially contaminated environment must be assumed to be contaminated. This will significantly complicate the evidence review and evaluation process. Maintenance of the chain of custody may be vital to ensure that evidence gathered in the course of an investigation is useable to convict the perpetrators. On the other hand, law enforcement officials must be sensitive to the public health sector's need to quickly collect and identify possible CBRN agents and eliminate the threat.

11. **Laboratory issues – designation, accreditation, quality assurance and forensic requirements to diagnostics and confirmation of diagnostics** – law enforcement authorities may detect dissemination of CBRN agents through reports of unusual behaviour or discovery of unexpected devices or odours, smoke, dust**.** Public Health, competent authorities and Reference laboratories may be called to provide diagnostic service for CBRN related incidents, but should be aware of the specific requirements**.**

12. **Media and public relations** – terrorist use or threatened use of CBRN agents is likely to have an extreme psychological impact on the civilian population, potentially resulting in challenges for law enforcement. Response planning must include a media strategy. Early coordinated statements in the media by law enforcement, public health, medical and political authorities are vital to provide accurate information and defuse the public's confusion and fear. A joint media team must be included in training and exercises. Distribution of credible, neutral information after a terrorist incident is critical. The media is often the best way to inform the public of what

actions to take during a crisis and post-incident. Messages must be coordinated with Public Health and competent authorities leading for developing and delivering medical/public health information associated with the event, while Law Enforcement must lead on developing/delivering information associated with the criminal investigation.

JOINT TRAINING AND EXERCISES

13. **Training and exercises** – it is essential to provide training in the recognition of potential incidents and hazards, the use personal protective equipment, as well as in the use of incident mitigation apparatus and methods. An inter-agency concept of operations and support means is critical for the success of the response. Public health and medical assets should be incorporated into training. Exercises should be planned and executed to build up relationships and identify and correct potential problems before an actual event occurs.

1. PRELIMINARY PRACTICES, CRITERIA AND CONDITIONS NECESSARY TO ALLOW INTERACTION BETWEEN LAW-ENFORCEMENT AND PUBLIC HEALTH AUTHORITIES

The issues

- Development of joint working relationships before incidents occur
- Management of joint investigations
- Establishment of synergy between law enforcement and public health investigations

Context

There are a number of preliminary practices, criteria and conditions which need to be put in place ahead of time in order to allow effective interaction between law enforcement and competent authorities and public health authorities. Such procedures include the setting up of joint work and its practical implementation, the regular update of each other's contact lists, the targeted identification of incidents, and the understanding of managing conflicting needs.

Threat assessment

Once a threat has been identified, and even before there is a confirmation of the presence of a risk to the public, law enforcement, competent authorities, and public health authorities could set up appropriate channels to exchange information and address a joint operation centre. This would need adequate anticipation, preparation and testing.

The threat assessment process needs to continuously evaluate the additional information derived from public health, law enforcement, competent authorities, and intelligence sources. Management-level law enforcement, competent authorities and public health officials should begin coordinating as soon as possible. Such coordination would enable the implementation of appropriate measures to protect and treat law enforcement personnel who are exposed to suspect material at the scene and elsewhere, as well as to protect and treat the public. If circumstances warrant suspicion that the incident is intentional, law enforcement services will focus their efforts and resources on conducting the criminal investigation as the lead agency.

Investigation

Investigation in the event of the deliberate release of a CBRN agent intends to identify the extent of the threat to national security and to lead to the identification, apprehension, and prosecution of the perpetrator(s). Public health and competent authorities' officials will focus their efforts and resources on conducting an epidemiological investigation aiming at identifying the source(s) and mode(s) of spread of the disease-causing agent, identifying exposed or at-risk persons, implementing measures to control the spread of the disease and treating exposed persons. Criminal and epidemiological investigations should be carefully

coordinated to

(1) avoid unnecessary exposures and duplication of efforts,

(2) facilitate sharing of relevant information, and

(3) otherwise complement each other. In a bioterrorism attack, the most important evidence may be disease- or the injury-causing biological or chemical agent itself.

Evidence

For investigative purposes, the evidence could include:

(1) the specific agent (weapon) itself,

(2) "fingerprints" (through DNA and other analyses),

(3) trail markers (i.e. the agent material could have contaminated every place it has been or was used by perpetrators, including containers, vehicles, and buildings), or

(4) the physical means used for dissemination, e.g. envelopes.

In most instances, the public health investigators who are trained to collect environmental samples and the national public health laboratory will be needed by law enforcement authorities to positively identify the CBRN-terrorism agent, compare that specific agent with other agents, and track the path of the agent.

Media Management

The media will have a significant impact on the response and the public reaction to a CBRN incident as is the case with any health crisis. As a result, each community should use a single point of contact (spokesperson), to be identified by each jurisdiction, to coordinate and disseminate the response to queries This should help ensure that the appropriate information, in particular sensitive information (eg. information about exposure to a potential contamination), is released to the media at the proper time. The establishment of a Joint Information Centre (JIC) comprising the competent law enforcement agencies, competent health agencies, and state and local officials would facilitate the development of coordinated messages. Of note for the EU level are the facts that:

- A press officer exists for DG-SANCO, along with an EU network of Health Communicators
- Europol has its own PR unit and has established a Counter Terrorism media network to facilitate the exchange of information among the appropriate PR units in the police forces of all Member States.
- The ECDC has a Health Communication unit, which is currently building links with the competent bodies for health communication in the national public health institutes in all Member States.

Examples of Good Practice, identified in some Member States

Knowing each other's contact points

Elements of good practice include a regular update of each department's contact details including the contact details of appropriate liaison personnel within the security services.

Procedures for the identification of events and setting up joint operations centre(s)

Public health officials and law enforcement officials can notify and involve each other early in an investigation even if it turns out to be a non-criminal event. For example, for the investigation of clinically confirmed cases of poisoning. It proved key to establish pre-incident communication mechanisms between the law enforcement and the public health communities.

The communication mechanisms seem especially important for the expeditious exchange of information in an actual CBRN incident. This exchange of information would require law enforcement and public health personnel to be familiar with one another, and to know which people in each agency need and should receive the information.

In some Member States, an early association of the Judicial Services to these joint activities is found beneficial.

Setting up of Joint Operations Centre (JOC)

To facilitate the sharing of information between law enforcement and public health officials, a Joint Operations Centre (JOC) that brings together all the elements necessary to respond to a CBRN incident was looked at as a model. Here it seems essential to involve the appropriate agencies in order to fully benefit from personal interaction and ongoing dialogue with those who will be responding to an actual biological or chemical event.

The concept of a JOC model provides a framework to structure and foster a communication capability that bridges the two communities. This concept needs to be implemented at all levels (operational, intermediate and strategic or national level). One way to maximize this framework is to form a CBRN Working Group involving the different agencies. Additionally, a CBRN Working Group can enable the various jurisdictions to identify at an early stage what information will be exchanged, when and to whom it will be provided, based on individual and departmental needs. Planning, training, and exercises prior to an actual CBRN-event can foster the public health officials' comfort level of involving law enforcement early on in their epidemiological investigation. However, to determine that there is a criminal intent, such as terrorism, clearly requires a joint law enforcement / public health investigation.

Joint information centre and establishment of joint information channels

(a) Information exchange channels

The timely exchange of information is critical to an effective response to a CBRN incident.

Yet, there are concerns within each professional community about the type of information that can be freely exchanged. Understanding each other's needs can be addressed in training programmes.

(b) Joint Investigative Information

The successful execution of the criminal and epidemiological investigations during a CBRN incident depends upon the efficient use of all available resources and the very early exchange of appropriate information at the operational, intermediate and command level.

It has been identified as a good practice for public health and law enforcement personnel to work in teams and jointly conduct interviews with victims and witnesses. Prior to the actual interview with a witness or victim, the joint investigation team can decide which person will begin the interview and the other member of the interview team should allow the lead interviewer to complete his or her interview without interruption or disruption to the flow of the questioning. It is recommended that the epidemiological interview proceed first during a joint interview. However, the order of the interviews must be decided on a case-by-case basis. When joint interviews are not possible, the separate investigative communities should be aware of the types of information their counterpart is seeking (see table in background section). Public health personnel could obtain and provide information from their epidemiological investigation to law enforcement personnel that would benefit a criminal investigation. Conversely, the law enforcement community could provide data to public health personnel that would benefit an epidemiological investigation.

The objective of the joint investigation and joint interviews of victims and witnesses is to maximize the efficiency of both public health and law enforcement investigators through the exchange of real-time information.

(c) Best Practices in the area of information exchange

- *1. Establishment of Information Exchange Groups:* At the national level, but also where possible at the regional level, such a group could be created from an existing group, such as the CBRN Working Group, and consist of all the potential players that may be involved in a response to a CBRN incident. This forum could facilitate information exchange.

- *2. Development of Good Personal Relationships:* Strong personal ties between the law enforcement personnel and the public health personnel were identified as fostering information exchange.

- *3. Inclusion of the adequate medical expert in the Criminal Investigation, such as Epidemiologists and Toxicologists:* This individual could be a member of the law enforcement staff or someone detailed to the law enforcement staff on a part-time basis and could help identify criminal information needed by the public health community and provide the necessary information to the law enforcement community.

- *4. Enhancement of the CBRN incident awareness of the Emergency Response Community:* Through training courses or professional associations the awareness can help to heighten the community awareness of the potential triggers that would prompt the exchange of information early in an incident.

- *5. Pre-Establishment of Agreements on the Sharing of Sensitive Information:* Establishing

agreements that identify the rules for the exchange and release of information can alleviate some of the concerns raised by both communities.

- *6. Pre-Establishment of Lab Test Processes and Agreements:* These agreements provide guidance as to how the public health community conducts lab testing for the prosecution of suspects.

- *7. Conduct Chain of Custody Trainings:* This training should be designed to inform the public health community to identify when they need to initiate the chain of custody for evidence in a CBRN incident and help to ensure evidence will be handled properly for the eventual prosecution of the criminal case.

Good Practice Checklist

Public Health	**Law Enforcement**
• Do the Public Health services maintain an updated list of contacts in the Law Enforcement sector for information exchange, investigation, and guidance? • Is the exchange of (sensitive) information laid down in national law and/or formalised? Does an information exchange group or specific legal or operational arrangements with Law Enforcement exist? • Was the possibility of creating of a Joint Operations Centre for common emergencies explored? (some MS have civil protection leading in this task) • Was the possibility explored to obtain security clearances for a number of Public Health service personnel? • Have Public Health service personnel participated in chain of custody training? • Was the possibility of participating in the development of protocols for forensic testing of clinical samples explored?	• Do the Law Enforcement services maintain an updated list of contacts in the Public Health sector for information exchange, investigation, and guidance? • Is the exchange of (sensitive) information laid down in national law and/or formalised? Does an information exchange group with Public Health or specific arrangements on sensitive information exchange exist? Is it possible to include epidemiologists/Public Health professionals in criminal investigations? • Was the possibility of creating a Joint Operations Centre for common emergencies explored? (some MS have civil protection leading in this task) • Were the requirements for security clearances for Public Health personnel participating in criminal investigations established? • Have Law Enforcement personnel conducted Chain-of-custody training? • Have the Law Enforcement authorities developed protocols for forensic testing of clinical samples?

2. RISK AND THREAT ASSESSMENT, INFORMATION EXCHANGE & JOINT WORKING

The issues

- Definition of threat and risk
- Principles for applying risk and threat assessment
- Interaction between public health and law enforcement on risk and threat
- Obstacles/solutions to information exchange
- Developing joint working relationships
- Managing joint investigations

Context

Threat Assessment

The ability to identify threats, to verify them and quantify the risks emanating from them are key stages in the management of the threat from chemical, biological or radiological weapons.

The identification and assessments of threats is principally based on the identification of intent and capability (and impact) of a criminal or terrorist individual or group. Knowledge of the likely targets should also be included. A threat assessment is an intelligence-based judgement, which will often contain highly sensitive information.

The risk posed by an identified threat combines scientific knowledge of the hazardous nature of threat and the vulnerability of the target (and associated people, buildings etc.) to a specific hazard. Risk assessment also should include the likely consequences of an event. The consequences may include not just the immediate physical and psychological impact of the incident, but also the consequences of the efforts that need to be taken to remedy the situation, this as well as the political and economic damage to the country and region. Threat assessments are necessary in order to provide targeted security measures that are appropriate and proportionate.

In the context of law enforcement, the aim of a risk assessment is to identify and examine vulnerable areas of the society that are, or could be, exploited. By examining weak and vulnerable areas, for instance within a certain business sector, it will then be possible to give recommendations about a number of diverse issues such as potential counter measures.

In the context of public health, the aim of risk assessment is to ensure that preventive and reactive measures to protect the public, including ensuring the availability of appropriate

treatments within the local health care systems, guidance and training for health care personnel.

Confidentiality, personal data protection and Security

Bringing law enforcement and public health services closer to each other is clearly of great benefit when dealing with CBRN threats, the exchange of information, knowledge and interpretation being the most significant. The following aspects coming into play for an effective exchange of information need to be taken into consideration:

- Law-enforcement agencies in some Member States work already very closely with national intelligence agencies (sometimes they are the same agency) and are routinely privy to sensitive intelligence information. They are familiar with the restrictive conditions on how intelligence is handled and disseminated; whereas public health services usually are not,

- Public health services staff and health professionals are legally bound by clinician-patient confidentiality requirements and personal data protection legislation.

