[PRACTICE]

D8.3, DEFINITION OF RESILIENCE MATRIX

D8.6 UPDATED RESILIENCE MATRIX

D8.7 DELIVERABLE PRODUCTION

PRACTICE WP8 deliverables

Dissemination level: Public

Nature: other

UNCLASSIFIED

SEVENTH FRAMEWORK PROGRAMME

UNCLASSIFIED

Title:	D8.3 Definition of the Resilience Matrix, D8.6 Updated Resilience Matrix, D8.7 Deliverable Production	
Date:	May 23, 2012	
Author(s):	Nigel Hale	CBRNE Ltd
	Dominic Kelly	CBRNE Ltd

This project has received funding from the European Community's Seventh Framework Programme. The views expressed in this document are purely those of the writer and may not in any circumstances be regarded as stating an official position of the European Community.

Summary Work Package 8

The objective of WP8 is to improve public knowledge and awareness of CBRN incidents by providing a toolbox of information, procedures and processes to understand the human and societal factors that influence the impact of and response to CBRN incidents, as well as reduce the impact of CBRN incidents on society and individuals. The effectiveness of the 'human and societal' toolbox will be tested (via WP6) with members of the public and professional responders in an exercise at a conference/shopping centre in Birmingham in August 2013.

The output will include tools and measures (i) to inform, educate and prepare the mindset of the EU citizen for a CBRN event, (ii) to provide guidance about protective behaviour and to aid the identification of relevant information sources during events, (iii) to mitigate the societal impact on communities and individuals post event, and (iv) to identify solutions aimed at recovery.

Work Package team:

Kristian Krieger, King's College London (KCL)
Brooke Rogers, KCL
Richard Amlôt, Health Protection Agency (HPA)
Dominic Kelly, CBRNE Ltd
Dave Usher, CBRNE Ltd
Nigel Hale, CBRNE Ltd
John Astbury CBE, CBRNE Ltd
Karin Lindgren, European CBRNE Centre, Umeå University (UMU)
Rebecca Nystrom, UMU
Erna Daniellson, Mittuniversitetet Mid Sweden University (MIUN)
Anna Olofsson, MIUN
Dzenan Sahovic, UMU
Ingrid Bastings, Netherlands Organization For Applied Scientific Research (TNO)
Maarten Nieuwenhuizen, TNO
Julia Pearce, KCL
Jan Ryland, KCL
Dianne van Hemert, TNO

Contents

Figures

1. Executive Summary

A design approach for a matrix based method to assess the vulnerability of members of the public to CBRN incidents is derived from an existing approach for the assessment of the resilience of organisations known as the Resilience Matrix (e.g. FP7-SEC-2009-1 Project IMCOSEC **I**ntegrated approach to **IM**prove the supply chain for **CO**ntainer transport and integrated **SEC**urity simultaneously). This new approach will ultimately be presented in a tool (the Tool) which will form part of the Project PRACTICE Toolbox. This deliverable presents the development of the model (the Model) – i.e. the equations, assumptions and relationships - that it is proposed will be implemented in that tool.

The derivation of the adaptation of the original Resilience Matrix (RM) approach to Project PRACTICE and an overview of the original method are presented.

This deliverable presents the Model as a proof of concept at the end of the first year of Project PRACTICE. The Model and the Tool will be further developed in Deliverable D8.16[1], having taken account of experience gained from the PRACTICE validation exercises.

The results of research presented in D8.8, observations from the Stakeholder Workshop (D8.4) and internal project workshops have been used to aid the development of the Model.

The Model uses the summary figure developed in D8.8 (see D8.8 Figure 10) and in particular the four factors of "Perception of Threat", "Trust in Responders", "Perception of Efficacy" and "Effectiveness of Communications" (The Four Factors) expounded there, along with the Extended Parallel Processing Model used in health care research as its basis.

