TERROR
Strengthened preparedness and response to biological and chemical terror attacks

Co-funded by the Health Programme of the European Union

BIOLOGICAL AND CHEMICAL TERROR ATTACKS:

Risk and Crisis Communication Guidance Tool

Author(s):

Lead author: Dr. Dimitrios Iliopoulos, NPHO - Greece

Co-authors: Georgios Dellis, NPHO - Greece
Stamatis Parisis, NPHO - Greece
Gerasimos Gerolymatos, NPHO - Greece
Maro Angelopoulou, NPHO - Grece
Urska Kolar , National Public Health Institute – Slovenia
Kjetil Berg Veire , Norwegian Institute of Public Health (NIPH) – Norway
Marit Garfjeld, Norwegian Institute of Public Health (NIPH) – Norway
Maja Knepr Šegina, Croatian Institute of Public Health – Croatia
Dragana Jovanovic – IPHS – Serbia
Milena Vasic, IPHS – Serbia
Vesna Karadzic, IPHS – Serbia
Katalin Steib, NNK - Hungary
Tanya Melillo , Department for Health Regulation - Malta

Contents

ANNEX A: Crisis Communication Check List **48**

This report arises from the TERROR Joint Action, which has received funding from the European Union through the European Health and Digital Executive Agency of the European Commission, in the framework of the Third Health Programme 2014-2020. The European Commission is not responsible for the content of this report. The sole responsibility for the report lies with the authors, and the European Health and Digital Executive Agency is not responsible for any use that may be made of the information contained herein. The authors are not responsible for any further and future use of the report by third parties and third-party translations.

Main messages

A biological or chemical terror attack will challenge how to communicate quick and coordinated both to the public and between the sectors responsible for the response.

Experiences from incidents and scientific literature point on challenges like lack of coordination, lack of information, fear and confusion, and misinformation.

Rapid, open, and coordinated communication with the public can determine to what degree terrorists will succeed with their intentions. Therefore, risk communication should be considered as a foundation for national security.

This guideline recommends the following steps to be considered and taken in all European countries.

Preparedness phase:

- Decision-makers should discuss risk communication across the security, civil protection and health sectors, and on a strategic level.
- Capacities for effective risk communication should be secured.
- Risk communication in terrorist attacks should be considered in developing, updating, and revising preparedness plans and exercises.
- Public awareness about biological and chemical incidents should be raised.

Emergency response phase:

- The communication response should be immediate.
- The information should be trusted, precise, and accurate.
- Information sharing between stakeholders should be rapid.
- The needs and expectations of the society and vulnerable groups should be included.
- All health-related information that can protect the public's health should be released.

Recovery phase:

- Communication with those directly harmed or affected should be continued for as long as they need it.
- Involvement with the general public should be continued.
- Trust and facilitation for understanding, learning, and healing should be restored.
- Documentation of what has been done should be ensured.

All phases:

- Social media is a leading channel for communication that should be used in a dialogical way.
- Disinformation should be monitored and handled
- Executive summary

The objective of WP7 of JA TERROR is to promote the implementation of Risk and Crisis Communication at all stages of risk management, on both national and EU level.

During a crisis or emergency, communication to the public may include media releases, website content, talking points for spokespersons, interviews, social media posts, public service announcements and advertising. It is important to determine which populations are at greater risk and use the most appropriate methods to reach both them and the public.

In addition to providing accurate and timely information, informative material for the public must also address and deal with misconceptions, misinformation and rumours.

Communication planning must be an integral part of Generic Plans, including the development of country-level technical guidance as well as public information and training.

To this end, the scope of this text is to develop a guide - handbook to act as guidance on risk and crisis communication between the relevant responders and towards the public, in the cases of terrorist attacks involving biological and / or chemical agent(s).

Creating, structuring and putting in writing the guidance on risk and crisis communication, has been a multistep procedure, during which the following crucial steps were taken into consideration:

- Identification of gaps in inter-sectoral risk communication procedures at all levels
- Identification of best practices and existing guidelines
- Main theoretical concepts
- Analysis of already applied experience implemented in Member States
- Analysis of After-Action Reviews from recent events and relevant Exercises.

This guidelines' handbook aims at providing advice regarding risk communication at a biological or chemical terror attack within Europe.

According to the WHO, risk communication describes the process of real-time exchange of information, advice, and opinions between experts or officials and people who are called to respond and deal with a hazard and/or hazardous event.

Also, Risk Communication as a term, is documented to refer to a broad and multi-disciplinary academic field, incorporating and describing all separate, interrelated and coordinated communication activities and tools of the whole communication spectrum, from communication channels with the public i.e. the media, web pages, and social media, communication with and amongst stakeholders, to community engagement.

Additionally, it is a common practice to divide risk communication into three phases:
The preparedness phase, the emergency phase, and the recovery phase.

This three-phase categorization is also used in the current document. After the introduction which includes the objective of the document and the description of its target audience, in the second chapter regarding the Recommendations, emphasis is given to

- Communications involving immediate response to questions like what has happened, to who, by whom.
- Coordination of the flow of information between central stakeholders at an international, national, regional, and local level.
- Risk communication at terrorist attacks to be considered in developing, updating, and revising preparedness plans and exercises.
- Public awareness to be raised.
- Handling of disinformation and fake news, the recognition, analysis and counteraction to both of which, have become an integrated part of all communication activities, the last few years.

In the third chapter, collection and evaluation of relevant literature and background reading to review and quote incorporated and was identified on the following four criteria categories:

- Definition of risk communication and basic principles.
- Information speed, frequency, accuracy and understandability.
- Openness and transparency.
- Communication as an interactive process.

Moving forward, the fourth chapter on Challenges, Gaps and Confidentiality included in the current document-handbook, incorporates the identified challenges, which have been recognized, described and observed from the perspectives of the emergency management phases.

Next, on chapter 5, crucial for efficient Risk Communication is the Risk escalation taking place during these incidents. Risk escalation is a risk response strategy that involves transferring the ownership and accountability of a risk to a higher Authority.

The response strategy is required to be designed and built upon clear and concise context. After an escalation procedure, it is a necessity to follow up on the communication actions that were agreed upon and report on the progress and outcomes.

To conclude this chapter, an escalation algorithm describes the flow of information between the Scene of incident (Hot zone), the Stakeholders and how the information ends at the Operational and Strategic level.

In the final chapter a brief presentation of serious CBRNE events in different countries from the perspective of the management at communication level is developed to give real-life events' examples.

1 INTRODUCTION

The purpose of this guideline is to provide advice regarding risk and crisis communication in the preparedness or response to a biological or chemical terror attack in Europe.

Risk and crisis communication is an integral and critical part of risk management. Risk communication is described by the WHO as the process of real-time exchange of information, advice, and opinions between experts or officials and people who face a hazard. It helps to raise awareness, enable informed decision-making, and foster trust during crises.

Risk communication as a field is broad, covering both communication channels such as media, web pages, and social media as well as stakeholder and community engagement through for example volunteer organizations and groups.

It should be noted that even though communication measures can help solve communication challenges, communication measures surely cannot alone solve management issues, for example, challenges regarding roles and responsibilities among governmental organizations in a crisis. Health preparedness and planning, as well as cross-sectoral collaboration between health, security and civil protection are addressed in WP 5 and WP 6 of JA TERROR respectively.

Crisis communication on the other hand, has been identified as a way to help and support social cohesion during such crisis and through the recovery phase, as described by the United Nations Office of Counter Terrorism/ UN Counter-Terrorism Centre (UNCCT) in the respective published communication toolkit.

Generally, it is common to divide risk and crisis communication into three phases: The preparedness phase, the emergency phase, and the recovery phase. We also use this categorization in this document.

About the project

The main objectives of the EU-funded project "Joint Action to Strengthen Health Preparedness and Response to biological and chemical terror attacks" (JA TERROR) are to address gaps in health preparedness and to strengthen cross-sectoral work with security, civil protection, and health sector response to such deliberate events. 17 countries and more than 30 partners are involved across Europe, in a project running for four years from 2021.

The specific objective of Work Package 7 about Risk and Crisis Communication is to promote the implementation of Risk and Crisis Communication in all stages of risk management, on both national and EU levels.

This guideline is one of the deliverables of the project.

Objective of the document

The main objective of the document is to provide practical information on how to manage the flow of risk and crisis communication among stakeholders and the public in the event of a biological or chemical terror attack.

Target audience of the document

The target groups of the Guidance Tool are decision-makers, risk and crisis communicators, and communication experts.

2 RECOMMENDATIONS

The recommendations in this guideline are given from a health sector perspective but should be applicable to all sectors with the responsibility to public health in the event of a biological or chemical terror attack, for example, both for the health, security, and civil protection sectors. These recommendations are defined, grouped, and presented per each phase in the emergency management cycle and should be considered in developing, updating, or revising the national, sector, and facility emergency management plans.

2.1 Preparedness phase

Introduction

A biological or chemical terror attack will need immediate communication response to answer questions like what has happened, to whom, what sort of substances are involved, how many casualties are there, what should people do to avoid danger and who is responsible.

In addition, a terror attack will evoke feelings like fear, anxiety, and other psychological reactions. According to Ruggiero & Vos (2015), such reactions may pose a greater threat than the act itself. People could for example become passive, ignore or misunderstand advice.

As communication plays a significant role as an amplifier/multiplier or saturator of a terrorist attack's effects, risk and crisis communication preparedness could determine to what degree terrorist actors will succeed with their intentions.

Decision-makers should discuss risk and crisis communication on a strategic level

Risk communication, risk perception, and risk behaviour should be considered foundations of effective national security and should be thoroughly prepared, according to Rogers and Pearce (2013).

Decision-makers should ensure that risk and crisis communication in the event of a biological and/or chemical attack is discussed at a strategic level and addressed in relevant policy documents. The results of the discussion should be able to answer the following questions:

- Who oversees early warning amongst stakeholders, both nationally and on an EU level?
- Who must coordinate the flow of information between central stakeholders at an international, national, regional, and local level?
- Who must inform the public on the available national communication channels, such as traditional media, web pages, and social media and answer the media in the event of a biological or chemical terror attack?
- What are the communication procedures to put in place?
- Who holds the information release authority and classification of information?

Capacities for effective risk and crisis communication should be secured

Risk communication is defined as a core capacity in the International Health Regulations (WHO). Capacities for effective risk communication regarding biological or chemical terror attacks should be overseen and secured. Moreover, risk communication competence is expected to be represented in strategic crisis management groups and central organizations should have the capacity for emergency communication among relevant governmental agencies and the media. A secure platform to exchange classified information to this purpose, can be developed as of crucial importance. (D7.2 by WP7).

Risk and crisis communication in terrorist attacks should be considered in developing, updating, and revising preparedness plans and exercises

European countries should ensure that risk and crisis communication is exercised and implemented in preparedness plans on all relevant levels, both nationally on a policy level and within the different entities with responsibilities. Both governmental organizations and representatives from civil society and/or the public should be involved in national exercises. The media is crucial when it comes to communication with the public in a biological or chemical terror attack and should also be given the opportunity to build competence, by for example being invited to seminars or conferences regarding the topic.

Public awareness about biological and chemical incidents should be raised

Awareness of biological and chemical terror attacks should be raised, for example by updating relevant national webpages with information about biological and chemical terror attacks, and public recommendations about what do to in the event of such an attack should be overseen and updated. At the same time, extensive information should be avoided in order not to provoke fear and confusion.

Relevant awareness information could for example be what to do when you think you might have been exposed to a harmful substance: Move away, do not touch your face, remove outer clothing, etc, as recommended in Pre-Incident Public Information Materials for CBRNE threats in Proactive – final brochure (page 9)[1].

2.2 Emergency response phase

The communication response should be immediate and timely

Immediate response and information sharing on web pages, the media, and social media is paramount to make it possible for people at risk to take action to protect themselves. Careful formulation and shaping of risk communication messages are to prevent negative health behaviour and initiate timely and appropriate individual and community reactions.