- Unfamiliarity with the needs and capabilities of each others services, public health and law enforcement agencies may cause them to not fully understand the needs and requirements of their partner agency

- In some cases, information may be protected and in the hands of people not trained in understanding the need to exchange it. Health professionals and clinical staff will in most, if not all cases, be legally bound by professional duties of confidentiality and personal data protection legislation from sharing information with law enforcement authorities, if not specifically authorised to do so by legal provisions for a particular purpose. Law enforcement staff may feel bound by formal systems for protecting information, in particular when it concerns personal data, or classified information. In some EU Member States, information held by law enforcement agencies may be further protected by duties to investigating magistrates .

- To provide a high degree of inter-operability it is therefore necessary for public health and law enforcement services to:

- Developing an understanding of other agencies systems, and of the legal requirements for protecting information and personal data.

- Provide liaison arrangements between their respective agencies

- Identify lawful mechanisms to exchange relevant information and intelligence.

- Europol - as facilitator of the exchange of information between the competent authorities of member states - should also provide all information which has a potential impact on the security of the European Commission in any of its sites through the Security Directorate.

Investigation

The investigation of an incident can have several aims. The principal agreed aims of a law enforcement service investigation - where appropriate in cooperation with competent

authorities - are:

- identifying the extent of the threat to public security;
- managing and minimising the impact of an incident;
- preventing further incidents from occurring;
- the identification, apprehension, and prosecution of the perpetrator(s);

Public health services and competent authorities will focus their efforts and resources on:

- conducting an epidemiological investigation, aimed at identifying the source(s) and mode(s) of spread of the disease-causing agent;
- identifying exposed or at-risk persons, and treating exposed persons;
- implementing measures to prevent further exposure and control the outbreak.

It is clear that some of the aims are common for both the public health, competent authorities and law enforcement services. Therefore, the criminal and epidemiological investigations can, if carefully coordinated, recognise, identify and manage the threat as quickly as possible and hence help to avoid unnecessary exposure of the public or investigators to hazardous materials.

Facilitating the sharing of relevant threat information may ensure the greatest possible efficiency in investigating an incident by minimising duplicated work and help to assign responsibility for work stream to the organisation best able to undertake them.

The role of public health authorities is especially important in chemical, biological or radiological attacks as examination and treatment of the clinical injuries that have occurred may present some of the most important evidence of the type of agent used.

Evidence

Evidence could include elements from the specific agent (weapon) itself, from "fingerprints" (other physical evidence from crime scenes such as DNA and other analyses), from trail markers (i.e., the agent material could have contaminated every place it has been or was used by perpetrators, including containers, vehicles, and buildings) or from the physical means used for dissemination, e.g. envelopes.

Law enforcement authorities will have existing forensic scene investigators, systems for collecting transferring and storing evidential materials and access to specialised laboratories. However, the usual investigators and laboratories may be unfamiliar with the risks associated with sampling evidence from the misuse of CBRN agents. Public health investigators who are trained to collect environmental samples and the National public health laboratory may be needed by law enforcement authorities to positively identify such agents, compare that specific agent with other agents, and track the path of the agent.

Joint interview teams

The most efficient execution of the criminal and epidemiological investigations during a CBRN incident will depend upon the maximum use of all available resources and the very early exchange of appropriate information at the operational, intermediate and command level.

When joint interviews are not possible, the separate investigative communities should be aware of the types of information their counterpart is seeking. Public health personnel could obtain and provide information from their epidemiological investigation to law enforcement personnel that would benefit a criminal investigation. Conversely, the law enforcement community could provide data to public health personnel that would benefit an epidemiological investigation.

Examples of Good Practice, identified in some Member States

- Where appropriate, Public Health, competent authorities and law enforcement personnel should work in teams and jointly conduct interviews with victims and witnesses. An epidemiological interview may proceed first during a joint interview; however, the order of the interviews is decided on a case-by-case basis.

- An information exchange group, at national level, but also where possible at regional level, can be created and should consists of all the potential players that may be involved in a response to a CBRN incident. Moreover, this group can also help to foster personal ties between response officials, facilitating less formal information-exchange relationships.

- Law enforcement and public health personnel have indicated that they would be more likely to provide information to their counterparts early in process if they have worked, talked, or met with them on a regular basis and trusted them.

- Some Member States include an epidemiologist in the criminal investigation, for some as a member of the law enforcement staff or for other someone detached to the law enforcement staff on a part-time basis. Law enforcement and public health personnel indicate that this liaison could help identify criminal information needed by the public health community and provide the necessary information to the law enforcement community.

- Ensuring that systems for vetting and accrediting staff from public health and law enforcement services are in place in order for then to be able to handle and filter classified information.

- Creating an understanding of the legal requirements that apply to the protection of personal data, including confidential patient information where there may be a need to disclose that particular information in clearly defined cases to a law enforcement authority; any such measures will need to be agreed upon in operational arrangements or in national legislation .

- Establish an efficient and clear role for the public health and law enforcement partner towards monitoring and decontamination facilities in relevant hospitals and the use of personnel protective equipment.

- Establish agreements on sharing relevant sensitive information. Establishing agreements that identify the rules for the exchange and release of information could alleviate some of the concerns raised by both communities. These agreements should identify what type of information will be shared, how individuals can exercise their rights as guaranteed by the fundamental right to the protection of personal data, how supervision is guaranteed by the national data protection supervisory authorities and how it will be restricted to limit unintentional release to unauthorized personnel.

- Establish lab test agreements. These agreements provide guidance as to how the public health community should conduct lab testing for the prosecution of the suspects. These agreements would establish what circumstances would necessitate specific lab tests for criminal investigations. The labs to send these samples need to be defined in advance.

- Conduct chain of custody training. This training should be designed to inform the public health community to identify when they need to initiate the chain of custody for evidence in a CBRN incident. This information helps to ensure evidence has been handled properly for the eventual prosecution of the criminal case.

Good Practice Checklist

Public Health and competent authorities	**Law Enforcement**
• Have Public Health services established an information exchange team jointly with Law Enforcement? • Were the key experts for threat and risk assessment within Law Enforcement services identified? • Were common definitions for 'risk', 'threat', and other working terms agreed with the Law Enforcement services? • Were Public Health personnel trained in the differences between threat and threat assessment and risk and risk assessment? • Have the Public Health services considered working with Law Enforcement services towards understanding the different conditions (if any) in force in Law Enforcement regarding the handling of intelligence and evidence? • Have the Public Health professionals to identified and become acquainted with legal mechanisms regarding confidentiality, codes of clinical practice and data protection regulations? • Have the public health services assessed the need for their staff to be subject to security vetting at an appropriate level?	• Have the Law Enforcement services established an information exchange team jointly with the Public Health services? • Were key persons/experts identified to work with in Public Health and was provide threat and risk assessment provided? • Have common definitions of terms for risk, threat, and other working terms been agreed? • Has Law Enforcement personnel been trained to understand the difference between threat/threat assessment and risk/risk assessment? • Are Law Enforcement working with Public Health to understand the different conditions (if any) in force in Law Enforcement regarding the handling of intelligence/evidence? • Have the law enforcement / intelligence services systems for assessing what information is useful / essential for public health services? • Have the law enforcement / judicial systems for identifying means of providing information / intelligence to the public health service which is necessary to the protection of the public health (this sentence seems to make no sense)? Do common training between the two professional communities exist? • Were common definitions for the terms 'risk', 'threat', and other working terms agreed with the Public Health services? •
Extant Guidance Gursky E, Inglesby T, Toole T. Anthrax 2001: Observation on the medical and public health response. Biosecurity and bioterrorism, 1, 2003, 97-110.	

Training material developed by the Commission, ECDC, Europol and national experts for the 2nd EU Joint Training for Law Enforcement and Public Health

3. EUROPEAN MEDICAL INTELLIGENCE AND INFORMATION SYSTEMS

The issues

- Identifying the instruments and systems for collecting information available
- Using these systems to protect the public

Context

To provide the highest level of protection for the health of people in Europe it is desirable that there are programmes that are capable of developing medical intelligence on health threats. This medical intelligence should be derived from collecting, evaluating, analysing and interpreting all relevant and accessible sources of medical, scientific, environmental and risk information on CBRN issues and agents.

Such medical intelligence can effectively inform strategic and operational health protection preparedness and to raise public health and public awareness. Such intelligence has been most effective in protecting against threats in the fields of communicable diseases and biological threats (including animal diseases), chemical and environmental threats; useful information can also be derived about radiological and nuclear threats; and these information systems can also help to develop preparedness and response activities, effective use of medicines, vaccines, and laboratories and develop an ability to monitor relevant scientific developments in general.

Important intelligence on the potential deliberate misuse of chemical, biological or radiological (CBRN) materials can also be derived in part from open accessible sources, however, because of the illicit nature of these threats the involvement of the intelligence and law enforcement services is essential, both in providing information that is not publicly available and offering a different analytical perspective. Such threat assessments are, however, inevitably sensitive and are protected.

Furthermore, the EU Members States' health authorities are under Decision 2119/98/EC required to report threats to health to each other.

Organisation of Medical Intelligence in the EU

Intelligence on CBRN related activities may or may not be carried out in all Member States as a specific activity. Where it is carried out, there is evidence that there are a wide diversity of agencies and organisations involved in each of the different Member States. The different elements that contribute to intelligence on CBRN related activities could be improved by the identification of current systems and activities in each Member State. A system of

collaboration, coordination and communication to ensure that different agencies and organisations are allowed to work in isolation and but also allows the sharing of reports and assessments (with all due safeguards) could be developed. This process needs to embrace the public health, intelligence and law enforcement communities.

Member States identifying that multi-agency intelligence systems concerning CBRN related activities have not yet been developed may wish to examine how their existing structures can incorporate such activities.

The development of intelligence systems for CBRN related issues is not only of the public health community but the reciprocal provision of health information surveillance and interpretations enhances the understanding of the technical aspects of these issues for the intelligence and law enforcement communities.

The systems that are currently in place within Member States are enhanced by a number of observational systems available within the EU.

Current systems available to EU Member States for medical intelligence gathering

MedISys (http://medusa.jrc.it/medisys/homeedition/all/home.html)

MedISys (Medical Intelligence System) is a tool which has been developed for the Programme on Preparedness and Response to Biological and Chemical Agents (Health Security: 17 December 2001). MedISys is an internet monitoring and analysis system developed by the European Commission's Joint Research Centre to rapidly identify potential threats to the public health using information derived from internet sources. The threats currently sought include:

- human communicable disease outbreaks,
- CBRN (chemical, biological and radio-nuclear) threats,
- animal disease outbreaks,
- environmental and food supply threats,
- medicines and laboratory incidents.

The system monitors tens of thousands of reports per day using thousands of search terms in 35 languages; it generates mail alerts every 20 minute. It is accessible via the internet, email and news feeder systems; it runs 24 hours per day, 7 days a week.

The site offers a limited amount of data for direct public access, specialist public health organisations can request access to the restricted site, which offers more analytical functionality, more information categories and access to a greater number of news sources.

The system is used daily by the public health surveillance institutions of Member States (e.g. surveillance institutes), European Centre for Diseases Prevention and Control (ECDC)), the

World Health Organisation (WHO), the European Commission, Health Canada, and some European Armed Forces.

In addition, the system is also made available to Health Canada (as reciprocity for letting us accesses the parallel GPHIN surveillance system).

EMM (European Media Monitor, http://press.jrc.it/NewsBrief/clusteredition/en/latest.html)

EMM is a live media monitoring system that gathers reports from news portals world-worldwide in 42 languages, aggregates and classifies the articles, analyses the news texts by extracting information and produces intuitive visual presentations of the data found.

EMM has become a crucial instrument in the daily work of the Commission and other public organisations. EMM is the news gathering engine behind a number of applications. These include the three public web portals NewsBrief, News Explorer and MedISys.

TARIQA

Tariqa is a software equivalent to MedISys, run for DG RELEX in managing external crisis. The topics covered focus mainly on:

- humanitarian aid
- cooperation matters
- conflicts
- terrorists activities
- physical security abroad.
- security abroad, and cooperation matters.

The system is accessible to EU delegations, the DG-External Relations and to the various crisis centres active in the Commission. Outputs are also made available to military forces on EU peace-keeping activities and to international organisations active in the field of humanitarian aide such as UNOCHA and UNICEF etc.

Current systems available to EU Member States for communicating threats to health

There are two main alert systems in the area of human health.

EWRS

Since 1999 the Commission has put in place (Decision 2119/98/EC) the Early warning and Response System (EWRS), used in the context of communicable diseases threats. It is web-based and links Member States Health Ministries, National surveillance institutes and ECDC.

Standard Operating Procedures have been endorsed by all network's partners. The system is used to interchange information on risk management (measures of public health) applied by Member States as well as for notification of threats, exchange of information and coordination of measures among partners.

RAS-BICHAT

The Rapid Alert System on Biological and Chemical Agents Threats is used for reporting health threats/events which are falling under the mandate given by the programme on preparedness and response to biological and chemical agent [Health security & Health Security Committee] and is used to report on health threats (CBRN) in relation to real or suspected terrorist activities. It is also web based and fulfils the purpose of rapid notification of threats, exchange of information and coordination of measures among partners. It links the designated competent authorities and 24H operational contact points of each Member States.

Animal health information systems

With more than 60% of human pathogens which are of zoonotic origin, and 80% of pathogenic agents having a potential bioterrorist use are zoonotic, it is important to pay particular attention to animal health issues and clearly consider them as part of public health issues. An Animal Disease Notification System (ADNS) is in place in the EU and provides information on each outbreak in a Member State of an infectious disease in animals, listed in Annex I of Council Directive 82/894/EC. This information is sent by the Member States to the European Commission. (http://ec.europa.eu/food/animal/diseases/adns/adns_en.htm).