The predictor of vulnerability chosen for the Model is the likely type of public behaviour that may occur. This is classified as either Adaptive or Maladaptive, where Adaptive indicates that the advice and guidance of the responsible authorities is likely to be followed and will reduce vulnerability, while Maladaptive indicates that the advice and guidance is unlikely to be effective and that the public will adopt responses other than those advised. Moreover, if Maladaptive behaviour is indicated this is because of a perceived imbalance between the public's perception of such threats and their perceptions of how well they and those responsible for their welfare will be able to deal with them. This, in turn, leads to broader negative psychosocial issues.

It is intended that the RM will be used by experts as a heuristic, semi-quantitative learning aid to help them to identify areas where the public may be vulnerable[2] to the effects of a CBRN attack or incident

An example spreadsheet implementation of the Model is presented to demonstrate the proof of concept in Figure 11.

[1] D8.16 was added to the Project PRACTICE scope by agreement with the REA, after agreement to take the opportunity to include lessons from the validation exercises.
[2] Throughout this deliverable Vulnerability refers to Psychosocial Vulnerability as defined in Deliverable D8.8 and D8.3

2. Introduction

This document incorporates three of the deliverables required for Project PRACTICE, namely D8.3 (Definition of the Resilience Matrix), D8.7 (Deliverable Production) and D8.6 (Updated resilience Matrix [Bridging Report]). The work reported in this document will be used along with the future work which is also outlined, to produce the final deliverable for the Resilience Matrix D8.16 (Updated Resilience Matrix after Validation Exercises). The Updated Matrix will form one of the new tools in the PRACTICE toolbox being developed in Work Package (WP) 5 and D8.16 will thus be accompanied by a user manual / guidance notes as required by WP5.

The work reported here is based upon an approach for the assessment of business resilience, known as the Resilience Matrix (RM) method, which has been presented by Hale and Kelly of CBRNE Ltd. A summary of the original Resilience Matrix method, the full definition of which is commercially confidential, is presented in Annex 1 and in overview in Section 3.

It was proposed for Project PRACTICE that this approach could be adapted so that it could provide guidance on potential vulnerability of the public to CBRN type events[3]. In particular it was proposed that this method of assessment of data may provide useful guidance to the development of the proposed User Manuals within Work Package 8 (D8.11, D8.12, D8.13) of the Project. It is also envisaged that the methodology will be utilized to analyse the results of the proposed three validation exercises in the Project.

In order to explore the applicability of the RM method to Project PRACTICE a series of discussions, workshops and internal meetings were held. A summary of the outcome of these is presented in Section 4 of this document as 'Development of the Conceptual Model' and the further more detailed development work undertaken to progress from conceptual model is presented in Section 5 'Detailed Development'. The way in which it is envisaged that the Tool which implements the model will be used is outlined in Section 6 and the remaining work to be

---

[3] Resilience and Vulnerability are meaningless terms in the abstract. One must ask "Resilient in the event of what?" or "Vulnerable to what happening as a result of what?" to be clear.

For a member of the public, taking the case of a CBRNE attack on them as an example; they might be considered to have resilience if they have the personal traits, capabilities, resources and experiences such that they can cope with them and possibly also recover quickly. "Resilience" in this sense refers to the concept that even in situations of multiple risks there are certain qualities within the individual or his/her environment that allow him/her to deal with these risks and thrive in spite of them (Luthar S.S 2003).

For an individual, they may be vulnerable if they are likely "to develop varied forms of psychopathology or behavioural ineffectiveness" or if they are "susceptible to negative developmental outcomes" (Zimmerman and Arunkumar 1994). So the vulnerabilities of a person are those areas where they may be susceptible to some form of undesirable response or outcome and their resilience is some measure of the sum total of their capabilities to deal with these vulnerabilities; resilience is a description of a general pattern (Luthar S.S 2003).

completed between now and the completion of D8.16 - which is due after the Project's validation exercises - is presented in Section 7.

The Model that is developed is based upon the Four Factor model presented in PRACTICE Deliverable D8.8 and the additional background research presented in D8.9 and D8.10.