The information should be trusted and accurate

Precise and accurate information is paramount to mitigate misinformation and manipulation from misinformed or ill-intentioned persons. For advice for first responders, see Public messages to use in the immediate response to a CBRN attack (Interpol).

Be careful to provide information both about what is known, what is unknown, and what is being done to get to know more about what has happened, where, and with what sort of biological or chemical agent. The organisation's credibility is crucial and should not be compromised at any time and for any reason.

Information sharing between stakeholders should be rapid

Immediate risk communication requires rapid information sharing and clarified roles and among the stakeholders with responsibilities to a biological or chemical attack. When roles and responsibilities are unclear, common cooperation on all levels is even more important.

More recommendations regarding information sharing and joint incident management between health, security and civil protection are also given in JA TERROR (D6.5. of WP6)

[1] Proactive – Final brochure (2023)

The needs and expectations of the society and vulnerable groups should be included

A bioterror attack will arouse fear, anxiety and concerns among the public. It is important to include the needs and expectations of civil society and especially those of vulnerable groups. See also recommendations from the EU project Proactive in Proactive – final brochure[2].

All health-related information that can protect the public´s health should be released

There might be several constraints on the information flow during a biological or chemical terror attack. The sort of information can be disclosed among stakeholders involved in the handling and the public, might be limited by criminal investigation and prosecution. The same goes for information that has been characterized as classified. All organizations with responsibilities should be committed to ensuring that all health-related information that can protect the public´s health and safety is released to the public.

2.3 Recovery phase

The aftermath of a biological or chemical terror attack will last for weeks, months, and years. People affected need to regain control over their lives. People harmed either directly in the terror attack or afterward by for example long-term damage will need support and information. The need for keeping attention to what has happened and using resources on risk communication will go on for a long time.

Communication with those directly harmed or affected should be continued for as long as they need it

There will be a wide variety of communication needs from different parts of the public after a biological or chemical terror attack. Those directly harmed need information about what has happened and how to recover their health as much as possible. Health effects could be long-lasting and have a negative effect on mental health. People affected need information about how they can act to help themselves and their families, for example, how areas might be contaminated and when it is safe to return to contaminated areas (Ruggiero & Vos, 2015). Volunteers need guidance about how to help. People not directly affected need to know what has happened, why and what is being done to mitigate the situation.

Involvement with the general public should be continued

All key institutions should have participatory mechanisms both to generic preparedness plans and exercises involving affected groups and organisations in the recovery effort (Ruggiero, Vos, & Paltalla, 2014).

[2] Proactive – Final brochure (2023)

Restore trust and facilitation for understanding, learning and healing should be restored

Risk and crisis communication is not limited to the simple issuing of messages and instructions. Risk communication is also a part of the understanding of what has happened, creating meaning of the event, and the view of the world and people themselves (Ruggiero & Vos, 2015).

Pay attention to how communication activities can help institutions, people, and society understand, interpret, and heal after a biological or chemical terror attack.

It is important to consider and address the needs, concerns, and feelings of those not directly affected by the terror attack, also after the incident.

Documentation of what has been done should be ensured

Terror attacks will most probably raise questions about how the incident was handled. What went wrong, and could anything has been handled in a better way? Be careful to document and archive communication measures, messages, and advice given at different time slots to make it possible to scrutinize the handling of the incident (lessons learned).

2.4 Recommendations regarding all phases

The role of social media

Studies show that users flock to online sites during emergencies, often in search of trustworthy information, with social media being among the primary sources of information in the event of a crisis (Konow-Lund, 2018). Social media has thus become a leading channel for disseminating information directly to users without the intermediary role of mass media.

Findings from a case study on social media activity during terrorist attacks in Norway offer seven recommendations for key communicators in official crisis management and response institutions, journalistic institutions, NGOs, and others: (1) acknowledge social media as important and master monitoring and management of features across social media; (2) synchronise communication and establish a standard operating procedure (SOP); (3) establish and make known a joint social media emergency account; (4) participate, interact and take the lead; (5) be aware of non-hashtaged content; (6) implement verification tools and practices and (7) engage with and learn from celebrities (Steensen, Frey, Hornmoen, Ottosen, & Konow-Lund, 2018).

It is important to use social media in a dialogical way. This translate to being a channel for disseminating information quickly and directly to users, as well as playing a critical role in information gathering. Backholm and others (2018) developed and tested a tool (RESCUE) for gathering information to better develop crisis communication (Backholm, Högväg, Knutsen, Lindholm, & Westvang, 2018).

Disinformation should be monitored and handled

The handling of disinformation and fake news has become an integrated part of all communication activities in the last few years. Events such as emergencies might for example draw attention from and be exploited by foreign information and manipulation interference operations[3]. Disinformation communicated during events with a high degree of uncertainty can influence both the definition of the situation and the social reactions (Innes, 2020). It would be plausible to assume that the development of artificial intelligence will reinforce this. In this document, we have not evaluated scientific papers about disinformation and given advice specifically regarding disinformation since this is a topic on its own.

There are immediately several good information sources and advice regarding disinformation and fake news, many of which were produced and distributed during the COVID-19 pandemic.

- Producing and disseminating facts and accurate information is the first step as described by an article from the United Nations[4] regarding the COVID-19 response. The UN also highlights collaborating with businesses like WhatsApp and Facebook, working with media and journalists, mobilizing civil society, and speaking out for rights as important mitigation measures.
- Monitoring the media landscape, engaging, debunking, and searching for partnerships are among the recommendations from the European Centre for Disease Prevention and Control[5]. Even though the factsheet is meant to counter online vaccine misinformation, the recommendations most likely would be applicable to other situations.
- NATO's approach[6] is to understand the information environment, engage with the public, expose major cases of disinformation, and coordinate with Allies and partners.

The framework Resist 2[7] also gives a comprehensive understanding and measures to counteract disinformation operations.

It is always important to monitor the information environment and identify disinformation narratives that could be harmful for the public.

[3] 2nd EEAS Report on Foreign Information Manipulation and Interference Threats: A Framework for Networked Defence (2024). Available at: EEAS-2nd-Report on FIMI Threats-January-2024_0.pdf (europa.eu)
[4] 5 ways the UN is fighting 'infodemic' of misinformation. (UN)
[5] Considerations for national health authorities to counter online vaccine misinformation. (ECDC, 2021)
[6] NATO's approach to countering disinformation. (NATO, 2023).
[7] Government Communication Service: RESIST 2: Counter-disinformation toolkit. (Resist 2, 2021).

3 EXISTING GUIDELINES AND LITERATURE

3.1 Definition of risk and crisis communication and basic principles

In these guidelines, we adopt the description and definition of risk communication as stated by the WHO.

According to WHO, risk communication is the real-time exchange of information, advice, and opinions between experts, community leaders, officials, and the people who are at risk and is an integral part of any emergency response. In epidemics and pandemics, in humanitarian crises and natural disasters, effective risk communication allows people at risk to understand and adopt protective behaviours. It allows authorities and experts to listen to and address people's concerns and needs so that the advice they provide is relevant, trusted, and acceptable[8].

Risk communication is described as "accurate information provided early, often, and in languages and channels that people understand, trust and use, enables individuals to make choices and take actions to protect themselves, their families and communities from threatening health hazards".

The definition of emergency risk communication according to the WHO is "an intervention performed not just during but also before (as part of preparedness activities) and after (to support recovery) the emergency phase, to enable everyone at risk to take informed decisions to protect themselves, their families and communities against threats to their survival, health and well-being".

On the other hand, a crisis communication plan enables authorities to deliver information that helps people act properly, taking into consideration their physical and mental health and well-being. Messaging refers to persuasive communication designed to change behaviours.

The definitions of risk and crisis communication differ, in the way that risk communication is based on ongoing projections and calculations of the potential for future harm (Infanti, et al., 2013), for example communication about the risk of smoking, while crisis communication is about emergencies, for example an occurring outbreak of transmittable disease.

The terms are however often used interchangeably, and the measures needed are with few exceptions the same.

In this guidance tool, we are using both terms. Both "risk communication", "crisis communication" and "emergency communication" will for the most be referred to as the same process as described and defined by the WHO.

[8] Communicating risk in public health emergencies (WHO, 2017)

Basic principles described in the existing guidelines we build upon are particularly about the need for rapid and timely communication, openness and transparency, and risk communication as an interactive process between decision-makers, experts, and the public.

In the following, we have extracted basic principles from existing guidelines that we think should be paramount for all risk and crisis communication. The Guidelines used as background are from, in addition to the guidelines from the WHO, the European Centre for Disease Prevention and Control (ECDC), Centres for Disease Control and Prevention (CDC), the European Food Safety Authority (EFSA), and Interpol (see also chapter 3.3).

Basic principles

- **Rapid and timely communication**

  Information should be provided accurately, early, often, and in languages and channels that people understand, trust, and use, to enable individuals to make choices and take actions to protect themselves (as stated by the WHO).

  In the early stage of a bioterror attack, in the absence of details, as much as possible should be provided about the substance and what the public can do to protect themselves and others (as stated by Europol). This requires respective preparedness of the organisation.

- **Credibility**

  In the effort of providing rapid and timely information, we should safeguard that the credibility of the organisation will not be compromised, so any released information should be accurate and truthful.

- **Openness and transparency**

  Openness is crucial to good risk communication and the reputation of an organization. If advice and action are to be trusted, it is important that risk assessments are published in a timely way and that information on which decisions are made can be scrutinized (as stated by the EFSA).

  Communication by authorities to the public should include explicit information about uncertainties associated with risks, events, and interventions, and indicate what is known and not known at a given time (as stated by the WHO).

- **Communication as an interactive process**

  Risk communication is about the real-time exchange of information, advice, and opinions between experts, community leaders, or officials and the people who are at risk (as stated by the WHO).

  When communicating about risks, the needs and expectations of civil society, and especially those of vulnerable groups, as well as plans on how to engage with such groups, should be included (as stated by the Proactive project).

- **Cooperation**

  Coordination of agencies responding to a biological or chemical terror attack is challenging, particularly when there are multiple interests and agencies and sectors such as the health sector, law enforcement, civil protection, etc. involved (as stated by the CDC). Good cooperation between different sectors is crucial to facilitate risk communication in emergencies.

3.2 Methodology

The guidance tool is evidence-based as it based on best practices and and after-action reviews from the COVID-19 pandemic

The methodology we have been following is:

- Identify best practices, existing guidelines and gaps to address within risk and crisis communication through experts' workshop (MS49 of WP7) and national meetings.
- Literature review of scientific findings about risk and crisis communication on biological or chemical terror attacks
- After-action reviews from the participating member states in the project
- Evaluation and feedback from the users of the guidelines (decision-makers, risk communicators, and communication experts) through national and European meetings and workshops

Limitations of the recommendations

Biological and chemical terror attacks are rare, and there are few lessons learned from practical communication activities regarding such attacks, mainly after COVID-19 pandemic. For incidents have taken place before social media came into people´s lives, best practices regarding risk communication still focus on efforts that should be forwarded to address.

Biological and chemical terror attacks refer to a great variety of methods and scenarios, and it is difficult to point out what could be the most probable scenario. Risk and crisis communication should be implemented in an all-hazards approach to mitigate gaps in preparedness plans and practice.

The recommendations in this guideline are mostly seen from a health perspective. Input from law enforcement and civil protection sectors in workshops and meetings has been highly valuable and have provided added value in minimizing uncertainties we have concerning this.

3.3 Existing guidelines and main theoretical concepts

Risk and crisis communication are broadly researched topics, addressed within multiple disciplines, such as Communication Studies, Psychology, Sociology, and other Social Sciences. In addition, addressing these topics often requires including elements of Environmental science and Medicine, making it a complex field. Since this is a field, where high uncertainties are the norm, literature suggests that to perform effective risk communication, critical evaluations of high uncertainty have to be undertaken that take account of the social, political, ethical, and material forces that delineate and shape its interpretation, uses, processes and ultimately its consequences (Wardman & Mythen, 2016).