The reference international Organisation on Animal Health is the World Organisation for Animal Health (OIE) to which Member countries (172 to date) report cases of notifiable diseases detected in their territories, including zoonoses, through the World Animal Health Information System (WAHIS), within 24H for exceptional epidemiological events, and every six months otherwise. Information provided is automatically disseminated to all OIE Members and accessible through the World Animal Health Information Database (WAHID: http://www.oie.int/wahis/public.php?page=home).

Similar approaches have been worked out for, plant health, and radiological issues.

Alerting and reporting of threats in the EU

Informing each other in the EU on CBRN threats or risks is a duty for Public Health under the above agreements and obligation. This obligation not only applies to EU Member States within the EU, but also on towards Member States outside the EU, through the new International Health Regulations (IHR), covering naturally or deliberately occurring diseases or CBRN threats. At national level, the need to share certain health information with law enforcement colleagues needs to be considered, as is the need to identify further threat information to identify potential criminal intention and release. If there is a clear health risk, the sharing of Public Health information has to take precedence.

The Commission services and/or various Agencies (e.g. ECDC, EFSA, ECHA, EMEA) manage early warning systems in different areas, which have direct (e.g. communicable diseases, radiation, chemicals) or indirect relation to CBRN (e.g. contaminated products: such

as pharmaceuticals, medical devices, food/feed, animal, plants, etc.), allowing Member States to be informed, exchange information or coordinate measures. ECDC facilitates the exchange of information and the cooperation between the competent authorities of the Member States in early warning and response to serious public health events.

Since several alerting systems may become involved, the international dimension need also be considered in a more detailed manner (such as NATO, WHO, OIE, IAEA, GHSI) by identifying at national level the actors involved when linking to EU and international organisations actions in case of a CBRN event.

Examples of Good Practice, identified in some Member States

A number of Member States have reported that they are running their own national medical intelligence activities from open sources and Public Health institutes and create national reports on a weekly or ad hoc basis.

For Public Health, there is a requirement on EU-wide (and through the WHO on international) reporting. This does not only apply to the need to report under different circumstances, but also to the need to follow-up, to report the initiated measures and the closing of an alert. The benefits are mutual: the alerting MS can provide significant information to protect citizens in other MS.

An essential example of good practice is the response to an alert. Receiving MS can provide feedback to an alert Even if rumours are aired through the media, sending the relevant and authenticated information by a proper government source into the selected alerting systems, provides a proper way to confirm or infirm a threat or risk. The sooner the information is provided to the other MS, the better. More measures can be taken, more consultation can occur, media responses can be developed, and in case of mass alerting need, the communication plans can be developed.

Because of the sensitivities of some of the information/intelligence handled particularly by the public health communities, it can be helpful to develop relationships with individuals from law enforcement agencies and authorities. Law enforcement and security authorities (and their respective agencies) would have the appropriate security information and would be able to develop relationships with key people in the other organisations. They would interpret the threat assessments in terms of the implications for the public health community. This mechanism builds trust between the organisations which is key to developing the collaboration.

Good Practice Checklist

Public Health	Law Enforcement
• Have Public Health services ensured that they have access to the available public and restricted EU information resources? • Do Public Health services have the ability to analyse the information gained from these sources in terms of their own national needs and vulnerabilities? • Are national dissemination and alerting systems in place in order to ensure that derived intelligence can be acted upon? • Do Public Health and Law Enforcement authorities have a formal cooperation mechanism where the different analytical skills of the separate organisations can be pooled to maximise the amount of information that can be gathered and the quality of the analyses derived? • Are Public Health agencies ensuring that their liaison staff conform to agreed security measures for the safe handling of sensitive information and does this staff have appropriate formal security clearance to provide quality risk assessments to Law Enforcement services.	• Have Law Enforcement services familiarized themselves with the existing medical intelligence systems? • Are the Law Enforcement authorities working with Public Health authorities in creating a system for receiving alerts and new information? • Do Law Enforcement services work together with the Public Health services in order to combine information gained from Public Health sources with those collected by the security sector in a formal cooperation? • Are mechanisms in place to share and handle sensitive or intelligence information with Public Health agencies through a small number of trusted individuals?

Extant guidance

Guidance for the existing formats of Public Health threat reports:

- ECDC, which creates an internal daily report and a weekly Threat Report available to MS in a password protected system. ECDC is also running the Early Warning and Response System (EWRS)
- Messages/alerts circulating through the various warning systems (EWRS, RAS BICHAT, RAS-CHEM, ECURIE, MIC, RASFF)
- The Global Health Security Initiative (GHSAG/GHSI) public and restricted website.
- EUROSURVEILLANCE – the EU sponsored European rapid e-publication journal on emerging health threats
- The Global Public Health Intelligence Network (GPHIN) website and electronic messaging system; a secure, internet-based early warning system that gathers preliminary reports of

public health significance in seven languages on a real-time, 24/7 basis.

- WHO: Global Outbreak and Response Network reports
- PROMED: the international emerging communicable disease threats electronic alerting system run by the International Society for Infectious Diseases

4. PERSONNEL SECURITY & MANAGEMENT

The issues

- Responsibilities of employers to monitor and support staff in protecting access to hazardous materials
- Responsibilities of employees to comply with increased security measures to protect hazardous materials and information assets
- Vetting of staff
- Control of visitors to sensitive sites

Context

Currently the protection of CBRN materials has become more important than ever before. If terrorist groups wish to procure material to undertake an attack, they may need to have access to a person working inside an organisation that uses such hazardous materials or has knowledge of how to access, process and misuse such materials. Therefore, personnel security measures at establishments that hold CBRN materials are of paramount importance. Personnel security measures must be implemented taking into account all vulnerable areas, not just storage facilities, such as site physical security and materials transportation.

There is, therefore, a need to develop local and national advice for vulnerable sites and determine what personnel security measures are appropriate. This should include what to look out for and the support of any national databases and vetting systems, if deemed appropriate.

Particular care should be taken for CBRN materials commonly kept in hospitals, universities and food/water testing companies, where public access is common and may be difficult to control.

Persons working with material that could be weaponised need to accept that they may have to submit themselves to closer personnel checks and monitoring. This will also include the colleagues providing the monitoring and the establishment of a reporting process relating to unusual activity.

Personnel security issues should encompass all aspects of personnel at a site and include long term staff, new staff, students, contractors and visitors. Action should be focused at document checks, reference checks and knowing what warning signs to look out for; contact with and speaking to referees; verifying qualifications with the relevant examining board and being aware of systems of evasion and fraudulent presentation that are in current use; ensuring that annual appraisals are conducted on staff; and ensuring that staff can report suspicious activity to a superior without fear of recrimination.

Many public health sector workers may object to such close scrutiny, particularly as this represents a change in the ethos of their work and suggest a climate of distrust of their colleagues. This is an area where there is a particular responsibility for law enforcement to assist public health with guidance on what to look for and what action to take should concerns arise. It is also important that personnel measures are implemented with consultation so that each party knows what to expect.

There is already a wide body of occupational safety directives referring to protection of employees and the minimum health and safety requirements[3].

Examples of Good Practice, identified in some Member States

Good practices will be dependant upon national laws and other requirements, any measures implemented within Europe must comply with the European Convention on Human Rights and Fundamental Freedoms and associated and related legislation.

An assessment of the current threat to specific industry areas could take into account the following good practices, which were identified in some Member States:

- Treating current and new staff separately as the employer would have to conduct most investigations regarding current staff, whereas new staff can be asked to provide evidence of their previous record and trustworthiness.

- Ensuring the availability of an expert team within law enforcement which is available to advise sites on personnel issues and take action in the event of a suspicious person being exposed.

- Establishing appropriate measures to deal with contractors and visitors – The practice can vary depending on the areas to which contractors and visitors have access to and whether they need to be escorted at all times. This includes that regular visitors are checked to the same level as current staff.

- Ensuring non-intrusive continuous monitoring of staff –making sure that managers are aware when their staff are under pressure for whatever reason, and the likelihood of them becoming 'at risk' from external pressure. This is usually achieved by annual appraisals and an effective reporting system, whereby staff can report incidents/concerns in

[3] 98/24/EC of 7 April 1998 on the protection of the health and safety of workers from the risks related to chemical agents at work (OJ L 131, 5.5.1998, p. 11);
2000/54/EC of the European Parliament and of the Council of 18 September 2000 on the protection of workers from risks related to exposure to biological agents at work (seventh individual directive within the meaning of Article 16(1) of Directive 89/391/EEC) (OJ L 262, 17.10.2000, p. 21);
2004/37/EC of the European Parliament and of the Council of 29 April 2004 on the protection of workers from the risks related to exposure to carcinogens or mutagens at work (Sixth individual Directive within the meaning of Article 16(1) of Council Directive 89/391/EEC) (OJ L 158, 30.4.2004, p. 50);
2004/40/EC of the European Parliament and of the Council of 29 April 2004 on the minimum health and safety requirements regarding the exposure of workers to the risks arising from physical agents (electromagnetic fields) (18th individual Directive within the meaning of Article 16(1) of Directive 89/391/EEC) (OJ L 159, 30.4.2004, p. 1).

confidence to a manager who is empowered to take positive action.

- Offering appropriate counselling to persons who develop identify potential security questions in order to resolve such issues. This would be a service that an employee could use without their employer becoming aware.

- Ensuring law enforcement authorities inform public health authorities on forgery methods and current trends in forgery methods.

- Ensuring that both law enforcement and public health research current vulnerabilities that may be provided by the internet, for example via personal profiles on internet sites such as Facebook and MySpace, and the ease by which seemingly valueless information can be obtained by outsiders.

- Ensuring that law enforcement and public health authorities jointly remind scientists and clinicians that as threats change so do their own professional responsibilities, so that publication of research work is responsible and considers the potential security implications of some data being made available to everyone.

Checklist Suggested Core Requirements

Public Health	***Law Enforcement***
• Have you set up collaboration with Law Enforcement Services to review the security protocols concerning CBRN materials? • Have you reviewed the possible misapplication of research and Public Health work, especially: the transferable knowledge of hazardous materials and their development, and the security of hazardous materials (in particular biological agents)? • Have you developed a culture of safety and security in line with the changing need for vetting and verification of all individuals within sensitive organisations or facilities? • Are you ready to accept advice, guidance and supervision from appropriate national security organisations, and work with law enforcement partners in a constructive way?	• Have you identified and made contact with organisations in the health sector that may, not knowingly, host materials and knowledge that represent CBRN security issues? Have you developed and built relationships with these organisations? • Have you developed security briefings and specimen systems for such organisations to use? • Have you developed systems for the accreditation of security systems for these organisations? • Have you developed expertise in validation of personnel credentials, without relying solely on computer checks (which can give a false sense of security)? • Have you established a system to share information regarding the identification of suspicious applications/ persons?

Extant Guidance

There are many examples of best practice included within International bodies such as WHO and IAEA.

5. FACILITY SECURITY & MANAGEMENT (BIOLOGICAL)

The issues

- understanding of the different perspectives held by public health and law enforcement authorities concerning the public risk that may arise by the misuse of biological materials commonly stored and used in public, educational and industrial facilities
- the establishment of a common understanding on reasonable levels of security that can be enhanced in response to changing threat levels
- the development of joint work programmes on the development of security for biological agents in particular

Context

Most biological threats are living organisms that can normally be found in the environment, or in plant or animal reservoirs. This could include humans or animals that are infected with such substances. There is a duty to ensure the safety and security of such substances; this must however be balanced against the ease that such substances can be extracted from the environment.

Standards of physical security for biological materials vary across the European Union dependant upon the perceived threat. The security and management of biological materials requires measures based upon where they are kept, the systems needed to keep them viable, and the nature of the pathogen, as different pathogens pose significantly different risks.

Joint Public Health and Law Enforcement Issues

An overall understanding must be agreed between both parties of what is required and what will be considered by both parties as reasonable. There is a need for change in culture whereby both professions would deal with issues new to each other. Each party will need to be clear about what is required, how this may be achieved and the justification behind such measures. In particular, public health must understand their duty to prevent biological materials from being used to create weapons, and law enforcement authorities must understand the new environment in which they operate, for example, understanding the different threats that may be contained in research laboratories and diagnostic laboratories.

Public health and law enforcement agencies could explore ways in which they can share relevant information, experience and practices on these subjects.

Examples of Good Practice, identified in some Member States

- National bio security frameworks have been established led by law enforcement authorities but involving also public health services. These frameworks were developed by first engaging laboratory workers and local scientists, then moving to regional groups and national establishments.
- Law enforcement services ensure that the developed security advice provides reasonable levels of control consonant with the ability of the scientific and technical community to continue to undertake their work with the least amount of disruption.
- Public health and law enforcement services have agreed on a priority list of dangerous pathogens and toxins to ensure that appropriate substances and materials are regulated
- Based on a risk-matrix, a common security guidance or good practice documents have been developed and published with agreed public health / law enforcement objectives and content. Law enforcement authorities provide increased security measures to these facilities at a time of increased threats.

Good practice checklist

Public Health	**Law Enforcement**
• Have the public health services developed a comprehensive understanding of public risk when looking at physical security of biological agents?	• Have the law enforcement authorities developed a clear understanding of the threat posed by biological materials to ensure that appropriate security measures are put in place to protect relevant assets?
• Have the public health services developed a comprehensive understanding of the risk of becoming a target of attack: either as a victim or as a source of weapon materials? Has this resulted in increased security measures for staff?	• Does law enforcement work with Public Health to assess sites that contain biological materials? Does law enforcement provide advice commensurate to identified risks?
• Has the public health hierarchy requested facility risk assessments; has cooperation with law enforcement been sought and obtained in this regard?	• Have law enforcement authorities identified key experts to interact with relevant health professionals? Have these experts received appropriate training jointly with Public Health experts?
• Have the public health authorities designated liaison persons to work with law enforcement? Has an effort been made to ensure that policies are provided in accessible language?	• Does law enforcement involve Public Health when developing priority lists of biological threats?
• Have the public health authorities worked with Law Enforcement to develop a common policy for bio-security? Have specific arrangements been made to review these on a regular basis and at times of	• Have the law enforcement authorities worked with Public Health to develop a common policy for bio security? Have specific arrangements been made to review these on a regular basis and at times of

increased threats? • Have the public health authorities identified legislation gaps?	increased threats? • Have the law enforcement authorities identified legislation gaps?