3. Background to the RM method

The RM approach is to examine what arrangements are in place within an organisation for dealing with specific threats and to examine cross-cutting arrangements like those for training and staff management in order to assess their effectiveness to reduce the threat. One of the key features of the tool is its ability to take account of inter-dependencies and interactions between arrangements for distinct threats (for example, there are obvious links between an organisation's response to terrorism and its response to crime more generally and for dependencies between arrangements for dealing with threats and cross cutting arrangements (for example, between arrangements for training staff to deal with terrorism and arrangements for training more generally). Furthermore, the RM approach allows for the application of 'weightings' or 'importances' to threats.

The likely performance of the organisation is scored against a 3x3 matrix (known as an "effects matrix"), where the columns of the matrix represent the performance of the organisation with respect to its People, its Processes and its Physical assets and the rows represent performance with respect to where these are targeted in terms of Prevention, Preparation and Protection. So, for example, examination of the effects matrix entries provides a holistic view of how an organisation uses each of its people, processes and physical assets to provide measures which prevent threats materialising, prepare for the consequences from them if they do arise or protect them when they do.

Each entry in an effects matrix is rated to represent the likely performance of the organisation's arrangements relevant to that entry (e.g. how well People assets are used to Prevent a threat or how well Physical assets are used to Protect against the consequences of a threat). Normally this is based upon a rating in the range 0 to 5 – where 0 represents poor or no arrangements and 5 represents excellent arrangements. The ratings are assigned by trained assessors based upon interviews with the organisation.

There are proprietary algorithms within the matrix tool that allow for the calculation of overall ratings for Resilience taking into account dependencies and weightings as discussed above.

For the purposes of the PRACTICE project it is clearly necessary to adjust the RM approach to indicate Vulnerability of the Public to a CBRN incident rather than Resilience of an organisation, but in essence a similar approach is proposed. To support the development of the User Manuals, the specific vulnerability that is examined is the development of varied forms of psychopathology,, behavioural ineffectiveness or the susceptibility to negative developmental outcomes – including broader societal impacts.

4. Conceptual Development of the new Tool

The following sections present a brief overview of the work that was undertaken to develop a conceptual model for the matrix tool and to test its validity during the first public workshop of the Project (see Usher and Kelly).

4.1 Preliminary Meeting

The fundamental structure of the RM method, which is shown Figure 1 and is expanded upon in Annex 1, was presented to members of the WP8 team at an initial internal meeting on 26 August 2011 at King's College London (Notes from the team Meeting are retained in the Project and are available upon request).