Additionally, we have adopted findings from the EU Horizon 2020 project Preparedness against CBRNE threats through common approaches between security practitioners and the vulnerable civil society (Proactive)[9], and Interpol[10]. Our overview of the scientific literature has been informed by the multidisciplinary approach of the broad risk and crisis communication field. It focused on the question if and to what extent the existing scientific literature explains specifics regarding risk and crisis communication in terror attack situations.

The search words used to gather the articles were »crisis communication« AND CBRN, "risk communication" AND CBRN, "crisis communication" AND terror, "risk communication" AND terror. Databases included in the search are Web of Science ProQuest Dissertations and Theses - A&I, EBSCOHost, Google Scholar, WorldCat, SCOPUS, and ScienceDirect.

Following these searches, exclusion, and inclusion parameters for articles to be included in the review were set. Articles needed to be published after 2000 and before October 2023 in peer-reviewed journals and English-language publications. Additionally, articles focusing on nuclear terror attacks and radiological threats were excluded, as these issues are beyond the scope of the Joint Action Terror.

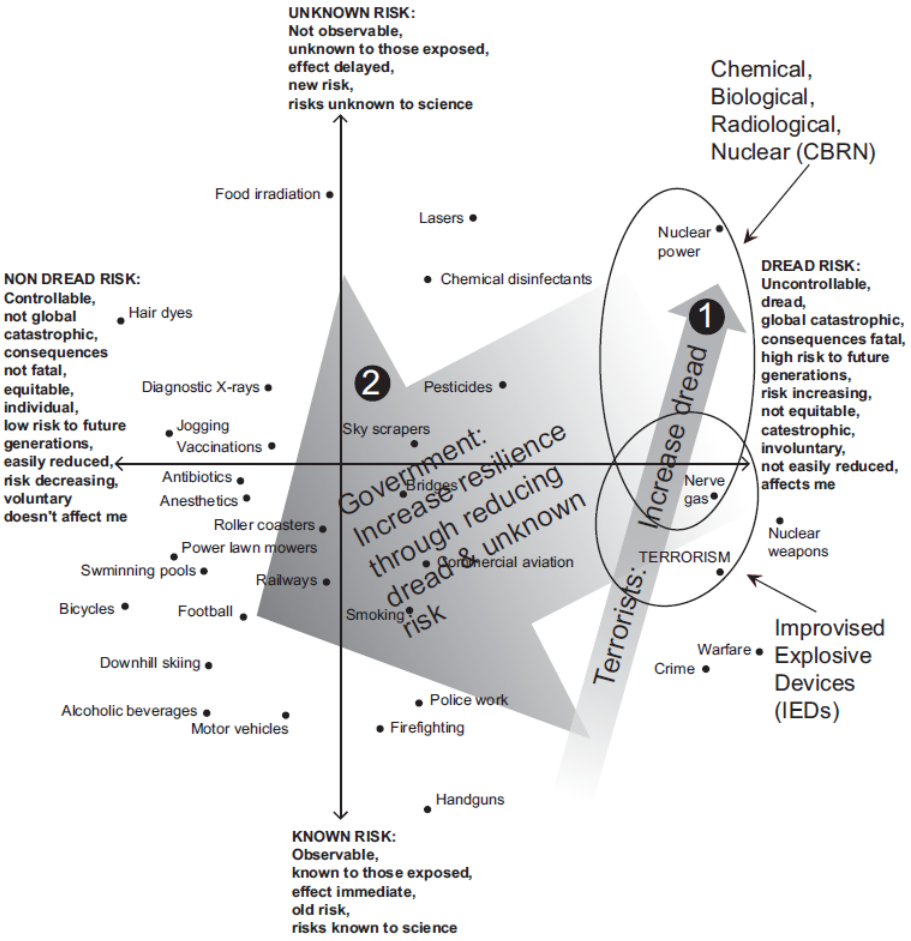
By employing these criteria, altogether 20 articles were found from which we introduce the main theoretical concepts, helpful in managing Risk and Crisis Communication. An unsurprisingly low number, mainly due to limited incidents globally, next to the fact that most of them remain "classified" information in terms of national and international safety.

Risk perception Matrix and trust

The theoretical framework employed in articles on risk communication is built on the legacy of psychometric studies, performed in the 1970s and '80s, with the most cited authors being Paul Slovic, Baruch Fischhoff and Sara Lichtenstein. Through the theoretical framework of those studies a risk perception matrix was developed, comparing different risk situations according to whether a certain risk is known and controllable. Based on their work Sheppard adapts the Risk Perception Matrix for terror situations, clearly showing the difference between terror situations and natural disasters, as well as differences in perceived risk among different terror situations (Sheppard, 2011).

[9] Proactive – Final brochure (Proactive, 2023)
[10] Public messages to use in the immediate response to a CBRN attack (Interpol)

Figure 1: Risk perception matrix and the competing influences of terror[11]



Following this matrix, Sheppard (2011) further explains people's responses in terror situations that are having harmful consequences for them. He characterizes types of behaviours as either adaptive or avoidance behaviour. Risk communication by the government should be based on observed sets of behaviours in particular situations, and thus adapted to the situation on the ground.

Rogers and others (2007) identify trust as a key issue impacting public perceptions of risk. They emphasize that: "The level of trust in an organizational body responsible for responding to the risk should be taken into account during both the policymaking and communication processes" (Rogers, Amlôt, Rubin, Wessely, & Krieger, 2007).

[11] Adapted from Paul Slovic, Baruch Fischhoff, and Sarah Lichtenstein, 'Facts and Fears: Understanding perceived risks' (pp 181-214) in Richard C. Schwing and Walter A. Albess, Jr (eds) Societal risk assessment: how safe is safe enough? Publisher: New York/ London: Plenum Press, 1980, p. 201, Figure 5

Ruggiero and Vos (2015) describe a preparedness paradox: "... *On one hand, to prepare the public to be able to act in a real situation in a timely manner and to harness public initiative to compensate for the scarcity of resources by, e.g., using self-diagnosis kits to lessen the burden on hospitals, will require a high level of public empowerment. On the other hand, lack of trust in and underestimation of the abilities of the public to act in and handle stressful situations by authorities can hamper public involvement. In addition, complicated expert knowledge and the low probability of such crises may hinder motivation for preparedness activities among the public, resulting in e.g., a lack of understanding of the risks involved...*"

Risk as feelings

Next to analysing circumstances, risk perception is also determined by cultural and individual factors. Rogers (2007) summarizes that risk has to be understood on three levels: (1) Risk as feelings: our initial, fast, intuitive reactions to perceived danger; (2) Risk as analysis: the logical, reasoned, scientific aspect of hazard management; and (3) Risk as politics: which arises when ancient instincts clash with modern scientific developments and analyses e.g. genetic cloning) (Rogers, Amlôt, Rubin, Wessely, & Krieger, 2007).

Slovic (2004) developed the concept of affect heuristic. He recognizes feelings as becoming salient in a judgment or decision-making process, depending on the characteristics of the individual and the task as well as the interaction between them. Individuals rely on experiential thinking and evoke images from the "affect pool" which determines their interpretation of events, without necessarily analytically weighing pros and cons before reaching a decision. *Using a readily available affective impression can be easier and more efficient, especially when the required judgment or decision is complex or mental resources are limited* (Slovic, Finucane, Peters, & MacGregor, 2004).

Presence is the emotional involvement in high-stakes situations like terror situations as shown by Kušen and Strembeck (2021) in their analysis of emotion exchange motifs in times of crisis.

According to them most common initial responses are *shock and fear, followed by an expression of a wider range of emotions, depending on the emotional state of those affected, their individual coping strategy, and the particularities of an event. The second phase thus exhibits a range of positive emotions such as relief, joy, and appreciation, but also sadness, disapproval, and rage towards the ones who are (supposedly) to blame*, as well as feelings of anger, which is relatively more intense during terror attacks, compared to natural disasters (Kušen & Strembeck, 2021).

Other research shows that people rate the severity of terror attacks according to casualty count, while ratings of fear and anger did not significantly depend on casualty count (Baucum & John, 2020).

Fischer-Preßler and others (2019) use Terror management theory (TMT) to explain collective sense-making in the terrorism context. According to TMT, *when terrorist attacks remind them of their vulnerability and mortality, people employ psychological defences aimed at reducing anxiety and enhancing their self-esteem by posing their worldviews (e.g., liberal values and lifestyle) against other worldviews. They accomplish this largely through interactions with others: agreement and approval from other people with the same cultural worldview (in-group) provide support for the "correctness" of one's worldview and help maintain self-esteem, whereas disagreement and disapproval reduce the psychological stability these provide.*

In particular, in the aftermath of terrorist attacks, people have been found to exhibit anxiety-reducing behaviour and worldview defense, such as through praying, searching for meaning and value, and engaging in pro-social and altruistic behaviour, but conversely also by exhibiting greater degrees of prejudice or stereotyping and showing less tolerance and greater hostility toward groups different from themselves (Fischer-Preßler, Schwemmer, & Fischbach, 2019).

Another concept arising from risk perception is optimism bias, which is important for risk communication in terror situations. Optimism bias is defined as the belief that "it won't happen to me" (Caponecchia, 2012). It is necessary to take this into account when planning risk communication before the event itself (Cooper, 2006).

Framing terror without prejudice

Media representations are a key concept in media studies that refers to how social groups (with common ethnicity, gender, age, religion, etc.) are portrayed in the media to audiences. Since anger is associated with terror events, subsequently prejudice, hostility, or calling out an "enemy" to blame is likely to follow (Kušen & Strembeck, 2021). Risk communicators have to be aware of the danger of singling out a specific social group, as this can cause further societal unrest. On the other hand, information sharing should be conducted in a transparent manner, which evokes trust in the official information sources.

Another useful concept from media studies is frames. They can be conceptualised as identifiable characteristics of mass-mediated news content. While frames may have a range of causes and effects, they exist first as words, images, and symbols that appear on paper and in other media (Woods, 2011).

Frames are indispensable tools for journalists to make sense of unfolding events, but they also constrain their perspective to most readily see what they expect to see. A study of frames used in analysis of terror events, suggests that the use of multiple threatening frames has an additive effect, increasing the dread in the audiences. As with media representations, news frames can lead to misleading interpretations of events. If set too narrowly at the start of unfolding events, new information that contradicts the dominant established frame might not effectively reach the audiences. Baden and others (2020) suggest that *their findings illuminate the important role of journalists' pre-established ideas, which shape their news selection and framing practices, contributing to the maintenance of existing news narratives* (Baden & Stalpouskaya, 2020).

4 CHALLENGES, GAPS AND CONFIDENTALITY

Identified and described challenges in this document are observed from the angle of emergency management phases. Challenges can be identified beyond the those described below but their sorting out through the emergency management cycle is to highlight and point out those that should be recognised on time and considered for appropriate timely actions. For example, "Insufficient knowledge about exciting and novel biological and chemical threats" and "Information management tool that is adapted to cross-sectorality" are crosscutting challenges throughout the whole emergency caused by a biological and chemical terrorist attack but should be considered and recognised from the preparedness phase to adequately prevent and respond to such event.

4.1 Preparedness phase

Unpredictable nature of terrorist attack

One of the main characteristics of a terrorist attack is its unpredictable emergency scenario that hampers first responders to be fully prepared for prompt actions based on precalculated risks. In terrorist attacks, there are many uncertainties and unclear information such as the precise number of terrorist and their location, the number of people in the affected area, the type of attack, and the biological and/or chemical agents, etc (Gaibulloev & Sandler, 2009), (Masood, et al., 2020).