Extant Guidance

Examples of information available on best security practice from the UK include:

- Physical Security: the building structure and associated features such as walls, ceilings, windows and doors. Equipment used should comply with a testing centres standard such as (in the UK) the Loss Prevention Certification Board (see www.redbooklive.com).
- Electronic Security: the protection of information databases and associated material. This could include all information stored in the various different formats (see www.cpni.gov.uk).
- Management Structures: ideally the owner of vulnerable substances should allocate responsibility to one person, who ensures the security and integrity of the substance (see www.sandia.gov).
- Procedures: sites that contain dangerous material must have good procedures to ensure the safety and security of the substances is maintained. Policy and procedures remain whereas individual people will move on in time. There are many good sources of reference for this including Sandia, IAEA and WHO.

6. TRANSPORTATION SECURITY, MATERIAL CONTROL AND ACCOUNTABILITY DURING TRANSPORT (BIOLOGICALS)

The issues

- Preparing samples to be transported for further analysis
- The requirements to keep materials safe in transit
- The varying international regulations promulgated separately for biological materials in transit
- Training of staff involved in the transit of hazardous materials, in particular biologicals
- Tracking and safeguarding materials in transit
- Ensuring the legitimacy of consignees
- Ascertain the adequate reception of forwarded samples

Context

Dangerous goods (classified in 9 classes) as hazardous chemicals (explosive, gas, flammable), toxic and infectious materials (micro-organisms) and radioactive materials need to be transported, nationally and internationally, for a variety of legitimate reasons. Special legislation, regulations or guidance exist in the EU and in each MS individually governing such transport activities.

In Europe, the transportation security, material control and accountability during inland transport of dangerous goods is governed through several EU and intergovernmental agreements:

- ADR - European Agreement concerning the International Carriage of Dangerous Goods by Road, concluded at Geneva on 30 September 1957, and amended every two years.
- RID - Regulations concerning the International Carriage of Dangerous Goods by Rail, appearing as Appendix C to the Convention concerning International Carriage by Rail (COTIF) concluded at Vilnius on 3 June 1999, and amended every two years.
- ADN - European Agreement concerning the International Carriage of Dangerous Goods by Inland Waterways, concluded at Geneva on 26 May 2000, and amended every two years.

These rules apply to international transport of their contracting parties. In the European Union, the rules have been made compulsory for all transport of dangerous goods by Directive 2008/68/EC on the inland transport of dangerous goods. Although the directive dates only from 2008, it replaces earlier directives on the road and rail modes, adopted in mid-90s.

The rules cover a wide range of issues, in particular classification of dangerous goods; packaging and their testing; training of personnel; role of safety advisers; documentation, labelling, placarding; procedures on consignment, carriage, loading and unloading; and construction and approval of vehicles. After the terrorist attacks in early 2000, a chapter has been added on the security of transport of dangerous goods.

The rules relating to the security of transport of dangerous goods focus on the issues that the transport sector should ensure itself. It does not look at issues that belong under the responsibility of the law enforcement sector.

The general provisions on security request notably that the identification of carriers is done properly, that areas where goods are stored are secure, and that a register of certificates for drivers are kept.

The rules also state that security awareness training has to be organised.

There are special provisions for so-called "high consequence dangerous goods" which have especially high risk potential when used in terrorist incidents. The rules specify these goods and require a special security plan. The minimum elements and criteria of the security are listed separately.

The movement of biologicals should be carried out according to legislation and regulations designed to ensure compliance with the Chemical Weapons Convention.

For transport purposes, micro-organisms (Class 6.2), are classified into the two categories A and B. Organisms assigned to Category A could be employed to effect by terrorists and are, therefore, required to be transported securely. Those in category B would, generally, pose little risk if misappropriated, for example, diagnostic specimens would be included in this category.

To address this security plan, all EU member states need to be aware of the international transport regulations and to produce national guidance on this issue to relevant professionals, particularly in the health sector. To facilitate secure exchanges of micro-organisms and other hazardous materials between EU member states it would be useful to have controlled access to contact details in each country of courier companies able to accept transport of dangerous goods. Each EU member state should also advise carriers of dangerous goods to relay their travel plans to the police in advance and/or to identify where they might find a safe haven en route should the need arise. For transport by air, IATA regulations stipulate clear packaging requirement.

Issues for Member States to consider

The new security measures include provision for consignors to:

- only offer dangerous goods to carriers that have been appropriately identified, and

- ensure that all transit sites for dangerous goods are secure;
- provide security training for all staff involved in the transport of dangerous goods and to raise their general security awareness.
- a requirement on carriers, consignors and consignees to co-operate with each other and with appropriate authorities to exchange threat information, apply appropriate security measures and respond to security incidents.

For 'high consequence' dangerous goods, there are extra requirements, such as the need to have a security plan be put in place. The security plan is to comprise at least the following elements:

- specific allocation of responsibilities for security to competent and qualified persons with appropriate authority to carry out their responsibilities
- records of dangerous goods or types of dangerous goods transported
- review of current operations and assessment of vulnerabilities, including inter-modal transfer, temporary transit storage, handling and distribution as appropriate
- clear statements of measures, including training, policies (including response to higher threat conditions, new employee / employment verification etc.), operating practices (e.g. choice / use of routes where known, access to dangerous goods in temporary storage, proximity to vulnerable infrastructure etc.), equipment and resources that are to be used to reduce security risks
- effective and up to date procedures for reporting and dealing with security threats, breaches of security or security incidents
- procedures for the evaluation and testing of security plans and procedures for periodic review and update of the plans
- measures to ensure the security of transport information contained in the plan
- measures to ensure that the distribution of the transport information is limited as far as possible. (such measures are not to cut across the regulatory requirements for the provision of dangerous goods transport documentation from consignors to carriers)

Suppliers of hazardous materials should be able to verify that the end user is a legitimate business; a mechanism for this needs to be identified with some urgency.

Referring to the hazardous agents requiring controls and regulation, it would be useful for EU member states to agree a implement the list of hazardous agents already agreed at international level (UN/ECE) in order requiring controls and regulation so as to ensure uniformity across the Union. For infectious diseases, the Health Security Committee identified a list of pathogens which are considered a high threat or very high threat for the EU. From both a safety and security viewpoint, laboratory waste must be disposed of in an appropriate manner.

Examples of Good Practice, identified in some Member States

- Security services of some EU Member States can establish where hazardous materials should be safely held and provide appropriate advice on site security, and movement security (including recruitment of appropriate staff and obtaining appropriately accredited contractor services).
- Governments of Member States can provide guidance to health professionals on best practice for shipping micro-organisms.
- Governments of Member States can make lists available of suitable couriers able to transport dangerous goods; an EC commissioned website where individual states could enter data and maintain information on suitability and reliability, would be useful to this intent.
- In some Member States, security specialists are involved in advising the courier services for proper storing and transportation of hazardous materials.
- Europol and Member States authorities can liaise and pool data on end-users so that providers of hazardous materials have a national contact to verify that the end user is a legitimate business. An identified mechanism is useful to verify that the end user is legitimated to receive hazardous materials along an authorization regime for hazardous agents.
- The European Commission could address the issue of agreeing a list of hazardous agents requiring controls and regulation to give uniformity across the EU.
- Governments of Member States can provide regulations governing laboratory waste disposal.
- Instituting a system of test moves to check initial systems and to ensure continued effectiveness at regular intervals thereafter.

Good Practice Checklist

Public Health	**Law Enforcement** */ Competent Authorities*
• Have the health/diagnostic laboratories considered the possibility to identify in advance the courier company they would use for a Category A infectious substance? Is this information available at short notice? • Has a tracking system been considered for all Category A infectious substances under	• Are Law enforcement services/Competent authorities working with Public Health services on identifying establishments that hold hazardous materials in each EU MS and on ensuring that hazardous materials are held securely according to acceptable standards? • Are Law Enforcement authorities /

transport? Is the sending laboratory able to inform the recipient laboratory that samples are being dispatched? Is the receiving laboratory able to inform consignees of the receipt of a Category A infectious substances within 24 hours of them being received? • Do institutes sending and receiving hazardous materials engage the services of a Dangerous Goods Safety Advisor? • Is training and information available to Public Health laboratories on how to handle discarded culture materials and on the need to dispose both safely and securely by autoclaving and/or incineration? • Do Public Health services have available the algorithm for obtaining the special licenses/approval from national authorities/agencies in both the country of dispatch and receipt for the international transportation of hazardous materials?	Competent authorities ensuring proper enforcement that carriers of dangerous goods have ADR (European Agreement on the transport of Dangerous Goods by Road) trained drivers? Is this requirement enforced? Has an analysis of the presence of appropriate legislation been identified? • What is the mechanisms when hazardous material transport requires "prior notice of shipment", in order to ensure that in certain cases, where the material is of higher risk, for arrangements for police patrol vehicles to observe the vehicle on the road or to provide escorts? • Are Law Enforcement authorities/ Competent authorities working with academia or experts to identify the best routes for a particular hazardous material transport and "safe havens" should the unaccompanied driver feel under threat whilst on the road?

Extant Guidance

List of pathogens which are considered a high threat or very high threat for the EU: http://ec.europa.eu/health/ph_threats/Bioterrorisme/keydo_bio_01_en.pdf (Annex 7: "EU list of high threat pathogens")

Restricted chemicals: http://www.australiagroup.net/en/precursors.html

Microbiological organisms that could be considered for use as weapons: http://www.iata.org/NR/ContentConnector/CS2000/SiteInterface/sites/whatwedo/dangerousgoods/file/Section3.6.2Mar05.pdf

UK practice on transport of infectious substances can be found at address below, it contains links to both European and international regulations: http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_075439.

UK recommendations on laboratory security standards are documented in *"Security Standards for Laboratories"*, published by NaCTSO – the UK National Counter Terrorism Security Office. This is a restricted document but may be available through international liaison arrangements on request.

IAEA 'Regulations for the Safe Transport of Radioactive Materials' 2005 Edition; Safety Requirements No. TS-R-1 are available over the internet at:

http://www-pub.iaea.org/MTCD/publications/PDF/Pub1225_web.pdf

UNECE: UN Model Regulations on the transport of Dangerous Goods
http://www.unece.org/trans/danger/danger.htm

7. JOINT ASSESSMENT OF SUSPICIOUS INCIDENTS

The issues

- Recognition of incidents by public health authorities that should be referred to law enforcement and other competent authorities
- Recognition of incidents by law enforcement and other competent authorities that should be referred to public health authorities

Context

Most public health, law enforcement, and other competent authorities share a single overarching objective: the protection of the public. However, public health and law enforcement personnel can be unfamiliar with how to trigger support from their colleagues in other agencies.

Joint assessment of incidents can be needed in order to:

- identify developing threats to the public (by different types of agents)
- develop a common strategy for investigating and managing the issues identified
- identify the synergies available between the public health and law enforcement resources that are achievable.

Crucial to the management of joint operations will be decisions about leadership:

- clear divisions in the duties that each must undertake on behalf of each other
- managing existing separate reporting structures / developing new common reporting pathways
- synchronising the different elements of each others operations (common "battle rhythm")
- maintaining a common information picture of emerging events

Examples of Good Practice, identified in some Member States

- An agreed set of the fundamental triggers required for public health or law enforcement authorities can initiate joint investigation.
- A memorandum of understanding (MOU) between law enforcement, competent authorities, intelligence services and public health authorities can detail their respective roles and responsibilities to jointly investigate incidents that comprise a defined set of circumstances.
- There needs to be clarity concerning the ownership and the leadership of such joint

operations.

- Furthermore, a commonly agreed "battle rhythms" and common reporting systems are beneficial.
- Some Member States tried to enhance the degree of inter-operability that can be achieved in a joint investigation and improve possible synergies (for example, improved ability to provide public protection, time and resource saving, improvement in ability to gather and process forensic evidence)

Good Practice Checklist

Public Health	**Law Enforcement and competent authorities**
• Do Public Health services understand the role and responsibilities of law enforcement authorities in the investigation of CBRN incidents, their systems of practice, and operational/ investigational priorities? • How developed are the communication channels regarding information exchange with the Law Enforcement authorities? Is a MOU in place? • Were common definitions agreed upon? • Have criteria (or 'triggers') been developed for assessing the type of incident that needs to be communicated to Law Enforcement authorities? • Has the possibility of establishing a forum which enables the separation of clinically confidential data from the shared information pool been considered? • Does a MOU/special arrangement exist for joint investigations with law enforcement authorities? Were joint teams and algorithms of functioning prepared?	• Do Law Enforcement authorities understand the role of public health services and the principles of epidemiological investigation in the investigation of a CBRN incident? • Were communication channels developed regarding information exchange with the Public Health services? Has a MOU been developed? • Were common definitions agreed upon? • Have criteria been developed for the assessment of the type of incident that needs to be communicated to Public Health authorities for their advice on public risk and human disease investigation strategies? • Has the possibility of establishing a system to ensure that requests for information that may be protected by clinical confidentiality issues are managed in a way that protects clinical practitioners from potential ethical / professional misconduct issues? • Does a MOU/special arrangement exist for joint investigations with the Public Health authorities? Were joint teams and algorithms of functioning prepared?