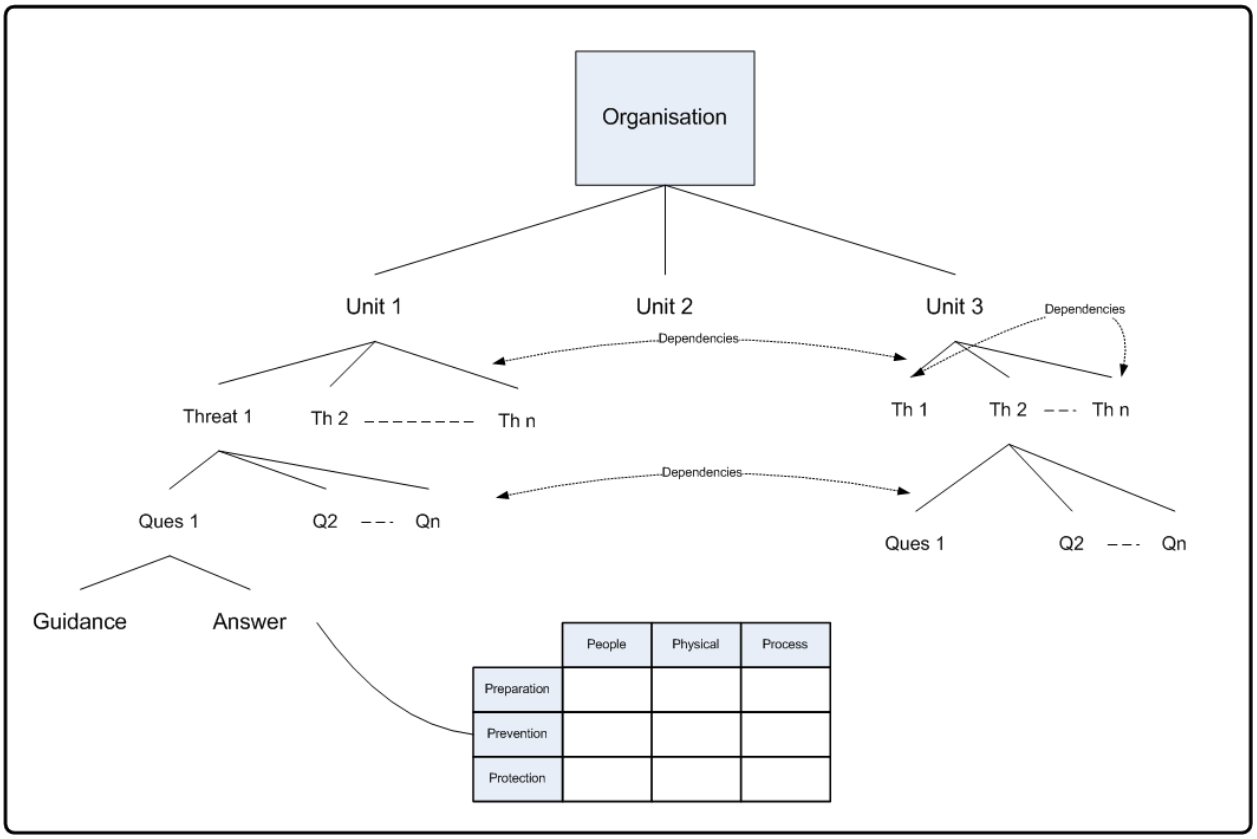


Figure 1: Basic Structure of the RM Approach

Notes to Figure 1: The Figure shows a database type structure where an organisation may be considered to be composed of multiple units (e.g. maintenance department, sales and admin, security etc). The organisation may be subject to a number of Threats (Threat 1 to Threat n) and for each Threat the database contains a number of Questions, which are each supported by Guidance which tells the user what to look for in terms of a 'good' answer to the Question. Each question is scored against a matrix (shown towards the bottom of the Figure) for each Unit. The tool performs some numerical manipulation of the scores according to pre-defined dependencies and algorithms to obtain an overall result.

The preliminary discussions at the meeting identified the following points as being relevant to the development of the RM method for PRACTICE.

- The System of concern (or the Organisation, using the nomenclature of Figure 1) is the Human Being or perhaps a collection of the same
- The dimensions could include things like;
  - Threat types
  - Human behaviours
  - The timeframe
  - The beneficiaries (Public, Emergency Services, etc)
- The Threat taxonomy could be based upon the Scenarios identified in PRACTICE Deliverable D2.1.
- The dimensions against which existing procedures and practices could be scored and their dependencies will need to be identified (with help from others).
- The types of dependency could be influenced by a wide range of factors including ethical and cultural ones.

4.2 Follow-on discussions with KCL

Further discussion of the methodology within the WP8 Team identified the following key conclusions;

- It is desirable for the tool to be able to tell us something about how badly a community/group of individuals would be affected by a range of different CBRN incidents. There are two aspects of importance: (1) CBRN incidents can have major psychological implications, endangering the mental and physical health of members of the public as well as broader societal implications. (2) Effective CBRN incident management depends on/can be undermined by maladaptive[4] behavioural responses of the public. Collectively these can be considered to be measures of Vulnerability. Since Resilience is more a product of the counter-measures - such as an adequate risk communication – and the RM development work is considered to be part of the threat assessment task of D8.3 (Definition of the RM) it should focus on the vulnerability indicators.
- The tool output should solely relate (collectively) to members of the public and determining their vulnerability.