Insufficient knowledge about existing and novel biological and chemical threats

There is evidence of limited understanding by the public of existing and novel biological and chemical threats used in terrorist attacks, related to their characteristics, differences between them, and protective measures. Additionally, it is noticed that the level of interest in knowledge about these threats differs between urban and rural populations, where in rural areas people are less concerned about being targeted in terrorist attacks (Wray, et al., 2008)[12]. While the general population mostly wants to know how to protect itself from hazardous agents, experts in the field and public health professionals are challenged with insufficient inter-institutional and inter-sectoral communication, including the exchange of information in a more systematic way and regular[13].

WP8 of JA TERROR has focused on this particular topic and produced guidelines accordingly.

[12] STAMINA- Demonstration of intelligence decision support for pandemic crisis prediction and management within and across European borders. D5.2 – Guidelines on risk communication principles implementation.
[13] National Research Council (US) Committee on Risk Perception and Communication. Improving Risk Communication. Washington (DC): National Academies Press (US); 1989. 6, Problems of Risk Communication.

Uncoordinated and separate sectoral risk communication planning

Risk communication planning with simulation exercises in the preparedness phase are of crucial importance to coordinate communication response during public health emergencies. It requires synergies and effective coordination between relevant institutions and sectors that is typically lacking in practice (Gooding, Bertone, & Witter, 2022). If a communication plan is developed in effective coordination between sectors and institutions, bureaucratic procedures for its implementation could be challenging, especially for chemical hazards (Barbour, Bierling, Sommer, & Trefz, 2020). For more information regarding cross-sectoral collaboration, you can also refer to the deliverables of JA TERROR WP6.

Knowledge gap of needs and capabilities for risk communication

Appropriate preparedness for efficient and effective risk communication in biological and chemical terrorist attacks requires fulfilling certain preconditions and securing capacities and capabilities for its unfolding according to needs assessment. It considers checking whether all capacity elements exist such as a coordinated risk communication operational plan for the public, media, and different stakeholders with well and detailed defined responsibilities and procedures; adequate space, equipment, and personnel to handle public information 24/7 a week; techniques for information sharing and dissemination to the various recipients; channels of communication with identified mechanisms for communication with multiple audiences, using various communication channels[14].

Insufficient stakeholders' engagement in risk communication planning

One of the identified challenges in strengthening capacity for and building community resilience in bio-chem terrorist attacks is the weak involvement of different stakeholders with diverse expertise and responsibilities at the local level in building risk communication planning and response network prior to an attack (Smith, Shapiro, & Callaway, 2024). Missing networking of institutions and organizations that have formal and direct (governmental institutions, environmental and public health agencies, security sector, etc) or indirect roles (NGOs, schools, industry, entrepreneurs) in incidents at the local level discourages the whole community approach and building risk communication infrastructure that could help in better understanding and aligning different stakeholders risk perception and relevance of incidents for particular stakeholders' groups.

An information management tool that is adapted to cross-sectorality

In the era of rapid development of Information Technologies, there are increasing demands for creating and using information management tools and cross-sectoral digital platforms to facilitate and intensify crisis communication exchange of data, information, and knowledge between sectors and institutions, both in- and between countries (Gamidullaeva, Tolstykh, Bystrov, Radaykin, & Shmeleva, 2021). Currently, cross-sectoral communication, especially in crises is a challenge and is very often based on personal contacts and professional connections.

[14] Centers for Disease Control and Prevention. Crisis emergency risk communication. 2014 edition. Be first. Be right. Be credible.

4.2 Emergency response phase

Risk perception of the community

Risk perception is subjective and based on the individual, group, or society estimation related to the negative consequences of hazardous events. No matter how objective conditions are, it is shown that behaviour is significantly influenced by risk perception. Various factors could affect the risk perception such as type of danger, personal trait, religion, culture, tradition, social values, internet access and use, etc (Al-Dahash, Kulatunga, & Allali, 2022), (Xu, Shangguan, & Xia, 2023).

Policy gap on information flow and transparency in information sharing between sectors

Risk communication in a policy context may face problems if all key elements of the emergency response phase are not covered by regulations. Thomas, Kaufman, Klemm, & Hutchins (2023) showed that government communication efforts in response to chemical and threats came with unsatisfactory results observed by the public, due to inadequate practice and not meeting the needs of the affected communities. Several reasons, such as different perspectives, ways of communication, and interests, explain why communication experts from different institutions/sectors find themselves in controversy (Poorvliet, Duineveld, & Purnhagen, 2016). Additionally, there might a policy gap in regulating information exchange, reporting, and flow between sectors and different institutions during emergency management, especially during response. Consequently, a lack of data and information on a particular bio-chemical attack affects accurate risk analysis and decision-making (Barr, Burtner, Pike, Peddicord, & Minsk, 2010).

Decreased trust in institutions

A failure in the communication process (insufficiently accurate and fast information, confusion) can lead to a decreased trust in important institutions (Burger, 2022). Reasons for decreased trust in institutions can vary from situation to situation (Abraham, 2011). Distrust of the public in institutions may be due to failure to admit mistakes when insufficiently verified information is shared when there is little evidence of potential hazard leading to insufficient understanding of risk, which promotes the spread of speculative opinions/rumours (Lok & Powell, 2000). Also, the public will be suspicious of institutional experts who are responsible for communication in an emergency, unless they are persons who have high credibility and enjoy a high level of trust. Trust in institutions can also be lost if risk communicators (from government or industry) do not consider and respect the public's perception of overexposure to chemical hazards from the air (Burger, 2022). Institutions that lose trust and credibility during a crisis have a very hard time regaining it later, and public mistrust can persist for a long period (Dedmon, 1996). The literature describes many factors that influence trust, such as competence, proposed knowledge and expertise, objectivity, efficiency, transparency, consistency, fairness (Burger, 2022; Boholm, 2019).

Overcommunication and disinformation

People can absorb only a limited amount of information so communication experts must identify the most critical facts and organize them according to the mindset of their audience (Bouder, 2022). Ineffective communication in crises can lead to other speculative and opposing viewpoints and opinions receiving greater media coverage. In recent times, the public is increasingly receiving and sharing news through online sources and social media, which leads to the rapid spread of misinformation about risks and this is becoming a major problem for societies around the world (Hansson, et al., 2020; Roozenbeek & van der Linden, 2019), while at the same time leaves a lot of space for targeted disinformation campaigns to interfere. (e.g. extensive anti-vaccination campaigns through social media)

Political intrusion in risk communication management

In risk communication management during complex crises that could be caused by terrorist attacks, political leadership is highly important to increase public adherence to collective action. It was highly expressed during COVID-19 pandemic around the globe, when political leaders jointly with public health professionals were advising the public to strictly stick to the anti-epidemic measures, including restrictions on movement in and outside the country (Van Bavel, et al., 2020; Grossman, Kim, Rexer, & Thirumurthy, 2020). Communication during disease outbreaks is very often under the pressure of political and economic influences, so that clear and transparent transmission of information can be hindered and thus gaining public trust is reduced[16].There were positive (engaging and nonaggressive) and negative (rude language and making use of fear) examples of political communication via mainstream and social media that influenced either in encouraging or discouraging way the public behaviours and adherence to the public health preventive measures (Liu, Mirkovski, Lowry, & Vu, 2023).

Classification of information

With threats of terrorist attacks of various types being a global reality and beyond solid forecast, national legislations in EU countries are challenged with the need on one side to ensure national security and on the other to give citizens the right to be informed. Classification of information should be comprehensively and clearly defined by the legal acts related to both dimensions, demands for the freedom of information, and application of norms on safeguarding of classified information or on restrictions to information. This is a very complex matter, and the public is not well trained on how to deal with classified information and on how to follow up the process of its authorisation. Information management systems often lack regular evaluation of the classification, detailed statistics, analysis, and reporting on classification and declassification that are standardised.[15]

[15] Classified Information: A review of current legislation across 15 countries & the EU.

4.3 Recovery phase

Updating of the existing protocols/plans

Confusion and ineffectiveness of crisis communication during emergencies due to failure to establish clear communication protocols and strategies continue during the recovery phase if mistakes are not recognized and those plans/strategies are not improved (Marcillo-Delgado, Alvarez-Garcia, & García-Carrillo, 2022)[16]. There is a lack of information on the evaluation of the communication plan and its effectiveness.

Lack of information on access to services dealing with the mental health of the population

Many studies have shown and confirmed that emergencies lead to increased stress and trauma in the population (Makwana, 2019)[17]. Many individuals and communities, especially people with disabilities and other vulnerable groups (Ahmad & Vismara, 2021), may have problems and encounter obstacles in accessing information on how to help themselves overcome stress and anxiety after a crisis. Experiences have shown that there is insufficient integration of psychosocial care into disaster response, as well as insufficient cooperation and collaboration between medical and mental health care providers (Ruzek, Young, Cordova, & Flynn, 2004). Often governments overlook the need for launching key messages about the importance of mental health in recovery and do not include information about access to relevant services that could provide this support and group education to the general population.

Loss of interest in time

Studies have shown a decrease in the volume of communication during the post-disaster recovery phase (Yeo, Knox, & Hu, 2022). After an emergency, people may have problems with the memory of an event and lose interest over time, so it is necessary to periodically repeat and transfer information during the recovery phase. Much information on websites regularly updated during response is not any more frequently refreshed in the recovery phase, which also contributes to the loss of interest in the community (Momenipour, Rojas-Murillo, Murphy, Pennathur, & Pennathur, 2021). Also, community leaders do not receive the updated necessary information from the government that they need to provide their communities with reliable information about the post-disaster recovery process.

[16] World Bank. (2020). Communication during Disaster Recovery.
[17] World Health Organization. (2022). Mental health and COVID-19: early evidence of the pandemic's impact: scientific brief, 2 March 2022 (No. WHO/2019-nCoV/Sci_Brief/Mental_health/2022.1). World Health Organization.

5 RISK ESCALATION

5.1 Definition and Basic Principles

Risk escalation is a risk response strategy that involves transferring the ownership and accountability of a risk to a higher Authority. It is usually applied when the risk exceeds the tolerance or capacity of an operational team[18].

Risk escalation is the process of informing and involving relevant Sectors who have the authority and responsibility to mitigate a risk that exceeds the capacity of a single Operational team[19],[20].

- Risk escalation can be proactive or reactive, depending on whether the risk is anticipated or realized.
- Risk escalation can also be formal or informal, depending on the communication channels and protocols used, though formal communication channels should be preferred when possible.
- Risk escalation strategies can also help avoid conflicts, confusion, or delays in risk management, as well as increase transparency and accountability.

Risk escalation is important because it helps to ensure that risks are addressed promptly and adequately by the relevant Sectors. By escalating risks, you can leverage the expertise, resources, or influence of higher Authorities, to respond, assess, analyse, prepare against, and mitigate risk (Hillson, 2016) [21].

It is important to escalate a risk when it surpasses predefined thresholds or criteria, such as probability, impact, urgency, or complexity 2. Additionally, if a decision or action is beyond your authority or capacity or involves changing the Plan, you should escalate the risk (Ferdosi, Rezayatmand, & Molavi Taleghani, 2020; Hillson, 2016)[22].

Moreover, if the risk affects higher Authorities, interests, responsibilities, capacity, or objectives, it should be escalated.

[18] CBRNE National Plan of Greece, Civil Protection and Relevant Sectors, 2019
[19] CBRNE National Plan of Greece, Civil Protection and Relevant Sectors, 2019
[20] Kennedy Inst Ethics J. 2014 Jun; 24(2): 121–139.
[21] Kennedy Inst Ethics J. 2014 Jun; 24(2): 121–139.
[22] CBRNE National Plan of Greece, Civil Protection and Relevant Sectors, 2019

Escalating a risk requires exact identification of all relevant Sectors that need to be informed, based on their role description under existing preparedness plans (Ferdosi, Rezayatmand, & Molavi Taleghani, 2020; Hillson, 2016)[23].