8. PERSONAL PROTECTIVE EQUIPMENT (PPE) OF INVOLVED STAFF; PROTECTING INVESTIGATORS

The issues

- Assessment of hazard and provision of appropriate personal protective equipment (PPE)
- Restriction on communication
- Resilience and degradation of physiological performance
- Resilience and degradation of equipment
- Standardisation of PPE ensembles (interoperability) versus need for differing standards of PPE to enable differing working practices
- Disposal of PPE
- Verification of PPE protection and reassurance of personnel
- Availability of decontamination facilities for operational staff of competent authorities/Public Health and LE

Context

Any CBRN incident will see the involvement of public health, health care responders, search & rescue / recovery, and law-enforcement.

In general, both police, competent authorities and public health personnel will need to survey and take samples from the scene in order to correctly identify the agent in question and define appropriate health measures and to investigate the crime, if any.

Forensic procedures are quite strict and involve a series of actions that aim at protecting the crime scene from contamination or interference which may compromise the quality of the evidence recovered and its evidential value.

Taking into account the procedures described in other sections of this material, the issues raised hereunder relate to the personal protective equipment (PPE) needed for the investigators.

An important assumption made ahead of this discussion is that both the law enforcement and public health investigators are going to enter the warm and the hot zone of an incident after all rescue and decontamination processes of the victims are completed.

Without detailing suitable appropriate PPE ensembles some brief notes on needs for scene setting purposes are:

First responders: usually do not wear CBRN specific PPE or may not have immediate access to such equipment. Fire-men may have full protection means with external air supply. They may

have access to some hazard alerting equipment (such as active personal radiation direct readable personal radiation dosimeters), although such technology is virtually absent for biological threats. They are protected by guidance concerning assessment of scene safety and instructions not to enter unsafe places.

Search & rescue: usually will have access to CBRN specific PPE, including self-contained breathing units. The PPE will usually be designed to cope with all hazards and may be gas tight (note: no protection from radiation, but protection from radiological contamination). It will usually be designed to provide robust physical protection. The design of such ensembles will often be compromised giving limited fine motor control and be heavy and physiologically restrictive (especially in very hot climates). Capable communication systems between rescuers and their command and control systems are often built in as these are necessary for operator safety, but there will often be severe restrictions on communication between the wearer and members of the public / others not having access to the dedicated communication channels used.

Immediately necessary health care: there are significant restrictions on the type of medical interventions that can be provided in multi-purpose PPE ensembles. Clinical care may be restricted to some protection of a patient's airway and the administration of drugs injected via specialised systems that can be handled whilst wearing PPE, such as nerve-agent antidote injections (combi-pens). The PPE ensembles for health care staff also need to take into account the potential requirement to be utilised in wet decontamination systems. These ensembles may, therefore, differ in type from those used by search & rescue staff.

Forensic scene management & evidence recovery: this may include both law enforcement and public health staff. Following initial assessment of an incident scenes and a more slowly considered risk assessment based upon clinical evidence from recovered victims, observation of the incident site and peripheral environmental sampling it is usually possible to reduce the PPE requirements need for scene entry to those needed only for the now most probable hazards likely to be encountered. These need to be combined with clothing that will ensure that the investigators do not contaminate the crime scene and maintain its forensic integrity as far as possible.

Examples of Good Practice, identified in some Member States

- A collaboration between law enforcement and public health personnel can be used to find agreement on:
    - the appropriate PPE to be used in crime-scene investigations,
    - the appropriate timing for public health investigations,
    - the appropriateness of public health undertaking forensic investigations on behalf of or under the supervision of law enforcement services.
- The use of existing European norms and directive standards for the procurement of PPE ensemble components to ensure inter-operability with agreed cross-agency safe working practices (certificated PPE, e.g. CE marked respirator standards, not 'N' designation filters).
    - Employment of site safety management (site safety plan and responsible officer)

- Training of decontamination procedures, appropriate removal of contaminated PPE, first aid issues

- Dynamic re-evaluation of PPE type needs at different stages of rescue, recovery and investigation may reduce the physiological burden on rescuers and investigators.

- Importance of designing complete PPE ensembles:
  - head and shoe covers
  - overalls / water-proof outers
  - need for gas-tight suiting
  - gloves (type / single / double)
  - respirators (type / range of filters / powered / entirely self-contained)
  - integral communication systems

- Pre-arranged systems for proper disposal of single use or decontamination of reusable equipment.

- Testing and verifying of appropriate PPE use in order to reassure field teams about the effectiveness of their protection systems and to ensure that the expected physiological limits are reasonable and workable.

- Regular exercises to test the processes and training sessions with involved personnel to familiarize themselves with the equipment. Maintenance of an appropriate level of fitness needs to be assured and maintained.

- Specific identifiers, records and external supervision for all persons entering hazardous working areas ensuring that the PPE is appropriate, communications can be maintained, physiological limits are not exceeded, and the design limits for the ensemble are not exceeded.

- Some Member States have established dispersal assessment capabilities to deal with joint risk and threat assessment of suspicious incidents, which is important to help identify how a CBRN substance is spread in the environment, for example in connection with an intentional release. Dispersal modelling is of crucial importance in an operational situation, for example in relation to sampling teams, medical countermeasures and evacuation plans etc.

Good Practice Checklist

Public Health	**Law Enforcement** ***and competent authorities***
• Have public health personnel a plan for the sampling and tracing procedures to be used at the scene? Are they included the forensic procedures and take into account the chain-	• Are the Police forces personnel in specialised crime scene investigation teams aware of the issues regarding the protection of Public Health and the necessary

of-evidence procedure? • Public health personnel need specific training in forensic evidential procedures including chain-of-evidence controls for sampling, documentation and material transfers. • Have public health personnel been trained in the selection and use of PPE that is compatible with crime-scene investigation needs, as well as a scene involving a possible CBRN agent? Are common field training taking place for Public Health and Law Enforcement personnel? • Is the public health sector taking the lead in creating protocols for clinical and epidemiological follow up of all personnel who have worked at the scene of suspicious incidents including; short-term needs for post-exposure prophylactic clinical interventions; short-medium term proof of protection by the PPE /safe working methods adopted at the incident scene; long term epidemiological evidence of harm created by accidental or inevitable exposure to novel agents by victims and response staff?	sampling to be forwarded to a pre-arranged reference laboratory? Is appropriate PPE for CBRN threats available for use by these teams under specific procedures and subject to their specialized training? • Have crime-scene personnel been trained in processing a crime scene involving a CBRN agent, which may necessitate novel monitoring and material recovery techniques as well as the possible need for handling of unusual hazards by public health staff working under the direction of law enforcement crime scene investigators (especially biological and radiological hazards)? Are common field training taking place for Public Health and Law Enforcement personnel? • Have the Law Enforcement services established a site safety management at the incident for overall safety issues and especially assigned to the Law Enforcement-entry team, including responsible site safety officer and site safety plan (e.g. risk assessment during presence at crime scene)?
Extant guidance Exchange of information and good practices during various workshops under the Health Security Committee (SANCO) since 2001; dispersal modelling: http://ec.europa.eu/health/ph_projects/2003/action2/docs/2003_2_03_report.pdf, http://www.bioberedskab.dk/model/index.htm EU norms and directives for PPE equipment	

9. DEFINITION AND ENFORCEMENT OF AREA-SECURITY AND HOT/SAFETY-ZONES FOR THE PURPOSES OF AN INVESTIGATION

The issues

- Definition of safety zones
- Legislation to support incident site working
- Providing safe systems of working for investigators
- Ensuring enforcement of cordons and site/public safety
- Management and authority to invoke safety and control measures

Context

Any CBRN incident response will involve large numbers of search & rescue, public health, health care provider and law-enforcement staff.

In general, the police is expected at the beginning to move everybody to a place of safety and keep people away from the scene and at a second phase to investigate the crime. Competent authorities or public health services provide advice on the nature of the material that has been released or misused and the health care provider services will provide care and treatment to those injured, provide resources, equipment and medical staff, alert hospitals, and evacuate the injured.

A physical cordon should be established around the suspected perimeter of the contaminated area (also called a hot zone) to restrict entry and exit. However, because most types of CBRN release result in multiple contaminated areas it may not be possible to establish a precise boundary between uncontaminated and contaminated areas.

There is no set size for a hot zone, each will be dependent on the nature of the incident and the type of material released. A covert operation may require that the hot zone is kept very small so as not to alert the public and a hot zone that potentially contains an explosive device will need to be very large because of this added threat. For example, a 400m zone is applied to most incidents involving explosive devices in the UK. A hot zone for an incident involving radiation will be based on the size of the radioactive source, its activity, dispersion and the availability of suitable shielding material; but may be as small as 30m in radius if the materials are encapsulated and not dispersed.

Due to the very nature of a CBRN attack, the size and shape of the hot zone is likely to change rapidly as factors such as weather change (for example rain), wind speed and wind direction changes and quantity and formulation of the contaminant.

The natural reaction of the public caught up in such an incident will be to get as far away

from the scene as possible. This could, of course, only extend the problem by spreading contamination and the removal and destruction of evidence. Every new hot zone will require a full set of zones (hot, warm, cold) and cordons together with personnel required to enforce and protect the zones. Multiple hot zones will tie up large numbers of staff and will drastically limit the number of personnel available to the incident commander.

The need, or not, to wear protective clothing is an important issue, on the one hand in order to ensure personnel safety and on the other to balance the use of difficult and expensive PPE suits. Many PPE ensembles will cause significant degradation of the ability of staff to work effectively and there may be a limit on the number of sets of protective clothing that will be available. A hot zone may need to be maintained for a prolonged period of time (days or weeks) until the law enforcement and public health investigations have been completed and the area is appropriately decontaminated.

In preventing the spread of contamination outside of cordoned areas, authorities will need to consider imposing measures which could be extremely significant changes from normal policing practices.

Failure to contain contaminated casualties may result in the persons concerned self-presenting themselves at nearby health facilities leading to the loss of this vital asset and the creation of further hot zones. Human nature is to evacuate casualties and coupled with living in a highly mobile society it may take a long time (especially in the case of a biological incident) to identify an outbreak as a deliberate CBRN attack.

The overarching feature which will dictate how to respond to an incident will be the level of contamination, mobility and the persistence of a CBRN substance (its ability to remain hazardous in the environment over time). The choice of management strategy will be strongly influenced by the persistence of the substance. Substances with low persistence such as cyanide disappear within minutes/hours. A persistent chemical substance might last several months or even years under the optimum conditions. A persistent radiological substance may take many decades to completely breakdown and the rate of decay may not be substantially affected by external factors such as the weather. These factors will have a significant impact on the ability of authorities to maintain zones/cordons over a prolonged period of time.

Responders must understand the limitations of the detection, identification and monitoring (DIM) equipment available to them. Chemical and radiological detection equipment has reached a good level of reliability and accuracy; however chemical detection equipment may not be sufficiently sensitive to levels of contamination that may still be harmful to human health; there are currently no reliable and quick ways of detecting biological agents, and such rapid detection systems that are available may be severely compromised by being agent specific and relatively insensitive. Defining the hot zone will be achieved by a combination of those operating the detection equipment, observation of casualties by health officials, scientific advice and law-enforcement's requirements to resource the management of the scene.

Control of contaminated areas

The law regarding entry to and control of public and private premises is often different in each Member State. The law in most MS does allow for entry with consent, with a search

warrant or other legal instrument. However, courts have recognised very specific situations when urgent circumstances are present as exceptions.

Obtaining consent from a judicial authority is often the easiest means to secure evidence that will be legally valid. It is recommended that legal advice should be sought in all cases where consent for access is not given. In the case of a CBRN incident urgent entry into premises may be necessary to protect life, which may, however, harm the recovery of evidence.

Therefore, law enforcement, public health, and public safety personnel should identify when, how and if, they are legally allowed to enter homes and workplaces without a warrant, or other explicit legal authority, in circumstances which suggest a serious, credible, and immediate threat to the public. In any case they should consider ways how to quickly obtain a warrant or a permission from a relevant authority (e.g., a court or other judicial authority). Joint co-operation and reliance on each others (public health and law enforcement) means may be necessary

When the forensic investigations into an incident have been concluded competent authorities and public health officials should advise as to whether there is a need for decontamination of the site, what standards of cleaning are required, approve of the methods proposed to clean the site and advise as to when a building can be re-occupied.

In general terms, when considering closure of premises, it is important to bear in mind that the decision to reopen premises may be more difficult than to close them down, particularly if a place was shown to be contaminated by chemical, biological or radiological materials. The legal consequences of decisions made by public authorities in this field are significant in the way that they set future expectations and take responsibility for the safety and effectiveness of the methods and standards that they propose.

Definitions

Cordons and zones are established around the scene for the following reasons:

- to guard the scene;
- to protect the public;
- to control sightseers;
- to prevent unauthorised interference with the investigation; and
- to facilitate the operations of the emergency services and other agencies.

A number of cordons/zones should be established. This will be done by the police in consultation with other agencies such as health and scientific advisors. Commonly used terms to identify these cordons and zones include:

Hot Zone: this is the scene of the incident and likely to be the most heavily

contaminated. The hot zone (and subsequent hot zones) will be defined by the area contaminated usually through the use of detection, identification and monitoring (DIM) equipment.

Warm Zone: area in which decontamination of casualties/personnel from the hot zone is carried out.

Cold Zone: the area outside of the warm zone where there is no contamination but is required for emergency services use.

Inner cordon: provides immediate security of the hazardous area and potential crime scene. All personnel at and within this cordon must have personal protective equipment.