[4] Maladaptive behaviour refers to types of behaviour that inhibit a person's ability to adjust to particular situations. This type of behaviour is often used to reduce one's anxiety, but the result is dysfunctional and non-productive. For example, avoiding situations because you have unrealistic fears may initially reduce your anxiety, but it is non-productive in alleviating the actual problem in the long term .[http://panicdisorder.about.com/od/glossaryip/g/MaladpBehavior.htm]

- The only opportunity to gain new input from the public in respect of the model, in PRACTICE, was going to be the D8.4 Public Stakeholder Workshop (see below) and the validation exercises being managed within Work Package 6.

Furthermore, discussions which were held prior to the formal publication of D8.8 (Krieger and Rogers 2012) identified the following "perceptions" as potential dimensions of the matrix or at least areas that could be incorporated into the model - these factors give us an idea why CBRN incidents can have adverse consequences beyond the purely physical damage, so in that respect, they are important determinants of the psycho-social vulnerability to CBRN incidents.

- Perceptions of the threat:

  There is a set of qualitative descriptors of threats (such as familiarity, understanding/knowledge, catastrophic potential, voluntariness of exposure, dread/fear, effects on children/future generations, manifestations of effects, reversibility, and more) that can be associated with public concerns/anxieties (which in turn can be linked to mental health issues and inadequate behavioural responses).

  These can be expected to vary with the chosen agent, the way a terrorist attack (or any other incident with CBRN materials[5]) plays out, etc.

  This is made more complex (and probably less robustly quantifiable) by the fact that perceptions are also shaped by related/connected perceptions through the so-called mental models (Glik et al., 2008). These link an actual threat with similar experiences, such as a dirty R-bomb with the Chernobyl accident. The extent to which such reference events matter depends not only on how long ago or how big the reference event was but is also institutionally mediated, i.e. varies from one country to the other and from one social group to the other.

  It was agreed that it is not necessary for the Model to integrate these mental models aspects, but that there should be guidance to users to run focus groups - or similar - to find out about pre-existing mental models and trust issues in their respective countries and that there should be a method for the results of those consultations to be incorporated into the model (e.g. by adding a co-efficient into the RM).

  There is little scientific literature providing numerical models of the perception of threats.

- The Public's Perceptions of Responders:

  This is normally subsumed under the label of 'trust'. It concerns levels of perceived competence, honesty and similar properties (fairness, credibility, integrity, reliability, etc.). If the public trusts the responsible organisations and thus believes in the effectiveness of the response, its anxiety/concerns are reduced and greater compliance with behavioural advice of the trusted authorities is likely.

[5] Note that terror-related CBRN incidents obviously add some uncertainty and anxiety in the perceptions of the public(s) because, e.g., you don't know whether there are further perpetrators somewhere. However, most of the literature looks more broadly at CBRN incidents.

These perceptions have been quantified to a degree in the so-called Trust Scales (Poortinga & Pidgeon 2003) and (National Trust measures 2012) (see D8.2 and D8.8 for trust measures) but there are other variables like, for example, the organisations of counter-terrorism, whether it is decentralised or centralised, whether civil contingency governance is part of the military infrastructure or has a parallel organisational structure, which will affect these perceptions.

Therefore, a second aspect that the model may need to address is organisational landscape and its perception by the public. There is however little numerical research on this topic such that the development of meaningful metrics will be difficult.

- Perceptions of the self and the costs of protective behaviour:

  A third set of factors that shape the resilience/vulnerability to CBRN attacks is the confidence of members of the public in their own effectiveness to undertake the recommended protective measures and their perceptions of the costs[6] of undertaking these measures. If confidence is high and costs are perceived to be acceptable in view of the benefits from taking prescribed measures, members of the public are more likely to take the protective measures. Conversely if the costs are seen to be too high or confidence is very low then maladaptive behaviours may follow.

  Confidence and cost perceptions are likely to vary by culture, institutional context and other contextual factors. Although cultural theory (Drake and Wildavsky, 1990, Sjoberg, 1996) has some relevance to this its validity has been contested heavily and it should only be used as a broad conceptual tool.

- The effectiveness of Risk Communication and its ability to address Perceptions:

  The resilience/vulnerability depends on the effectiveness (quality and timing) of risk communication itself. Risk communication can mitigate those factors that cause concern among members of the public, such as lack of understanding by providing information. The quality of (existing) risk communication is therefore an important factor to consider and to integrate into the matrix.