It is important to communicate the risk escalation report on time, using the agreed communication channels and protocols. Furthermore, it is necessary to follow up and monitor the progress and outcome of the risk escalation and provide feedback and updates to Operational teams and other relevant stakeholders (Ferdosi, Rezayatmand, & Molavi Taleghani, 2020),[24].
It is essential to escalate risks as early as possible while the appropriate criteria are met, making sure not to over-escalate or under-escalate risks as this may damage credibility or create confusion. It's also important to escalate risks constructively and collaboratively while building trust and rapport with those involved. Lastly, it is essential to escalate risks consistently and transparently while documenting and recording the process and outcome as well as the lessons learned (Ferdosi, Rezayatmand, & Molavi Taleghani, 2020),[25].

Define Criteria

Firstly, make sure that clear criteria for escalating risks are well established, such as impact, probability, urgency, or severity of the risk. These criteria should be aligned with the scope, goals, and priorities documented in a risk management plan. Having clear escalation criteria will help the Operational Team avoid over-reporting or under-reporting risks and ensure communication and sharing of the rightly identified risks to the right people at the right time (Hillson, 2016).

Assess Triggers

After the definition of the escalation criteria, there is also the need to monitor and assess the risks constantly and identify any trigger that could indicate the need for escalation. A trigger could be a change in the risk's status, a new risk emerging, a risk exceeding a threshold or a risk affecting a critical operational path (Ferdosi, Rezayatmand, & Molavi Taleghani, 2020),[26].

Prepare Reports

During the escalation procedure, it is also very useful for all relevant Sectors to prepare a concise and constructive report that summarizes key information on the risk, its impact, its causes, its mitigation actions, and possible recommendations. The use of a specific template for escalation reports is desirable, which should incorporate data, evidence, and visuals to develop the analysis (Hillson, 2016)[27].

[23] CBRNE National Plan of Greece, Civil Protection and Relevant Sectors, 2019
[24] WHO Risk Management Strategy. Reducing uncertainty around the achievement of WHO's objectives and outcomes, 3 May 2023.
[25] Bioterrorism Incident. Pre-Planning & Response Guide. 2nd Edition -2010, Interpol
[26] WHO Risk Management Strategy. Reducing uncertainty around the achievement of WHO's objectives and outcomes, 3 May 2023.
[27] Kennedy Inst Ethics J. 2014 Jun; 24(2): 121–139.

Communicate messages

The procedure followed to communicate escalation messages to incident managers is crucial for maintaining a positive and collaborative relationship. It is important to follow appropriate channels to share the key messages and incorporate them into the expectations and preferences of relevant Stakeholders. Be proactive, and transparent as the event unfolds and avoid criticizing others[28],[29].

Follow up

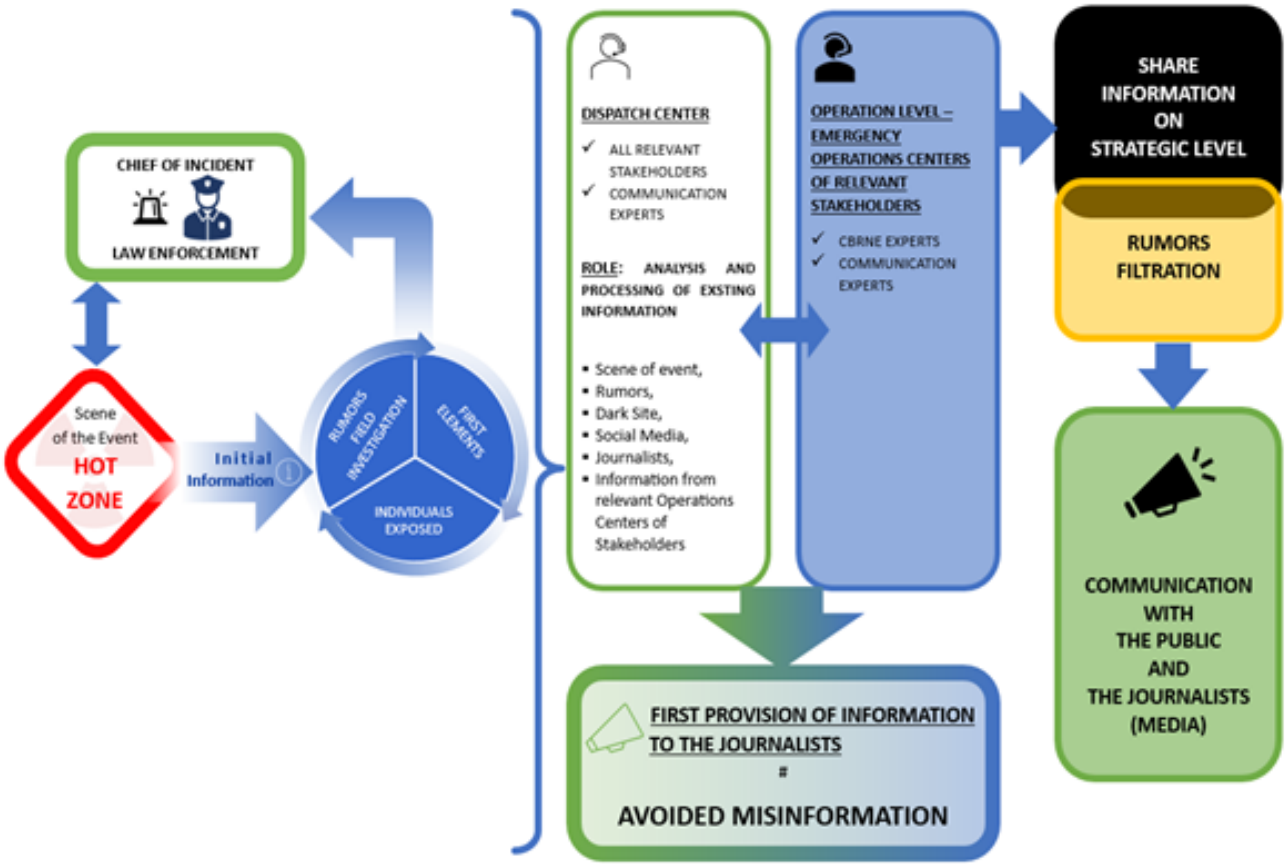
After an escalation procedure, it is a necessity to follow up on the actions that were agreed upon and report on the progress and outcomes. Senior Stakeholders should be informed of any changes or issues that arise and provide feedback and support if needed. Update regularly the risk register with new information and de-escalate the risk if it is resolved or no longer relevant (Hillson, 2016),[30].

Lessons Learned

Risk escalation experiences provide an opportunity to learn and improve risk management skills and practices. The management team should evaluate the effectiveness and efficiency of escalation processes, identify any gaps, and challenges as well as identify best practices. It's very important to solicit and incorporate any feedback from incident managers and acknowledge achievements[31],[32].

[28] WHO Risk Management Strategy. Reducing uncertainty around the achievement of WHO's objectives and outcomes, 3 May 2023.
[29] Bioterrorism Incident. Pre-Planning & Response Guide. 2nd Edition -2010, Interpol
[30] WHO Risk Management Strategy. Reducing uncertainty around the achievement of WHO's objectives and outcomes, 3 May 2023.
[31] WHO Risk Management Strategy. Reducing uncertainty around the achievement of WHO's objectives and outcomes, 3 May 2023.
[32] Bioterrorism Incident. Pre-Planning & Response Guide. 2nd Edition -2010, Interpol

5.2 Escalation algorithm



The table depicts the flow of information among relevant stakeholders via the decisions and steps taken when managing an ongoing incident.

Namely, how the main messages get analyzed at operational and strategic level and end up to get diffused to the public, avoiding misinformation.

5.3 Risk Score

RISK SCORE (severity)	RECOMMENDED ACTION
Extreme	Immediate action required.
High	High priority action required.
Moderate	Develop procedures to manage risk.
Low	Risk monitoring: Check risk causes, develop Contigency Plans

Reading the table:

- ***Green:*** *acceptable risk / minor risk where no further action or additional controls are required except monitoring locally within Directorates and local government*
- ***Yellow****: unacceptable / major risk where control measures should be put in place which will have the effect of reducing the impact of an event or the likelihood of an event occurring. Immediate action must be taken to manage the risk and entered on the Directorate Risk Register*
- ***Brown – Red:*** *unacceptable high risk: control measures should be put in place which we'll have the effect of reducing the impact of an event or the likelihood of an event occurring. A number of control measures may be required. Where the risk involves work in progress, urgent action should be undertaken.*

The above risk score interpretations and corresponding actions refer to the basic principles of all three major pillars of Preparedness and Response in order to address a major event: Risk assessment, risk management and risk communication.

6 CASE STUDIES

The management of CBRN terrorist incidents, with a specific focus on the preparedness for risk and crisis communication, is greatly aided by the fortunately limited number of examples that have emerged in various parts of the world. This chapter will present the Tokyo sarin gas attack (chemical), the anthrax attacks in New York following 9/11 (biological), and the case of polonium poisoning in London (radiological).

6.1 The Tokyo subway sarin attack

The Tokyo sarin attack, carried out by followers of the Aum Shinrikyo cult, occurred on March 20, 1995. The perpetrators deployed the nerve gas in the Tokyo subway system during the morning rush hour.

Members of the cult punctured plastic bags containing sarin with the tips of their umbrellas, releasing the gas in several subway cars. The attack resulted in the deaths of 13 people and injured over a thousand others. The attack demonstrated the consequences of inadequate communication with the public and response partners during a large-scale chemical incident. [33]

[33] Key Planning Factors and Considerations for Response to and Recovery from a Chemical Incident, (FEMA, 2022)

Delay in Reporting and Coordinating Actions

One major issue was the delay in reporting the critical problem and coordinating actions among civilians, transit authorities, and first responders. Despite individuals becoming aware of the crit-ical issue, there was a slow response in reporting it and taking coordinated actions.

Inadequate Communication within the Subway System

The communication within the Tokyo subway system was insufficient. Although the subway train control center was notified of the critical issue, there was a failure to halt the trains immediately. As a result, trains continued on their scheduled routes, leading to the contamination of multiple train lines, stations, and hundreds of people.

Lack of Information Delivery to Public

The absence of immediate and clear/precise information delivery to the public led to medical facilities being overwhelmed with patients, including those at little to no risk of illness.

Crippled Medical System Communications

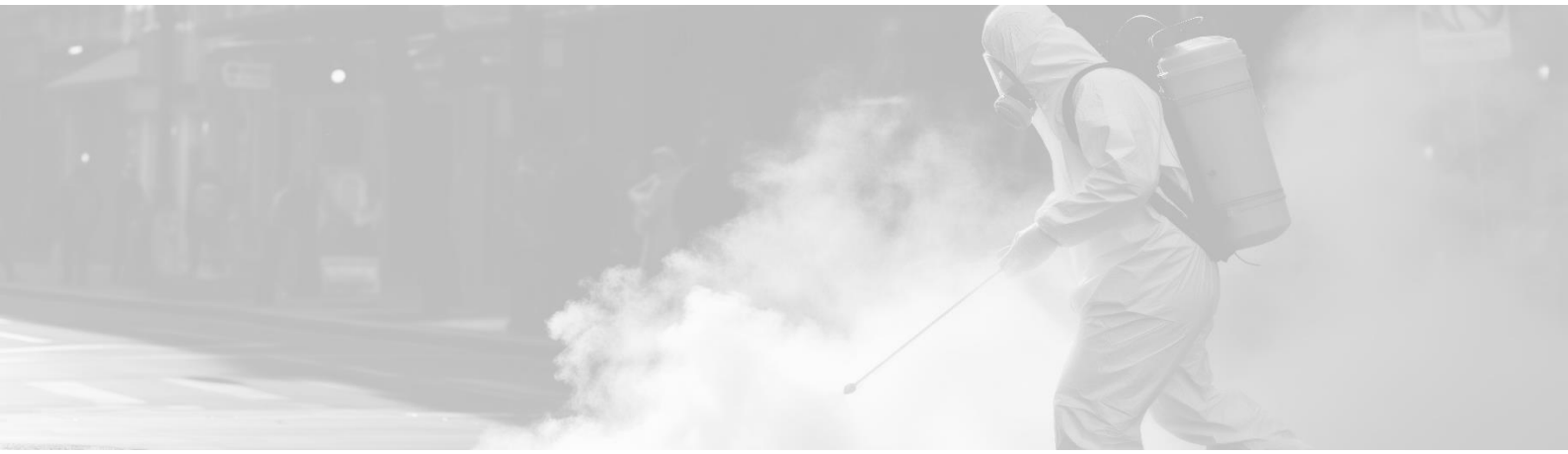
The sarin attack severely affected the medical system's communication. The sheer number of rescue vehicles activated clogged regular communication channels, and ambulance crews strug-gled to communicate with the dispatch center to determine which hospitals could receive pa-tients. This communication breakdown hindered effective emergency medical response.