Outer cordon: seals off an extensive area around the inner cordon;

Traffic cordon: set up at or beyond the outer cordon to prevent unauthorised vehicle access to the area surrounding the scene.

The law in the different Member States that enable law enforcement agencies to enforce such cordons varies. For example, in terrorist or suspected terrorist incidents in the UK, it is a criminal offence to contravene a prohibition or restriction imposed under the Terrorism Act 2000. This includes the crossing of a police cordon.

The agencies controlling the cordons may vary, according to the purpose of the cordon. For example:

Inner cordon: Police will control all access and exit to the inner cordon through a cordon control point; however working within the inner cordon may be controlled by another agency who has oversight of the health and safety requirements needed.

Outer cordon: Police will control all access and exit points to the outer cordon. Non-emergency service personnel requiring access through the outer cordon should be vetted at this control point.

Examples of Good Practice, identified in some Member States

- A single agency in charge of the various zones to prevent power-struggles, confusion and duplication of work. For example, in the UK the police control the various zones as they have the powers to enforce the cordon. This arrangement has been accepted by the other UK emergency response services.
- A verifiable identification system for personnel entering and leaving a contaminated area to ensure that only necessary and authorised staff are involved with an incident. Such a system will also account for the number and location of personnel at the scene.
- Provide information to the public, e.g. in the form of handouts. Studies have shown that the public can become uncontrollable if they are detained and not kept informed.

- Sufficient numbers of suitably equipped and trained personnel to maintain cordons and carry out the effective decontamination of casualties.
- Have a place sufficiently robust legislation to enable the enforcement of cordons and ability to take potentially highly controversial decisions.
- Regular exercises to test the planning and to ensure that all agencies work closely together and understand each other's roles.
- Talk with the neighbours
- For the identification of authorised personnel, which is suitably protected and briefed to be in the inner cordon, inner cordon controllers can issue identifiers such as armbands as well as record all personnel already inside or entering the inner cordon.
- Trained clinicians at the scene to assess casualties (and therefore identify disease/nature of material) leading to directed decontamination and rapid treatment.
- Explore/develop or collaborate in order to have available modelling capabilities for the hot zone and any resultant plume to allow dynamic positioning of cordons due to change of conditions, e.g. wind direction, etc.
- Reliable system to communicate these changes/decisions together with any new hot zones to all interested parties.
- Occupational risk assessment for personnel working in the various zones. Consideration can also be given to the health and hygiene of the personnel as well as their need for future follow up.

Good Practice Checklist

Public Health	**Law Enforcement** ***and competent authorities***
• Have the Public Health services established a protocol for the definition of a hot zone (depending on the suspected agent of exposure) in collaboration with Law Enforcement services?	• Have Law Enforcement and other competent authorities developed protocols for the definition of a hot zone (depending on the suspected agent of exposure) in collaboration with the Public Health services?
• Does a system for registration of casualties for treatment and long term follow-up exist?	• Does a system for registration of casualties for forensic purposes exist (in collaboration with Public Health services)?
• Have protocols for decontamination of casualties (depending on the suspected agent of exposure) been developed?	• Have protocols for the provision of security of the incident area as well as the different zones (hot, warm, cold) been developed?
• Have protocols for the provision of	• Have protocols for the post mortem

clinical care to patients in the different zones been developed? • Have protocols for recovery of forensic evidence from clinical specimens been developed? • Have protocols for the management of contaminated fatalities been developed?	recovery of evidence and victim identification been developed? • Have protocols for information management and resource coordination been developed?
Extant guidance • World Health Organisation (WHO) Health aspects of biological, chemical and radio-nuclear threats manual; • NATO NBC Handbooks; • Member States emergency service guidance documents. For example: London Emergency Services Liaison Panel: Major Incident Procedure Manual (7th Edition)	

10. LABORATORY ISSUES: MAINTENANCE OF THE CHAIN OF EVIDENCE

The issues

- Identification and classification of hazards
- Principles guiding the collection of samples for forensic purposes (who collects what)
- Laboratory pathways

Context

Public health, competent authorities, and law enforcement personnel need to take samples for their own purposes.

The following scenarios may often occur:

- Both streams of work need to take samples from a crime scene
- Both streams of work need to take samples from the same evidence

In a CBRN incident sampling becomes especially difficult since the samples to be collected can be contaminated with hazardous substances (biological (i.e. infectious agent), chemical and/or radioactive material)

Chain of evidence

Law enforcement agencies need to obtain samples that are able to stand legal scrutiny if they, and their derived analyses, are intended to be introduced as evidence in court proceedings.

In order to be acceptable, the sample has to follow the so called chain-of-evidence. This requires that the entire itinerary of the sample, from the very moment it is collected to the eventual disposal of the sample, has to be clearly registered.

This register enables knowledge and eventually tracing of:

- who manipulated or was in contact with the sample;
- where and when the sample was stored;
- what analyses the sample underwent.

The chain-of-custody process also contains all the information about:

- how the sample was collected;

- the packaging, transportation and conservation methods used to transfer the specimen to, and maintain it inside, the laboratory;
- unmistakable and unambiguous identification of all and every single collected sample;
- the means by which the sample was manipulated, analysed and studied.

Every sample must be collected according to a technical instruction, which contains rules as to:

- how the sample is to be collected;
- directions for transport and conservation on its way to the laboratory.

It is a requirement for every sample to be accompanied by a document which contains the chain of custody. This has to be detailed in a log with all the mentioned information from the very moment it was collected to the moment it is presented to the judicial authorities.

CBRN specimens

All of the above requirements apply also to CBRN incident related specimens. However, special care may have to be taken to avoid personnel, the laboratory and/or the environment becoming contaminated by hazardous materials that may be contained in these samples.

It is extremely useful to have rigid and strict safety and security instructions on how to handle these samples.

Should the samples contain unknown mixes of chemical, biological or radiological materials then an incident-specific system of safe working may need to be devised. This should usually be done in the following order (steps can be missed out if there is conclusive evidence that, for example, a biological agent will not be present):

1. at-scene exclusion of explosive risk (flame testing)
2. at-scene exclusion of high level radioactivity (total gamma ray and gamma-spectroscopy assessment). If radiation is detected then the sample(s) should be passed to a radio-analytical facility at this point (sample can be passed and analysed in a sealed container if there is still concern regarding the additional presence of a microbiological pathogen)
3. removal to a category III (BSL-3 or P3) microbiology laboratory capable of excluding very high threat biological agents (usually using rapid isolation techniques such as polymerase chain reaction technology - PCR)
4. removal to a category III (BSL-3 or P3) diagnostic laboratory to identify any significant biological agents present, not in agreed very high threat biological agent lists
5. removal to a forensic explosive analytical facility for definitive testing for

presence of explosive/accelerant properties

6. removal to a forensic chemistry facility for identification of any chemical hazards.

This order is not definitive, but takes account of the fact that many forensic explosive and chemistry facilities - in general forensic institutes - will not have biological hazard containment facilities and therefore biological hazards need to be eliminated before these facilities can safely receive such specimens. Analytical effectiveness of some of these steps may be impaired if explosive risk limitation steps are taken with samples (such as mixing specimen materials with water-ethanol mixtures).

It can be seen from reading through this list that many samples may need to be collected, split and transferred/passed between several laboratories, therefore indicating the need to maintain a proper chain-of-custody procedure.

Examples of Good Practice, identified in some Member States

- Public health officials/investigators can have a list of contacts in their law enforcement agencies and/or judicial authorities who can give advice, training, and provide supervision when a chain-of-evidence issue arises.
- At the earliest possibility of a criminal act, public health and law enforcement sectors can try to work in coordination to devise appropriate forensic investigation strategies which offer safe systems of working and in order to make best use of the laboratory skills and services available.
- Chain of evidence manuals can take account of the needs of all foreseeable laboratory institutions that can undertake sample analysis, whether they are dedicated forensic facilities or not.
- In specialised laboratories (BSL 3 or BSL 4, chemical defence or radionuclide laboratories) forensic equipment are made available in order to allow joint investigation teams to perform the necessary investigations on the spot)

Good Practice Checklist

Public Health and competent authorities	**Law Enforcement**
• Are Public Health services working with Law Enforcement authorities and judiciary authorities in providing training for chain-of-evidence processes to Public Health and laboratory professionals? • Has the appropriate safe working system for collecting, handling and testing of samples from a CBRN incident per scenario (unknown mix, C, B, R) been identified in advance? • Have the appropriate laboratories that can handle contaminated specimens	• Are law Enforcement authorities working with judicial and Public Health services to train their personnel in the chain-of-evidence procedure? • Has the appropriate safe working system for collecting, handling and testing of samples from a CBRN incident per scenario (unknown mix, C, B, R) been identified in advance? • Have the appropriate laboratories been identified in advance that can handle contaminated specimens (radioactive, chemical or biological) and their

(radioactive, chemical or biological) and their limitations been identified in advance? Were possible capacity gaps analysed and were steps taken to cover them via international collaboration with other MS? • Has the appropriate paperwork needed (with the agreement of Law Enforcement) for the chain-of-custody for the samples from CBRN incidents been prepared?	limitations? Has cross-training taken place? Has the appropriate equipment been provided to the forensic laboratory personnel to build capacity (e.g. PCR testing)? • Are Law Enforcement authorities working with Public Health personnel in preparing the appropriate paperwork needed for the chain-of-custody for the samples from CBRN incidents? • Has the collaboration with Public Health to recover and use forensic evidence from clinical specimens and ensure chain of evidence been formalised?
Extant guidance All law enforcement agencies that conduct forensic investigations have technical instructions for collecting samples and for maintaining the chain of evidence. These are specific to each MS legal constituency and must be followed by both law enforcement and public health services when undertaking forensic analyses. Guidance for sampling in a CBRN incident developed by the Danish National Centre for Biological Defence http://ec.europa.eu/health/ph_threats/com/preparedness/docs/biological.pdf	

11. LABORATORY ISSUES: LABORATORY DESIGNATION, ACCREDITATION, QUALITY ASSURANCE AND FORENSIC REQUIREMENTS

The Issues

- Understanding the different role and processes utilised by diagnostic, exclusion and confirmatory laboratories
- Identifying appropriate specialist and reference laboratories
- Utilising laboratories not normally accredited to provide forensic services
- Understanding the difference in dealing with clinical versus environmental samples
- Understanding the different processes and levels of proof used in developing clinical suspicion of a disease, obtaining clinical confirmation and providing satisfactory proof of disease to evidential standards
- Preserving evidential samples
- Disposing of hazardous evidential waist

Context

The nature of materials used in CBRN attacks poses a potential problem to law enforcement and public health services, in that the materials used may be unusually hazardous to analyse and may be of a type such that forensic laboratory assays and methods are not available.

Therefore, during the investigation of an incident involving CBRN substances, law enforcement and public health investigators may need to consider the use of laboratories that normally do not provide forensic services.

Law enforcement and public health investigators need to have a clear understanding under which conditions samples can be handled safely and how to identify unusual and hazardous materials to an acceptable evidential standard.

They should, therefore, identify a network of laboratories whose purpose, range of investigations, forensic capability, safe handling techniques and investigational methodology is well documented. These laboratories might include:

- forensic science laboratories
- clinical science laboratories
- laboratories accredited to undertake specified individual investigations

- laboratories with specialist hazardous material handling techniques
- other scientific research laboratories, or institutions

When identifying laboratories within this network it is important to have an understanding of their laboratory quality control and quality assurance schemes; their ability to process materials under chain of evidence controls; and their ability to handle, manage, store and dispose of materials that may contain mixed hazards.

Designated Forensic Laboratories

Such laboratories usually only handle and analyse samples taken from a crime scene. In some Member States, the staff of these laboratories may also act as investigators of the crime scene and be responsible for the recovery and documentation of evidence alongside law enforcement agencies, in other Member States laboratory staff is not allowed to investigate at crime scenes: laboratory staff operate independently from law enforcement while scientific forensic experts at crime scenes support law enforcement staff (personal protective equipment (PPE), risk assessment) and all evidence is taken by the law enforcement officers.

Their output will be an evidential report which ought to be acceptable in a criminal court of the jurisdiction which jurisdiction they serve. These reports usually detail the method of specimen recovery, the procedure used in analysis, the accreditation of the laboratory to undertake the investigation, the qualifications and experience of the supervising scientist and the probability with which the result can be relied upon to support the interpretation that the supervising scientist has assigned to the test.

The samples analysed in a forensic laboratory will usually not be destroyed (although some types of investigation will degrade or destroy the part of the material that has been analysed). Where possible, the samples, or the major part of the sample, or a properly representative part of the sample, have to be preserved in order that independent studies can be undertaken on behalf of any defendant or through a court order for a second expertise.

Clinical Science Laboratories

Such laboratories are often found within larger clinical settings, often associated with hospitals. They usually perform high numbers of tests on a daily base often using highly automated assay systems[4]. In addition, the laboratories performing the tests are most likely certified and accredited by professional organisations or according to ISO standards.

The standard of analytical quality in these laboratories is guided by the clinical needs they serve; often highly specific in what they identify, but the accuracy of quantitative tests may be restricted to the needs of diagnostic speed and may not have the precision

[4] licensed according to Directive 98/79/EG (in vitro diagnostic directive: IVDD)

sought by a forensic investigation.

In respect to biological agents subject to national and European surveillance[5,6], confirmation of the biological agent, and reporting to national surveillance service, is required. The confirmation of such agents usually takes place at reference laboratories, often designated by national authorities as national reference laboratories. Such laboratory services may be provided by the National Public Health Institutes which are also responsible for the surveillance or by large university hospitals or even academic centres. It is not compulsory that these laboratories are accredited or certified, although growing number of public health laboratories are accredited or certified by appropriate professional standards bodies. These laboratories are authorized to work with high risk pathogens as laid down in Community legislation.