4.3 The Conceptual Model

The fundamental conclusion drawn from the preceding Sections is that some of the factors that affect the public perception of risk and those that affect the public's behaviour following an incident are well known and researched. However, because of the complexities of the issues and the principal subjects (i.e. people) there is little numerical modelling available that can be used to form a sound basis for a numerical Model. There is, however, sufficient knowledge and data to enable a representative model to be produced, which encompasses the general features of the published research, which could be used by those qualified and experienced in the field of human psychology and behaviour to guide their efforts.

[6] Costs in this context mean costs to self and include some subjective elements like loss of amenity and loss of dignity as well as direct health issues or financial costs.

The discussions noted above led to the conceptual model as shown in the upper half of Figure 2. It also shows the link to the other human behaviour work being undertaken in WP8, which is encompassed by the bottom half of the figure.

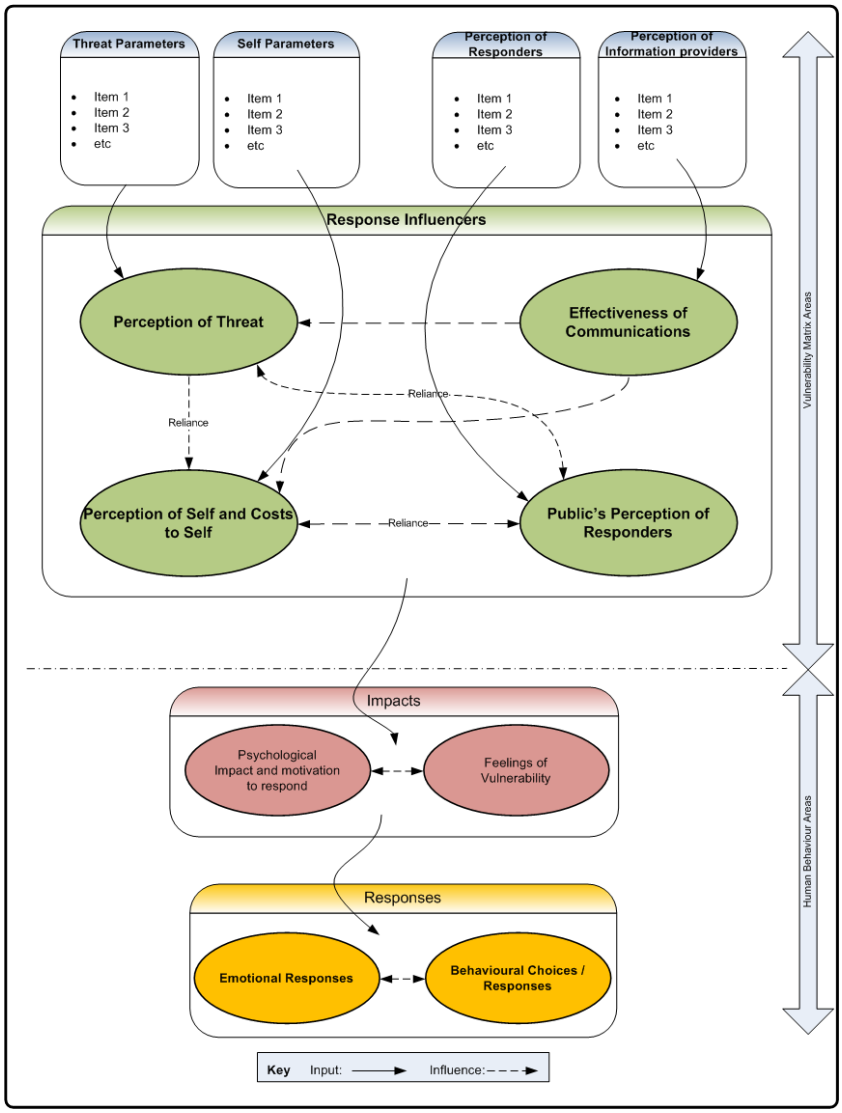


Figure 2: The Conceptual Model of the Resilience Matrix for Vulnerability Assessment