Lack of Information Delivery to Hospitals

Essential incident information was not delivered promptly to Tokyo hospitals. Doctors at hospi-tals near the affected subway stations reported receiving no information from city fire or police departments about the nature of the incident. The absence of immediate and clear information delivery forced hospitals to rely on television news reports for details, contributing to delays in appropriate medical treatment.

The attack highlighted the importance of pre-planning and the need to pre-identify and link a range of experts that responses to certain situations might demand. Effective communication between experts and responding partners, especially during a chemical incident, was emphasized as critical for the dissemination of potentially life-saving information.

6.2 The anthrax attacks in New York City



In the week following 9/11, letters containing anthrax spores were delivered to several news media offices and two Senators in the USA. As a result of the attack, 5 individuals died, and an additional 17 people were infected.

The anthrax attacks in the United States in 2001 revealed several gaps in risk communication. Public uneasiness and fear were very apparent in the weeks following the announcement of the first anthrax case. This was seen in the run on antibiotics that took place, particularly in Florida and New York City, a phenomenon that one Florida pharmacist described as "semi-educated panic".[34]

[34] Working Paper. Anthrax In America: A Chronology and Analysis of the Fall 2001 Attacks. Center for Counterproliferation Research, National Defense University, 2002)

Initial Lack of Information and Uncertainty

In the early stages of the anthrax attacks, there was a lack of clear and accurate information regarding the source, extent, and nature of the anthrax contamination. The uncertainty surrounding the attacks contributed to public anxiety and confusion.

Delay in Public Warnings

There were delays in providing timely and comprehensive public warnings about the potential risk of anthrax exposure. As a result, individuals who may have been exposed to anthrax were not promptly informed, leading to increased health risks.

Challenges in Coordinating Communication Between Agencies

The anthrax attacks involved multiple government agencies, including public health, law enforcement, and homeland security entities. Coordinating communication between these agencies proved challenging, leading to inconsistencies and delays in conveying critical information to the public.

Limited Guidance for Exposed Individuals

Individuals who may have been exposed to anthrax did not receive immediate and clear guidance on what steps to take, such as seeking medical attention or taking preventive measures. Specific groups that were affected by the attack (postal workers) argued that the quality of care and attention they received was inadequate compared to that given to other affected groups, in particular congressional staff. With regard to information concerning the risks from exposure to anthrax spores and medical treatment options, postal workers routinely opined that the information they received from federal and public health authorities was incomplete, inaccurate or contradictory. This response argues for the creation of targeted communication strategies to deal more effectively with the concerns of affected groups as part of future responses.

Communication Gaps with Healthcare Professionals

Communication gaps existed between public health authorities and healthcare professionals, leading to challenges in disseminating accurate information to medical practitioners who play a crucial role in identifying and treating anthrax cases.

Media Handling and Sensationalism

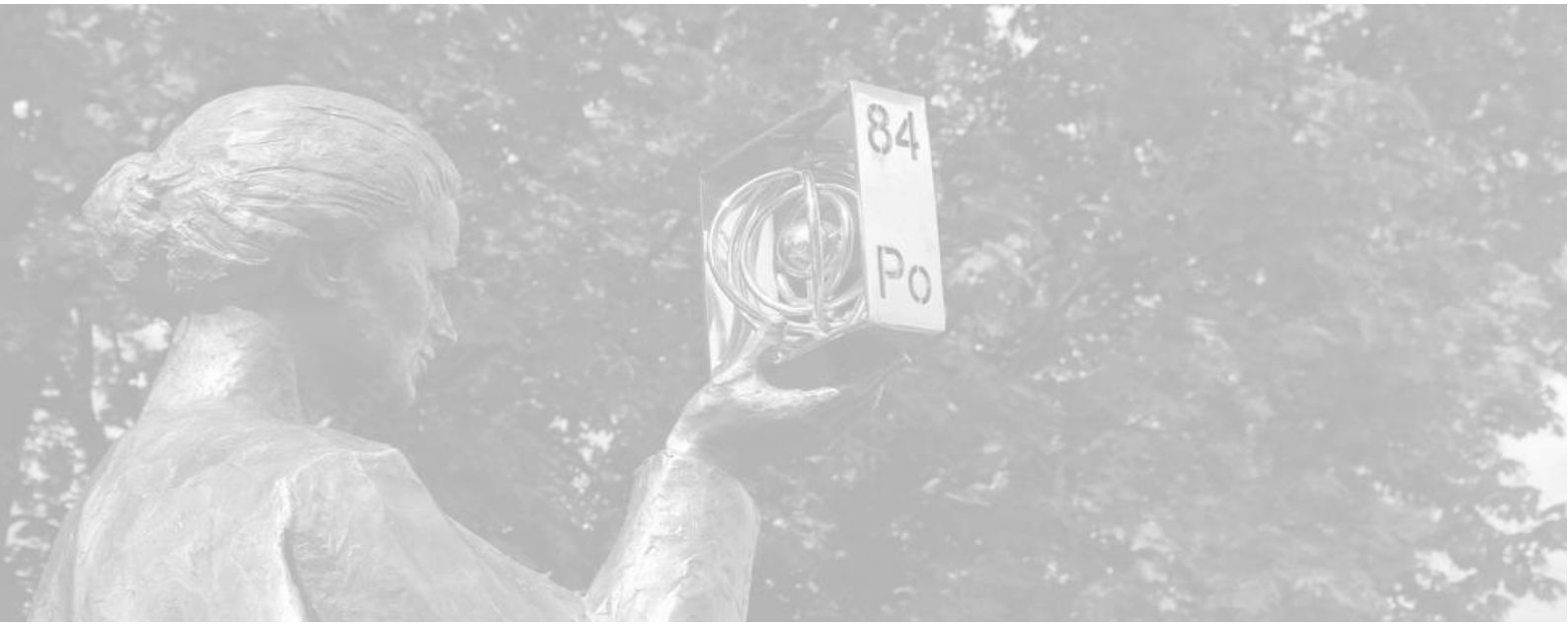
The media's coverage of the anthrax attacks contributed to unnecessary panic and sensationalism. This could have been mitigated through more transparent communication strategies and collaboration between public health officials and the media.

Limited Public Education on Anthrax

There was a lack of sufficient public education on anthrax, including information about its symptoms, transmission, and appropriate preventive measures. Educating the public about anthrax could have helped alleviate fears and reduce the risk of exposure.

Addressing these gaps requires a comprehensive approach, including improved coordination between government agencies, clear and consistent messaging, proactive public education campaigns, and effective collaboration with the media. Learning from the challenges faced during the anthrax attacks can help enhance future risk communication strategies in biosecurity incidents.

6.3 The London polonium-210 poisoning



In November 2006, Alexander Litvinenko, a former Russian intelligence officer, fell seriously ill and was hospitalized. It was later determined that he had ingested a lethal dose of the radioactive isotope polonium-210.

The investigation into Litvinenko's death led to the conclusion that he was poisoned by two Russian agents, Andrei Lugovoi and Dmitry Kovtun. Litvinenko ingested the polonium when he met with the

two men for tea at the Millennium Hotel in London. The use of a rare and highly toxic substance like polonium raised concerns about nuclear terrorism and led to diplomatic tensions between the United Kingdom and Russia.

The incident prompted a significant investigation and inquiries, highlighting the challenges associated with investigating and prosecuting cases involving radioactive materials. The findings of the investigation were published in the Litvinenko Inquiry report, which detailed the events leading to Litvinenko's death. [35]

The primary responsibility for managing and communicating public health risk fell to the Health Protection Agency (HPA), which had been established in 2003 to bring together skills and knowledge in infectious diseases, chemical and radiation hazards, and emergency response. The HPA had emergency plans, but no 'polonium plan', so there were many gaps in crisis communication (Troop & Dittner, 2010).

Coordination Among Authorities

Coordination among various authorities, including law enforcement, public health agencies, and diplomatic channels, was crucial. Gaps in coordination hindered a cohesive and transparent communication strategy.

Delay in Information Release

There was a notable delay in releasing information to the public about the poisoning. Litvinenko fell ill in November 2006, but it took several days for authorities to confirm that he had been poisoned with polonium-210. During this time, there was uncertainty and speculation in the media, leading to public anxiety

Unclear Risk Communication

The authorities' communication about the potential health risks associated with the nature of the polonium and the extent of the risk to the public was not always consistent. Media speculation and sensationalism increased uncertainty and contributed to heightened public concern. Better coordination with the media and providing accurate information could have mitigated unnecessary panic.

[35] The Litvinenko Inquiry, Report into the death of Alexander Litvinenko, Chairman: Sir Robert Owen, January 2016.

Handling of Public Concerns

The incident raised public concerns about the safety of public spaces, especially places that Litvinenko had visited before his illness. More proactive communication was needed to reduce these concerns.

International Communication Challenges

The incident had international implications, involving diplomatic tensions between the United Kingdom and Russia. Effective communication between the two countries was essential, but there were challenges in coordinating and sharing information transparently.

Communication with Healthcare Professionals

There were challenges in effectively communicating with healthcare professionals, particularly those involved in treating Litvinenko. Ensuring that medical staff had accurate information about polonium, its symptoms, and the appropriate medical responses was crucial for patient care.

A cross-sectional telephone survey and qualitative analysis (Rubin, et al., 2007) (1000 people completed the cross- sectional survey, and 86 potentially exposed people completed the qualitative interviews) conducted on the subject indicated that clarifying the fact that the case is related to espionage and thus the risk of the polonium incident to individual health is low had a reassuring effect on the public. However, they expressed a need for more information regarding the individual risk of exposure and its health effects.

These gaps in crisis communication during the polonium incident highlight the importance of transparency, clear messaging, and effective coordination among authorities during public health crises with international implications.

6.4 The Salisbury incident

On March 4, 2018, ex-Russian intelligence officer Sergei Skripal and his daughter were found ill on a bench in the British city Salisbury. They turned out to being exposed for the nerve agent Novichok, together with a police officer and after some time two more people who got exposed and poisoned by handling the agent from a litter bin. One of them died from poisoning. The Government described the incident as an attempted assassination.

The communication towards the public was generally considered appropriate given the circumstances.

Regular updates

Authorities, including public health officials and law enforcement agencies, provided regular updates to the public regarding the investigation, the nature of the nerve agent used (Novichok), and safety precautions.

Precautions were provided

Efforts were also made to reassure the public, provide accurate information, and advise on any necessary precautions, such as avoiding areas where the poison was found and following hygiene guidelines.

Transparency

Additionally, there was transparency about the ongoing investigation and efforts to identify and hold accountable those responsible for the attack. While there was certainly concern and apprehension among the public, widespread panic was largely avoided.