Laboratories Accredited to Undertake Specified Individual Investigations

Such laboratories usually exist for the purpose of quality assurance, or for reference purposes to confirm the findings of another laboratory. Their services may include the use of alternative testing methodologies.

They may not be appropriate to use for primary forensic analysis as their operating methodology may be designed to simply confirm or refute the presence of a particular pre-defined material. They may be able to offer a range of such investigations; however, this should not be confused with the services that a laboratory capable of exhaustive analysis may be capable of providing.

Their importance lies in the quality of analysis that they may be able to bring to the identification of a particular hazard, as they may be able to offer highly specific or unusually sensitive methods; and they may be able to offer confirmatory analyses based upon alternative testing techniques to re-enforce the strength of the forensic evidence available to investigators.

Laboratories with Specialist Hazardous Material Handling Techniques

It is foreseeable that evidential specimens taken where the misuse of chemical, biological or radiological materials is suspected may be especially hazardous. In such instances it is important that forensic investigators have access to facilities that are capable of managing these materials safely. Therefore, security issues must be sorted out in advance.

These laboratories may be able to offer specialist handling and transportation systems from the incident scene to their analytical facilities; the storage of unusually hazardous materials; and the safe destruction of these materials when they are no longer required for evidential purposes.

---

5 EU Decision 2119/98/EC 'setting up a network for the epidemiological surveillance and control of communicable diseases in the Community'

6 EU Decision 2000/96/EC 'on the communicable diseases to be progressively covered by the Community network under Decision No 2119/98/EC' and any subsequent amendments.

7 Directive 98/79/EG (in vitro diagnostic directive).

Examples of the use of such specialist facilities may include the analysis of radioactive materials, chemical warfare agents and high risk biological pathogens.

Other Scientific Laboratories, or Institutions

These may include tertiary education facilities, research and development organisations and industrial manufacturers.

Such laboratories may possess unusual skills, equipment and capacity for analysing substances where capability in the normal forensic network does not exist.

Tertiary education facilities and research and development organisations may be able to offer access to newly emergent analytical techniques that have not yet gained accreditation or acceptance for use in forensic or diagnostic laboratories.

Industrial manufacturers may have particular expertise where the hazardous materials are presented as contaminants of manufactured items, where the presence, by design, of other chemicals or biological materials may mask the presence of the hazard to be identified.

Definition of Terms

Laboratory Accreditation

Laboratories performing analyses for forensic purposes (whether or not they are designated forensic laboratories) should, where possible, be accredited in line with appropriate international standards and norms, or to an appropriate equivalent national standard. An example of these standards is the UNE-EN-ISO/IEC 17025 'General requirements for the competence of testing and calibration laboratories'.

Accreditation usually refers to a single study methodology only (for example: a laboratory is accredited to obtain DNA profiles from blood; and not from any other biological sample). A laboratory may hold several accreditations, one for each analytical method or closely related group of methods. In some Member States, also a flexible accreditation is possible: laboratories here can show expertise in a broader range of analytical methods e.g. a flexible accreditation in mass spectrometry which could include several mass spectrometric techniques and single component analysis and additionally multi substance screening analysis for general unknown techniques.

Accredited laboratories have to be audited at regular intervals (for example once per year or one per eighteen months).

A laboratory which does not carry a specified accreditation, may be used to analyse forensic samples; however, they may require the explicit approval of a court, or have to present additional evidence in court justifying their ability to analyse the specimen to a judicially acceptable standard. This may be particularly relevant in respect of the use of novel CBRN agents for which an accredited analytical method may not exist.

Unlicensed diagnostic tests

Diagnostic tests, especially those used in reference laboratories, may not be licensed according to the in vitro diagnostic directive[7] for the following reasons:

1. The suspected case falls in the category of a rare pathogen; therefore, there is no market for a commercial test and indeed it is impossible to subject the test to sufficient numbers of occasions of use to meet the quality assurance standards necessary to receive CE authorisation.

2. The test is made by subjective interpretation, and therefore falls outside of a standard reproducible method, even when performed by highly trained personnel to strict standard operating procedures (for example electron microscopy of viral particles).

Quality control

Quality control is the process of inspecting testing systems; repeating analyses to ensure that consistent results are obtained (or a statistically appropriate proportion of all assays) to give re-assurance that the process used to perform the investigations can be relied upon to be accurate; and testing samples using other methodological assays to ensure that a high degree of reliability can be placed upon the reported results.

Quality assurance

Is a wider ranging methodology than quality control and encompasses controls assurance in all stages of management of an investigation and assay to ensure that there is the highest degree of confidence in the quality of results obtained. Important elements in assuring quality include:

- Use of components and reagents of proven quality and fitness.
- Records of training and retraining of staff and undertaking recurrent reviews of performance
- Testing of known standards to ensure that expected results are obtained on a regular basis
- The inclusion of reference specimens in normal work streams to give blinded checks on performance
- The issuing of reference specimens to multiple reference laboratories at the same time (quality assurance circles) to compare performance between laboratories
- Review of trends in identification rates (including if possible false positive and false negative identifications rates)

Storage and disposal of hazardous specimens

Specimens derived from investigations of CBRN related incidents may retain a degree of hazard that renders them unsafe for storage or disposal using conventional means. This is particularly problematic for radioactive materials. Most micro-biological agents can be denatured by chemical, heat or irradiation. Most chemicals can be denatured or safely

absorbed; or destroyed by high temperature incineration. Care should be taken to ensure that the permission of courts is obtained to dispose forensic specimens.

Where medium to long-term storage is mandatory especial arrangements may be required to arrange the necessary security commensurate with their chemical, radiological or microbiological properties. Such storage requirements may include for example:

- Shielded secured facilities for radioactive materials that hold appropriate licences for the inventory of radionuclides contained in the specimens;
- Very low temperature (-80˚C / -196 ˚C liquid nitrogen) storage of biologically active materials;
- Hermetically sealed temperature controlled vessels for chemical agents made of inert materials.

Individual MS may also have legislation governing the storage and disposal of human tissues that have to be considered.

Clinical evidence

Clinical diagnosis is the synthesis by a physician of a physical examination of the patient and the consideration of results of appropriate imaging, physiological and laboratory service investigations to determine the most likely clinical syndrome that explain a patient's illness.

In many cases clinical judgement as to the most probable disease process is sufficient to instigate treatment (the success or failure of treatment in itself is a diagnostic tool). Definitive evidence of the actual cause of disease may not be sought.

Laboratory testing is most likely to be sought, and be definitive, in the case of infectious diseases and internal radioactive sources; chemicals and toxins may be apparent only because of their metabolites, or may no longer be present in the body at the time of onset of illness; laboratory investigations of injury due to purely external radioactive sources may only provide indirect evidence of cause.

It follows that the diagnosis and management of clinical disease is often undertaken on the basis based on the most likely cause of illness. Therefore, where the diagnosis of clinical disease forms part of the presentation of evidence to a court, the physicians concerned need to be made aware of the standards of proof that they may be required to testify to. If made aware of these requirements early in the course of the management of a patient the clinical staff may want to obtain additional specimens or order for other investigations to be carried out that would not necessarily be required for the management of the patient's clinical disease. It should be noted that there are particular ethical issues to be considered when obtaining specimens not directly necessary for patient care and in releasing patient confidential information to law enforcement agencies.

Standards of proof

Clinical investigators and laboratories that do not ordinarily undertake forensic

investigations may be unaware that they may be required to state in their evidence the probability with which an observation or assertion can be given; or to certify that their evidence meets an agreed objective standard defined by their Member States legal system.

Therefore, it is good practice, where laboratories whose primary purpose is the support of clinical diagnosis are used for forensic purposes, that the reporting staff from such laboratories are trained in giving evidence according to the standard of proof required by the Members States judicial system; and that law enforcement officers meet clinicians caring for potential victims to discuss the needs for clinical evidence and the standards of proof that will be required.

Examples of Good Practice, identified in some Member States

A joint team of public health and law enforcement officers to oversee the laboratory services that are being used to investigate the potential misuse of a chemical, biological, radiological, or nuclear substance to ensure that the most appropriate facilities are employed to identify the material, to a high standard of proof, managed under appropriate safe systems of working.

Good Practice Checklist

Public Health/competent authorities	**Law Enforcement**
• Have Public Health authorities developed a list of all appropriate laboratories (reference, clinical, forensic) that may be able to support their investigations? • Does this list contain the current accreditation status as well as capacity for testing? • Are the Public Health laboratories working with Law Enforcement on the requirements for forensic testing, chain-of-evidence controls, and the legal standards of proof required by the jurisdiction they serve?	• Have Law Enforcement considered working with Public Health in creating a list of all appropriate laboratories and to, furthermore, encourage the collaboration between forensic laboratories and Public Health laboratories in order to complement each other? • Have Law Enforcement officers been acquainted with the benefits and limitations of using diagnostic laboratory facilities, especially when investigating unusual, novel or rare microbiological diseases? • Have the Law Enforcement worked with Public Health to familiarize the Public Health laboratories with their needs and requirements for forensic testing? • Have the laboratories performing forensic analyses been accredited according to international standards?

Extant guidance

- Laboratory designation, accreditation, and quality assurance and forensic requirements; the European network for accreditation:

  http://www.european-accreditation.org/content/ea/EuropNetwork.htm

- The European Network of Forensic Science Institutes (ENFSI) has been established with the purpose of sharing knowledge, exchanging experiences and coming to mutual agreements in the field of forensic science. ENFSI is recognised as an expert group in the field of forensic sciences. One of the core aims of the ENFSI is to encourage all ENFSI laboratories to comply with best practice and international standards for quality and competence assurance: www.enfsi.eu

12. MEDIA & PUBLIC RELATIONS: ADDRESSING THE PUBLIC IN CASES OF JOINT OPERATIONS

The issues

- Informing the public and maintaining their confidence and trust by ensuring early announcing, transparency and understanding of the public needs and perception of risks
- Preventing panic and public order disruption
- Public reassurance, vigilance, and awareness
- Ensure that public acts in a way that mitigates and minimise the impact of an incident
- Ensuring that the public assists in prevention & detection of crime
- Enabling the earliest possible return to normality
- Ensure media's right and duty to inform the public
    -

Context

CBRN attacks have significant impact regardless of the nature and scale of the attack – they are after all designed to promote terror in a population, and have a designed and specific class of psychological harm.

The media is the most important tool to communicate consistently and quickly with the public.

The general public can turn to both the police and health professionals for questions and they should not be discouraged from this interaction. Nevertheless, one need to be aware that this needs to be balanced with an awareness of the media needs; they may have difficulties to accurately report a story because of its complexity, the many players involved, and their differing agendas.

Good media management strategies provide a degree of control and help reduce the potential for inaccurate and speculative reporting. However, good coordination and working within the time pressure of the media can create an additional significant increase of work for the responding organisations.

Examples of Good Practice, **identified in some Member States**

Before an event (preparedness/primary prevention)

- Ensuring public relations and communications staff are incorporated into and part of all agencies contingency planning (public health and law enforcement)
- Developing an emergency communication plan, including agreed communication protocols and emergency public communication clearance processes
- Building productive relationships with the media based on trust, recognising each others' roles and requirements
- Organisation of media training for appropriate staffs in their respective roles (spokespeople, communicators, key hierarchy persons,…) and if possible running exercises
- **During an event**
    - **Logistical aspects**:
    - Using trained spokespersons who will explain the current situation to the media
    - Give early announcements regarding the incident
    - On-site briefings and interviews as soon as possible; use back-office public relations staff as little as possible
    - Scheduling of regular press briefings
    - Provision of media pool facility where possible and keep up active contact with major news agencies and other major news providers in order to reduce the impact of rumours, appellation to media's responsibility
    - Hotlines and appeals on TV with appropriate call centres and public advice lines, if appropriate with international numbers, in case international calls are to be expected / anticipated
    - Use of official websites to inform the public; link them to others' and update them regularly
    - Anticipate possible disruptions of infrastructure; prepare the public for possible short/mid-term consequences in their daily life
    - **Clear messages:**
    - Use key messages, show situation is under control
    - Keep the message consistent, empathetic, short and concise, and public safety focused
    - Early announcement of what is known as well as honesty about what is not known

- Sharing of dilemmas with the public
- Avoiding overly confident reassurances or misleading information
- Ensuring consistent message/language by all parties
- Ensure that the media do not fill gaps and make you spend time correcting wrong information
- Dispel media speculations and react to unjustified criticism
- The public message on the seriousness of the event should be consistent with the visible number of reactive measures adopted to tackle the problem.
- Public health to clarify technical terms
- Law enforcement to clarify terrorist / criminal terminology (avoid dubious terms, terrorist myths)
- Coordination and agreement on a common and consistent message:
- Intra-agency: experts/individual public relations liaison staff
- Inter-agency through formally designated public relations units
- Discuss with media what goes wrong, listen to their needs
- Monitor the media response and analyse the public needs and risk perceptions
- Provision of a single spokesperson (possibly per each response level) can help avoiding conflicting messages and counter different groups running their own publicity campaigns
- Issue public safety/health information briefings outlining effects of contamination, where to go for health screens, etc. (MS/EC/ECDC/EUROPOL linked websites)

After the event (tertiary prevention)

- Inter-agency cooperation can ensure good logistic support for drafting, agreeing and scheduling joint press releases
- Continuation of providing regular updates to media

Summary

- **General:**
- Avoiding over-reactions;
- Seeking to maintain public confidence;