The Salisbury incident demonstrates that preparedness, swift response, and transparency are crucial for successful risk management, especially in a complex situation such as the use of chemical weapons.

7 CONCLUSIONS

This "Risk and Crisis Communication Guidance Toolkit" provides a comprehensive framework aimed at planning to enhance the effectiveness of communication during biological and chemical terrorist attacks. In summary, it highlights the critical role of risk and crisis communication as an integral element of national security strategies. Effective communication is presented not merely as a tool for information dissemination, but as a strategic function that can significantly mitigate the psychological and social effects of terrorism.

The guidance tool presented draws from already existing basic principles, originating from existing guidelines that we think should be paramount for all risk and crisis communication. These principles focus mainly on the need for rapid and timely communication, openness and transparency, and the implementation of risk communication as an interactive process between decision-makers, experts, and the public. The guidance tool is evidence-based as it based on best practices and and after-action reviews from the COVID-19 pandemic. The Guidelines used as background are from, in addition to the guidelines from the WHO, the European Centre for Disease Prevention and Control (ECDC), Centres for Disease Control and Prevention (CDC), the European Food Safety Authority (EFSA), and Interpol (see also chapter 3.3).

Communication during a crisis needs to be well coordinated and strategically planned during the various phases of emergency management, initially in preparedness, emergency response and the subsequent recovery phase. During the preparedness phase, the emphasis is on establishing a strong communications infrastructure, training spokespersons and creating clear communication channels between government agencies, emergency responders and the public. This phase involves both crafting messages that can be readily adapted to a variety of scenarios and, of course, ensuring that these messages are based on transparency and credibility to - crucially - build public trust in agencies and representatives before a crisis occurs.

In the emergency response phase, the need to provide timely, accurate and clear information to the public is underlined. The effectiveness of this depends on the ability to convey complex messages and information that may be frightening to the public, which should be provided in a way that is both understandable and achievable.

The importance of empathy, recognising the public's fears and providing guidance to help people make evidence-based decisions during a crisis is stressed and the role of the media as a systematic partner in ensuring that the public receives consistent and reliable information is highlighted.

Finally, in the recovery phase, the emphasis is on maintaining public trust and rebuilding social resilience and cohesion. Communication efforts during this phase should aim at providing continuous updates, combating misinformation and providing psychological support to the public to help them process the crisis and return to normality. This chapter concludes that the effectiveness of communication in the recovery phase can have a significant impact on public perception and resilience to future crises.

In summary, it is useful to understand that risk and crisis communication should be seen as a continuous process that is adjusted by phases during a crisis. A preventive approach is essential for its success, while communication strategies should not only remain at this stage but also at a level of response to the X stimulus, making them demanding and complex in order to cope with multiple scenarios. The complexity of this communication lies not only in the complexity of the planning as such but precisely in the coordination of multiple levels and representatives from governmental levels to partner agencies, civil society representatives, the media, so that the messages are consistent and reliable.

In conclusion, in cases of interest, that is the deliberate release of biological and chemical agents towards a terrorist attack, risk and crisis communication is vital for building social resilience, managing the consequences, limiting the 'damage' but also the later phase of maintaining public trust by ensuring transparency making this process more than just managing information flow.

8 REFERENCES

Abraham, T. (2011). Lessons from the pandemic: The need for new tools for risk and out-break communication. Emerging Health Threats Journal.

Ahmad, M., & Vismara, L. (2021). The psychological impact of COVID-19 pandemic on women's mental health during pregnancy: A rapid evidence review. International Journal of Environmental Research and Public Health, 18(7), 7112. https://doi.org/10.3390/ijerph18077112

Al-Dahash, H., Kulatunga, U., & Allali, B. (2022). Factors affecting risk perception during terrorist attacks. International Journal of Disaster Risk Reduction, 80, 103114. https://doi.org/10.1016/j.ijdrr.2022.103114

Backholm, K., Högväg, J., Knutsen, J., Lindholm, J., & Westvang, E. (2018). Tailoring tools to the rescue: Lessons learned from developing a social media information gathering tool. In S. Hornmoen & K. Backholm (Eds.), Social media use in crisis and risk communica-tion (pp. 185-203). Emerald Publishing. https://doi.org/10.1108/978-1-78756-269-120181013

Baden, C., & Stalpouskaya, K. (2020). Maintenance of news frames: How US, British, and Russian news made sense of unfolding events in the Syrian chemical weapons crisis. Journal-ism Studies, 21(16), 2305-2325. https://doi.org/10.1080/1461670X.2020.1813352

Barbour, J., Bierling, D., Sommer, P., & Trefz, B. (2020). Risk communication infrastruc-ture and community resilience: Does involvement in planning build cross-sector planning and response networks? Journal of Applied Communication Research, 48(1), 91-113. https://doi.org/10.1080/00909882.2019.1704825

Barr, J., Burtner, E., Pike, W., Peddicord, A., & Minsk, B. (2010). Gap assessment in the emergency response community. Pacific Northwest Lab.

Baucum, M., & John, R. (2020). The psychophysics of terror attack casualty counts. Risk Analysis, 40(2), 399-407. https://doi.org/10.1111/risa.13396

Boholm, Å. (2019). Risk communication as government agency organizational practice. Risk Analysis, 39(8), 1695-1707. https://doi.org/10.1111/risa.13312

Bouder, F. (2022). Principles and challenges of risk communication/crisis communication spe-cifically addressing issues relating to pandemics. Underlagsrapport till SOU.

Burger, J. (2022). Trust and consequences: Role of community science, perceptions, values, and environmental justice in risk communication. Risk Analysis, 42(12), 2362-2375. https://doi.org/10.1111/risa.13929

Caponecchia, C. (2012). Relative risk perception for terrorism: Implications for preparedness and risk communication. Risk Analysis, 32(9), 1524-1534. https://doi.org/10.1111/j.1539-6924.2011.01759.x

Cooper, M. (2006). Pre-empting emergence. Theory, Culture & Society, 23(4), 113-135. https://doi.org/10.1177/0263276406065125

Dedmon, J. (1996). Thinking the unthinkable—Crisis communications. In M. Hopkins (Ed.), Dartnell's Public Relations Handbook (pp. 207-224). The Dartnell Corporation.

Ferdosi, M., Rezayatmand, R., & Molavi Taleghani, Y. (2020). Risk management in execu-tive levels of healthcare organizations: Insights from a scoping review (2018). Risk Manage-ment and Healthcare Policy, 13, 215-243. https://doi.org/10.2147/RMHP.S245546

Fischer-Preßler, D., Schwemmer, C., & Fischbach, K. (2019). Collective sense-making in times of crisis: Connecting terror management theory with Twitter user reactions to the Berlin terrorist attack. Computers in Human Behavior, 100, 138-151. https://doi.org/10.1016/j.chb.2018.04.032

Gaibulloev, K., & Sandler, T. (2009). Hostage-taking: Determinants of terrorist logistical and negotiation success. Journal of Peace Research, 46(6), 739-756. https://doi.org/10.1177/0022343309342338

Gooding, K., Bertone, M. L., & Witter, S. (2022). How can we strengthen partnership and coordination for health system emergency preparedness and response? Findings from a syn-thesis of experience across countries facing shocks. BMC Health Services Research, 22(1), 1-19. https://doi.org/10.1186/s12913-022-08300-0

Grossman, G., Kim, S., Rexer, J., & Thirumurthy, H. (2020). Political partisanship influ-ences behavioral responses to governors' recommendations for COVID-19 prevention in the United States. Proceedings of the National Academy of Sciences, 117(39), 24144-24153. https://doi.org/10.1073/pnas.2007835117

Hansson, S., Orru, K., Siibak, A., Bäck, A., Krüger, M., Gabel, F., & Morsut, C. (2020). Communication-related vulnerability to disasters: A heuristic framework. International Jour-nal of Disaster Risk Reduction, 49, 101645. https://doi.org/10.1016/j.ijdrr.2020.101645

Hillson, D. (2016). Risk escalation – A new strategy. PM World Journal.

Infanti, J., Sixsmith, J., Barry, M., Núñez-Córdoba, J., Oroviogoicoechea-Ortega, C., & Guillén-Grima, F. (2013). A literature review on effective risk communication for the preven-tion and control of communicable diseases in Europe. Stockholm: ECDC.

Innes, M. (2020). Techniques of disinformation: Constructing and communicating "soft facts" after terrorism. British Journal of Sociology, 71(2), 284-299. https://doi.org/10.1111/1468-4446.12735

Konow-Lund, M. (2018). News workers' reflections on digital technology and social media after a terror event. In H. Hornmoen & K. Backholm (Eds.), Social media use in crisis and risk communication (pp. 113-134). Emerald Publishing. https://doi.org/10.1108/978-1-78756-269-120181010

Kušen, E., & Strembeck, M. (2021). Building blocks of communication networks in times of crises: Emotion-exchange motifs. Computers in Human Behavior, 115, 106619. https://doi.org/10.1016/j.chb.2020.106619

Liu, L., Mirkovski, K., Lowry, P., & Vu, Q. (2023). Do as I say but not as I do: Influence of political leaders' populist communication styles on public adherence in a crisis using the global case of COVID-19 movement restrictions. Data and Information Management, 7(1), 1-10. https://doi.org/10.2478/dim-2023-0001

Lok, C., & Powell, D. (2000). The Belgian dioxin crisis of the summer of 1999: A case study in crisis communication and management. Dept. of Food Science, University of Guelph.

Makwana, N. (2019). Disaster and its impact on mental health: A narrative review. Journal of Family Medicine, 6(2), 3090.

Marcillo-Delgado, J., Alvarez-Garcia, A., & García-Carrillo, A. (2022). Communication strategies on risk and disaster management in South American countries. International Journal of Disaster Risk Reduction, 79, 103153. https://doi.org/10.1016/j.ijdrr.2022.103153

Masood, A., Scazzoli, D., Sharma, N., Le Moullec, Y., Ahmad, R., Reggiani, L., & Alam, M. (2020). Surveying pervasive public safety communication technologies in the context of terrorist attacks. Physical Communication, 40, 101073. https://doi.org/10.1016/j.phycom.2020.101073

Momenipour, A., Rojas, B., & Duquenoy, P. (2022). Trust and risk communication in terror-ism: A case study of the Westminster Bridge terrorist attack. Journal of Information Ethics, 31(1), 73-92. https://doi.org/10.3172/JIE.31.1.73

Moss, J., Tindale, R. S., & Wu, J. (2022). The importance of risk perception: Factors influ-encing COVID-19 risk perception and self-reported health behaviors. Risk Analysis, 42(2), 194-208. https://doi.org/10.1111/risa.13730

Mulyasari, F., & Shaw, R. (2013). Role of women as risk communicators to enhance disaster resilience of Bandung, Indonesia. Natural Hazards, 69(1), 2137-2160. https://doi.org/10.1007/s11069-013-0798-4

Olofsson, A., & Rashid, S. (2011). The white (male) effect and risk perception: Can equality make a difference? Risk Analysis: An International Journal, 31(6), 1016-1032. https://doi.org/10.1111/j.1539-6924.2010.01566.x

Palen, L., & Hughes, A. (2018). Social media in disaster communication. In H. Rodríguez, W. Donner, & J. E. Trainor (Eds.), Handbook of Disaster Research (pp. 497-518). Springer. https://doi.org/10.1007/978-3-319-63254-4_25

Palttala, P., Boano, C., Lund, R., & Vos, M. (2012). Communication gaps in disaster man-agement: Perceptions by experts from governmental and non-governmental organizations. Journal of Contingencies and Crisis Management, 20(1), 2-12. https://doi.org/10.1111/j.1468-5973.2011.00656.x

Pechta, L., Brandenburg, D., & Seeger, M. (2010). Understanding the dynamics of emer-gency communication: Propositions for a four-channel model. Journal of Homeland Security and Emergency Management, 7(1), 1547-7355. https://doi.org/10.2202/1547-7355.1700

Peters, E. M., Burraston, B., & Mertz, C. K. (2004). An emotion-based model of risk per-ception and stigma susceptibility: Cognitive appraisals of emotion, affective reactivity, worldviews, and risk perceptions in the generation of technological stigma. Risk Analysis: An International Journal, 24(5), 1349-1367. https://doi.org/10.1111/j.0272-4332.2004.00531.x

Peterson, M., & Gist, M. (2021). Transnational information exchange, social capital, and risk perception in the context of global health and pandemics. Pandemic Communication and Re-silience: Multidisciplinary Perspectives, 15, 103-121. https://doi.org/10.1007/978-3-030-77099-9_8

Reynolds, B. J., & Seeger, M. W. (2005). Crisis and emergency risk communication as an integrative model. Journal of Health Communication, 10(1), 43-55. https://doi.org/10.1080/10810730590904571

Richtel, M., & Baker, M. (2020). How misinformation spreads: Covid-19 falsehoods move faster than scientists can keep up. The New York Times, 8, 2020.

Rocque, M. (2012). Exploring school rampage shootings: Research, theory, and policy. The Social Science Journal, 49(3), 304-313. https://doi.org/10.1016/j.soscij.2011.11.001

Rohrmann, B. (2000). A socio-psychological model for analyzing risk communication pro-cesses. Australasian Journal of Disaster and Trauma Studies, 2000(2).

Sandman, P. M. (2006). Crisis communication best practices: Some quibbles and additions. Journal of Applied Communication Research, 34(3), 257-262. https://doi.org/10.1080/00909880600771619

Sauer, L. M., Catlett, C., Tosatto, R., & Kirsch, T. D. (2014). The utility of and risks asso-ciated with the use of spontaneous volunteers in disaster response: A survey. Disaster Medi-cine and Public Health Preparedness, 8(1), 65-69. https://doi.org/10.1017/dmp.2014.12

Siegrist, M., & Cvetkovich, G. (2000). Perception of hazards: The role of social trust and knowledge. Risk Analysis: An International Journal, 20(5), 713-720. https://doi.org/10.1111/0272-4332.205064

Sjöberg, L. (2000). Perceived competence and motivation in industry and government as fac-tors in risk perception. Risk Analysis: An International Journal, 20(5), 149-162. https://doi.org/10.1111/0272-4332.00010

Spence, P., Lachlan, K., & Burke, J. (2007). Adjusting to uncertainty: Coping strategies among the displaced after Hurricane Katrina. Sociological Spectrum, 27(6), 653-678. https://doi.org/10.1080/02732170701534267

Spence, P., Lachlan, K., Burke, J., & Seeger, M. (2007). Media use and information needs of the displaced victims of Hurricane Katrina. Communication Research Reports, 24(3), 217-224. https://doi.org/10.1080/08824090701439058

Stamoulis, P., Tsourvakas, G., & Vamvakas, V. (2020). Risk communication and decision-making: Ethical principles, trust, and technology. Risk Analysis, 40(11), 2355-2371. https://doi.org/10.1111/risa.13564

Tapsell, S., Penning-Rowsell, E., Tunstall, S., & Wilson, T. (2002). Vulnerability to flood-ing: Health and social dimensions. Philosophical Transactions of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences, 360(1796), 1511-1525. https://doi.org/10.1098/rsta.2002.1013

Trnka, S., & Trundle, C. (2014). Competing responsibilities: Moving beyond neoliberal re-sponsibilisation and individualised subjectivities in disaster preparedness. Social Anthropolo-gy, 22(3), 340-351. https://doi.org/10.1111/1469-8676.12076

Tull, M. T., Edmonds, K. A., Scamaldo, K., Richmond, J. R., Rose, J. P., & Gratz, K. L. (2020). Psychological outcomes associated with stay-at-home orders and the perceived impact of COVID-19 on daily life. Psychiatry Research, 289, 113098. https://doi.org/10.1016/j.psychres.2020.113098

van der Meer, T. G., & Verhoeven, J. W. (2014). Emotional crisis communication. Public Relations Review, 40(3), 526-536. https://doi.org/10.1016/j.pubrev.2014.03.004

van Gorp, B., & Smets, K. (2017). News frames and national integration: How news cover-age of anti-immigrant violence has varied in three national contexts. Ethnic and Racial Studies, 40(14), 2585-2603. https://doi.org/10.1080/01419870.2016.1271833

Vaughan, E., & Tinker, T. (2009). Effective health risk communication about pandemic in-fluenza for vulnerable populations. American Journal of Public Health, 99(S2), S324-S332. https://doi.org/10.2105/AJPH.2009.162537

Vos, S. C., Sutton, J., Yu, Y., Renshaw, S. L., Olson, M. K., Gibson, C. B., & Butts, C. T. (2018). Retweeting risk communication: The role of threat and efficacy. Risk Analysis, 38(12), 2580-2598. https://doi.org/10.1111/risa.13140

Wæraas, A., & Maor, M. (2015). Understanding organizational reputation in a crisis: The role of situational crisis communication theory. Handbook of Crisis Communication (pp. 285-299). Wiley Blackwell. https://doi.org/10.1002/9781444314885.ch14

Weber, E. U., Blais, A. R., & Betz, N. E. (2002). A domain-specific risk-attitude scale: Measuring risk perceptions and risk behaviors. Journal of Behavioral Decision Making, 15(4), 263-290. https://doi.org/10.1002/bdm.414

Weinstein, N. D. (1989). Effects of personal experience on self-protective behavior. Psycho-logical Bulletin, 105(1), 31-50. https://doi.org/10.1037/0033-2909.105.1.31

White, M. P., Pahl, S., Buehner, M., & Haye, A. (2003). Trust in risky messages: The role of prior attitudes. Risk Analysis: An International Journal, 23(4), 717-726. https://doi.org/10.1111/1539-6924.00350

Williams, A., & Davis, M. (2020). When only big data can save us: Communication and the social implications of data rescue as a strategy to address climate change. Media, Culture & Society, 42(7-8), 1084-1100. https://doi.org/10.1177/0163443720914026

Wilson, G. A. (2013). Community resilience, social memory and the post-2010 Christchurch (New Zealand) earthquakes. GeoJournal, 78, 303-317. https://doi.org/10.1007/s10708-012-9430-6

Witte, K. (1992). Putting the fear back into fear appeals: The extended parallel process model. Communication Monographs, 59(4), 329-349. https://doi.org/10.1080/03637759209376276

Wong-Parodi, G., & Feygina, I. (2020). Understanding and countering the motivated roots of climate change denial. Current Opinion in Environmental Sustainability, 42, 60-64. https://doi.org/10.1016/j.cosust.2020.01.009

Xie, B., & Zhuang, J. (2014). Social media and risk communication. In J. G. Voeller (Ed.), Wiley Handbook of Science and Technology for Homeland Security (pp. 234-255). Wiley. https://doi.org/10.1002/9780470087923.hhs621

Xu, J., & Li, Y. (2021). An emotion contagion model for disaster emergency communication on social media. Journal of Computational Science, 52, 101215. https://doi.org/10.1016/j.jocs.2021.101215

Zaval, L., Keenan, E. A., Johnson, E. J., & Weber, E. U. (2014). How warm days increase belief in global warming. Nature Climate Change, 4(2), 143-147. https://doi.org/10.1038/nclimate2093

Zhang, L., & Haller, A. (2013). Making air pollution visible: A social media perspective of haze pollution in China. Journal of Asian Pacific Communication, 23(1), 230-247. https://doi.org/10.1075/japc.23.1.11zha

Zhang, X., Dang, Y., & Chen, X. (2022). Visual risk communication on social media: A cross-cultural study on the flu and COVID-19 pandemics. Journal of Risk Research, 25(4), 407-425. https://doi.org/10.1080/13669877.2021.1909712

ANNEX A: Crisis Communication Check List

PREPAREDNESS PHASE

Preparation and Planning

Establish a Crisis Communication Team	
Identify key members from public health, emergency management, law enforcement, and communication specialists.	
Establish clear roles and responsibilities.	
Have the team trained.	
Incorporate the team into the organization processes.	
Develop Crisis Communication Plan	
Create templates for press releases, social media updates, and internal memos.	
Establish specific decision-making process.	
Establish protocols for message approval and release authority.	
Have the plans official signed and incorporated into the overall crisis planning.	
Ensure budget and necessary equipment.	
Test the Plans	
Organize frequent training sessions for the communication team.	
Run simulations of various scenarios to evaluate the communication plan.	
Train Spokespersons and Key Leaders (KLs) and Subject Matter Experts (SMEw)	
Train individuals to serve as spokespersons.	
Provide training to the organization personnel.	
Prepare a Media Card, with key points all personnel should have in mind in case of media engagement.	

Building Relationships	
Engage with Media	
Develop relationships with key media contacts.	
Educate them on your organization's work.	
Prepare mail lists.	
Community engagement and preparedness	
Establish communication channels with community leaders, NGOs, and other stakeholders.	
Educate the community on biological and chemical threats.	
Prepare mail lists.	
Constant Monitoring	
Develop monitoring capacity media (train, acquire platforms, cooperate with organizations – academia).	
Identify disinformation threats and develop reactive capacity.	
Develop relationship with information sources.	

EMERGENCY RESPONSE PHASE

Initial Response

Activate Crisis Communication Plan	
Set the team ready and in place.	
Make a strong statement across your organization and ensure the plan is respected by all members in what concerns the communication.	
Develop and Maintain Situational Awareness	
Gather accurate and timely information.	
Verify any information.	
Monitor the information environment.	

Outreach

Issue Initial Statements	
Share the initial details of the incident, focusing on the verified facts and the immediate steps taken.	
Explain the measures being implemented to manage the situation and ensure public safety.	
Hold regular briefings with the media to provide updates.	
Allow time for questions and clarify any misunderstandings.	
Address people's concerns and anxieties.	

Facilitate Dissemination by using Multiple Channels
Present the initial information about the incident, highlighting the confirmed details and immediate responses.
Outline the actions being taken to address the situation and safeguard public safety.
Ensure two-way communication is available.
Enable access to information, as far as it is possible.
Set up hotlines, email addresses, and social media channels for public inquiries.
Respond to public concerns with empathy and clear information.
Stick to the main values:
Be consistent, timely and accurate.
Address disinformation:
Identify disinformation narratives and mal-actors.
Address rumors and misinformation promptly.
Evaluate and Adjust the Communication (and overall) Strategy
Monitor the Media and Social Media:
Focus on the people's sentiment.
Understand the interaction dynamics between your organization and the people.
Identify weaknesses on your plan.
Identify additional (or changes in the) needs for information of the community.
Make adjustments
Make the necessary adjustments in your communication strategy.
Acknowledge any main concerns identified to your organization, that might need to be considered.

RECOVERY PHASE

Don't interrupt your Engagement
Keep providing updates on recovery efforts and the long-term health impacts.
Provide resources and support to individuals and communities affected.
Maintain open communication with the media and community stakeholders.
Strengthen relationships established during the crisis to enhance future preparedness.
Keep Maintaining Situational Awareness
Continue monitoring and maintain situational awareness.
Watch out for disinformation narratives that may emerge.
Evaluation and Review
Evaluate the effectiveness of the communication response.
Highlight strengths and pinpoint areas needing improvement.
Gather feedback from the public, stakeholders, and team members.
Utilize surveys, interviews, and public meetings to collect comprehensive feedback.
Document the Event
Document the crisis event, communication strategies, and outcomes.
Create detailed reports for both internal review and external stakeholders.
Revise Plans
Revise the crisis communication plan based on lessons learned.
Modify training programs and protocols accordingly.
Provide Support
Provide access to information on respective resources and support.
Additionally, provide information on mental health resources and support services.