– Honesty: no need to tell everything (especially when law enforcement inquiries are involved) but tell the truth (media can cross check with witnesses)

– Keep constant contact with the media; offer short concise communications; they become for media and public a source of info they trust and respect

– Communication plans and concepts established for preparedness purposes should focus on the main elements of the incident and the adequate response. They should remain sufficiently open so that they can be adapted easily to the communication needs surfacing during the unfolding of a real event

- **Clear messages**

– Aiming to clearing up of confusion quickly

– Correcting inaccuracies quickly

– Using key messages

– Avoiding of ambiguity

– Characterising terrorists as criminals;

– Being confident and reassuring, showing experience and expertise in dealing with these matters

- **Be available**

– Scheduling of intensive talks to communities

– Availability of permanent online presence (to reassure the public); offering short concise communications

– Be available to answer media questions at all times(24/7) but that does not mean accept every media bid, be selective and strategic

- **Use available resources**

– Use dedicated / well-known PR staff: they become a trusted and respected source of information for the media and the public

Good Practice Checklist

Public Health / Competent authorities	**Law Enforcement**
• Have Public Health services prepared communication plans (or annexes) for the management of CBRN incidents? • Have messages and instructions for the public based on a priority	• Have Law Enforcement authorities prepared communications plans (or annexes) for the management of CBRN incidents? • Has it been considered to

list of high threat agents been prepared? • Has the capacity for hotlines and call centres for responding to the public been build-up? • Have exercises on the subject of communication been held? • Have Public Health services participated in relevant communicator networks at the EU level? • Have productive relationship been created with media at the national level (for example in the form of regular meetings, training, lessons learnt sessions)? • Has an algorithm of information flow and communication (who will be in charge, spokespersons, press releases, etc.) been agreed with Law Enforcement services? • Has this aspect been included in the MOU for collaboration?	prepare messages and instructions for the public based on a priority list of high threat agents? • Has a specific website for public information been created? • Have exercises on the subject of communication been held? • Have Law Enforcement services participated in relevant communicator networks at the EU level? • Have there been efforts to create a productive relationship with media at the national level (where appropriate)? • Has an algorithm of information flow and communication (who will be in charge, spokespersons, press releases, etc.) been agreed with Public Health services? • Has this aspect been included in the MOU for collaboration?

Extant guidance

- EPC Working Paper, Improving the Quality of Risk Management in the EU: Risk Communication, 2003 B. Ballantine, The European Policy Centre.
- Communicating in a Crisis: Risk Communication Guidelines for Public Officials, 2002, SAMHSA (http://www.riskcommunication.samhsa.gov/RiskComm.pdf)
- Terrorism and other Public Health Emergencies: A Field Guide for Media, US DHHS, http://www.hhs.gov/emergency
- Bioterrorism: A Journalist Guide to Covering Bioterrorism, 2nd Edition, 2004, D. Chandler & I. Landrigan, Radio and Television News Directors Foundation.
- Journalisten- Handbuch zum Katastrophenmanagement, German Committee for Disaster Reduction, 2002, 7.Auflage
- CDC, Crisis and Emergency Risk Communication, Oct 2002, B. Reynolds (http://emergency.cdc.gov/firsthours/resources/websites.asp)
- M O D E L, Emergency Response and Communications Planning for Infectious Disease Outbreaks and Bioterrorist Events, Oct 2001, Association of State and Territorial

Directors of Health Promotion and Public Health Education

- Northwest Centre for Public Health Practice, Univ of Washington
    - Module on Emergency Risk Communication for Public Health Professionals (http://www.nwcphp.org/training/courses-exercises/courses/risk-communication)
    - Module on Effective Communication for Environmental Public Health (http://www.nwcphp.org/training/courses-exercises/courses/communication-for-eph)
- WHO, Field Guide: Effective Media Communication during Public Health Emergencies, 2005, V. Covello (WHO/CDS/2005.31a)

13. TRAINING AND EXERCISES

The issues

- Regularity and intensity of training
- Different levels of management may require different training
- Inter-agency versus intra-agency training
- First line officials need hands on training
- Awareness of allied technical and professional persons needs to be stressed

Context

Training in public health surveillance and response at the EU level has developed extensively in the past decade through the European Programme for Intervention Epidemiology Training (EPIET) and several large national Field Epidemiology Training Programmes (FETP)

In addition, modules for joint training between law enforcement and public health have been developed by DG-SANCO / DG-JLS / EUROPOL / EPIET, via a series of train-the-trainer modules. However, these modules have not yet led to the widespread establishment of national and regional level training programmes to develop the joint working of law enforcement and public health services.

Since this paper considers developing the collaboration between two very different disciplines and between different organisations at multiple administrative levels, obstacles to smooth collaboration are to be anticipated, especially when it may be expected that collaborative operations will take place under time pressure, be subject to public scrutiny and the two organisations separately may have differing goals to the outcome of their operations.

Joint training at operational, tactical and strategic levels can be an instrument to identify and remove these obstacles.

Principal elements of a training system

Ideally, at all levels (local, regional, national and international) law enforcement and public health professionals would engage in joint training on topics that concern both disciplines. This type of training should focus on shared relevant technical knowledge (theory) and on strengthening practical skills.

By composing training teams that consist of senior trainers in both disciplines (law enforcement and public health), and by planning a series of national train-the-trainer courses the training can be further disseminated.

A curriculum of joint law enforcement and public health training should ideally be harmonised or in many ways made comparable amongst EU Member States and possibly be in line with similar courses in countries outside the EU, in order to enable international investigations. The focus of the training should be on dealing with crisis situations and optimising synergy between disciplines during crisis control.

The frequency of the training should allow the maintenance of a sufficiently large body of trained experts in law enforcement and public health authorities that are able to work together effectively during a crisis. Ideally, there should be a regular audit to establish that collaboration is being effectively maintained by means of simulation exercises.

There are no fixed rules on the minimum frequency or duration of training, but a good generic rule is that training should be of such frequency and duration that those who are trained form a multidisciplinary team of front line professionals that are on a first name basis, and can explain each other's role in the team during a crisis.

In addition to training and simulation exercises, countries may choose to arrange exchange of senior trainers between law enforcement and public health authorities for certain, possibly extended, periods in order to understand each other's organisation and modus operandi.

Requirements for effective training

Part of the training will need to include the coordinated management of the response processes. This can only be done if there is agreement on the coordination procedures.

If not in place, joint arrangement or MoU can mention workshops aiming at identifying good practice in coordination and management of joint operation (line of command, communication and jurisdiction issues etc) and can lead to accepted procedures.

Examples of Good Practice, identified in some Member States

- National coordination of joint training with input from both law enforcement and public health authorities. This can include developing joint training material and joint case studies with country specific scenarios.
- To identify the trainees, transparent and effective selection procedure for participants are useful to achieve training objectives for the target audience.
- Lectures and facilitations by experts in the field; training method focussed on sharing expert experience
- Joint evaluation/debrief of real life situations where cooperation between law enforcement and public health was required to identify strengths and weaknesses; training scenarios developed from such debriefings can be particularly valuable

Good Practice Checklist

Public Health	**Law Enforcement**

• Have joint training material with the Law Enforcement authorities been developed? Have there been efforts to harmonise among other MS and possibly internationally?
• Have joint case studies with country specific scenarios been considered?
  • Had these case studies detailed objectives per module of training?
  • Was appropriate quality assessment used?
• Have regular trainings for the staff participating in epi investigations been set up following a transparent procedure?
• Have the Public Health services fostered and participated in real-life debriefing of joint investigations with the Law Enforcement services?
• Have training needs assessment been performed for this type of joint training?
• Were priorities for such joint training set up?
	• Has joint training material with Public Health services been developed?
	• Were true joint case studies with country specific scenarios used or the experience from other MS?
	• Were regular trainings for the staff participating in epi investigations following a transparent procedure set up?
	• Have the Law Enforcement services fostered and participated in real-life debriefing of joint investigations with Public Health services? Have these experiences been used as examples for training?
	• Have training needs assessments been performed for this type of joint training?
	• Were priorities set up for such joint trainings?

Extant Guidance • European forensic epidemiology course (on request to DG-SANCO / ECDC / EUROPOL) • EPIET (2-day) module on BT response (Berlin 2003, on request available to ECDC)) • Public Health general: Lectures and Case studies of EPIET www.epiet.org • Training Material produced by Interpol • CDC-forensic epidemiology course http://www2.cdc.gov/phlp/ForensicEpi/Background.asp • EU health sector exercise repository (for authorities)	

Annex 1: DEFINITION AND SEMANTICS

CBRN-Defence, by NATO. Plans and activities intended to mitigate or neutralise adverse effects on operations and personnel resulting from: the use or threatened use of C, B, R or N weapons and devices; the emergence of secondary hazards arising from counterforce targeting; or the release, or risk of release, of Toxic Industrial Materials into the environment . However the reference to "weapons" may lead to confusion, as precursors are not necessarily a weapon (yet).

Communicable or infectious disease. Diseases caused by infectious agents such as bacteria or viruses. Individuals may be infected from agents in the environment, infected animals, and infected people. These diseases are distinguished from genetic diseases, diseases caused by toxic exposures, and chronic illnesses such as diabetes and cardiovascular disease. The terms "communicable" and "infectious" are used interchangeably. Examples: the common cold, salmonella, Severe Acute Respiratory Syndrome (SARS).

Cordon sanitaire. An area that has been closed off to prevent the spread of a communicable disease. No one will be allowed to enter, and persons in the area may be kept from leaving or may be evacuated, depending on the nature of the threat.†

Epidemic disease. The occurrence of more cases of disease than expected in a given area or among a specific group of people over a particular period of time. Synonymous with the term "outbreak."

Epizootic. An outbreak or epidemic of disease in animal populations.‡ Examples: avian flu in fowl, foot and mouth disease in cattle.

Hazard. A hazard is a substance, agent, condition, situation or event (incident) which poses a level of threat or harmful effect to life, health, property or environment. Most hazards have only a theoretical potential of harm, however, once a hazard has the potential to reach a large number of persons or area, it can create an emergency situation.

Incidence. The rate of new cases in a community over a given time interval, such as two cases per day. Examples: 20 cases of chickenpox in a week; 20,000 new cases of tuberculosis in a year.

Incubation period. The time between when a person is first exposed to a communicable disease and the time when the person exhibits symptoms of the disease and becomes capable of spreading it to others. Diseases with short incubation periods, such as measles or smallpox, can cause fast spreading epidemics or pandemics because there will be a constant supply of infectious persons as new contacts become infected. Diseases with a long incubation period such as tuberculosis spread much more slowly, but can also reach high levels in the community.

Isolation. Separation of infected individuals from those who are not infected. Example: placing a person with infectious tuberculosis in a restricted-access hospital room.

Medical intelligence. That category of intelligence resulting from collection, evaluation, analysis, and interpretation of foreign medical, bio-scientific, and environmental information that is of interest to strategic planning and to military medical planning and operations for the

conservation of the fighting strength of friendly forces and the formation of assessments of foreign medical capabilities in both military and civilian sectors.

Outbreak. Synonymous with "epidemic." The term is alternatively used to describe a localized (as opposed to generalized) epidemic.

Prevalence. The total number of cases of disease in a community at a point in time. Example: the total number of persons living with HIV in a major city.

Pandemic. An epidemic occurring over a very wide area (countries or continents) and usually affecting a large proportion of the population. The term "panzootic" is used to describe a pandemic in animals. Example: winter flu pandemic in the northern hemisphere.

Quarantine. Preventing a person who has been exposed to a communicable disease, but is not yet showing signs of infection, from coming in contact with others. Example: requiring health care workers exposed to SARS to stay home until the incubation period has passed.

Risk. Risk is related to the likelihood of occurrence of the hazard and to the potential vulnerability or impact it may cause if it occurred. Qualitatively, risk is proportional to both the expected losses which may be caused by an event and to the probability of this event.

Risk assessment. In the context of public health, risk assessment is the process of quantifying the probability of a harmful effect or hazard to individuals or populations. In the context of law enforcement, the risk assessment is a function of the threat related to vulnerability of the target and the potential consequence of the release of the threat.

Risk management. A process, distinct from risk assessment, of weighing policy alternatives, in consultation with interested parties, considering risk assessment and other factors relevant for health protection of consumers and for the promotion of fair trade practices, and if needed selecting appropriate prevention and control options.

Social distancing. The process of reducing contacts between individuals to reduce the chance of the disease spreading. Community social distancing can include barring public gatherings, closing public places such as malls and movie theatres, cancelling sporting and entertainment events, and closing nonessential workplaces.

Surge capacity. The maximum patient load a hospital or medical system can handle.

Threat. Threat relates to the likelihood of occurrence of the hazard or event with a harmful effect. In contrast to risk, a threat is not related to the impact it may cause. In the context of public health, a threat is defined as a substance, agent, condition, situation or event (incident), which by its presence has the potential to rapidly harm, directly or indirectly, an exposed population, sufficiently to lead to a major crisis.

Dormant threat- The situation has the potential to be hazardous, but no people, property or environment is currently affected by this. For instance, a hillside may be unstable, with the potential for a landslide, but there is nothing below or on the hillside which could be affected.

Potential threat- Also known as 'Armed', this is a situation where the hazard is in the position to affect persons, property or environment. This type of hazard is likely to require further risk assessment.

Active threat- The hazard is certain to cause harm, as no intervention is possible before the incident occurs.

Mitigated threat- A potential hazard has been identified, but actions have been taken in order to ensure it does not become an incident or at least significantly reduce the danger.

Threat assessment. Threat assessment focuses on the probability of the harmful effect or hazard to be present. In the context of law enforcement, the threat assessment is a function of the intention and the capability to harm.