4.4 Stakeholder Workshop

The Public Stakeholder Workshop for WP8, which was held on 26 January 2012 in Birmingham is reported in PRACTICE Deliverable D8.4 (Usher and Kelly) to which reference should be made for a complete record of it. Among other things the workshop sought to explore some of the factors that influence public perception and feelings during a CBRN type incident. This was achieved by the use of injects[7] followed by collective interviews with focus groups. The conceptual model outlined in Figure 2 was used to help construct the question sets used by the interviewers and to test in broad terms if the conceptual model was a valid representation.

[7] Pieces of information (in the form of handouts)

Some of the key points that arose from the Workshop, which are relevant to this deliverable are;

- The presence of family groups – rather than individuals – would have a significant impact on the behaviour following and incident.
- Pre-event messages (in the case of the workshop in the form of simulated newspaper articles) can have a significant impact upon perceptions of risk and actions prior to and perhaps during an incident.
- Trust in first responders was generally high in the group although there were concerns that this trust was itself open to abuse by terrorists or similar groups.
- Need for officials to be known and trusted
- The public generally have little knowledge of the specific chemical agent (Sarin) selected for the desktop review.
- There were individuals who, although they trusted first responders and the like in principle, thought that they would undertake behaviour like fleeing the scene of the incident even if this was advised against.
- Individuals would go to recognised and trusted official web-sites and the like to obtain further information regarding any advertised threat. NHS and Government web-sites were specifically mentioned.
- Some groups noted that they would have difficulty complying with directions from First Responders if those directions involved what they perceived to be a significant loss of dignity such as undressing in a public or semi-public environment.
- There was a general feeling that individuals would need the Responders to explain to them why certain actions were being requested of them rather than them just being given directions.

Although the bullet points presented above are selected to demonstrate that the elements of the model are relevant, this conclusion is also supported by a broader examination of the results presented in D8.4 (Usher and Kelly).

5. Development of the Model

Subsequent to the Workshop, research undertaken in support of Deliverable D8.8 showed that the science of the determination of public vulnerability has been broadly researched and that a number of Factors have been identified as being a key to that determination. D8.8 presented a summary model, reproduced below in Figure 3, which shows how these inter-relate at a conceptual level.

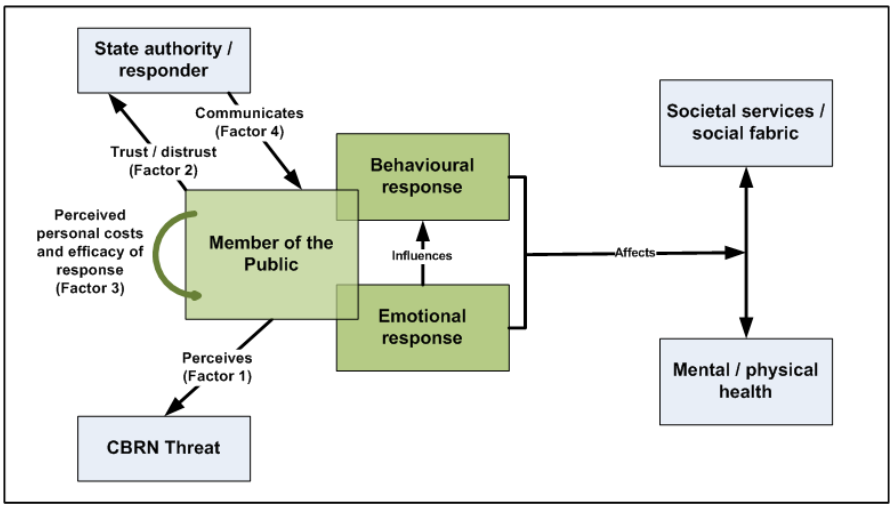


Figure 3: Factors Determining Psychosocial Responses (From D8.8)

Because of the parallel development of D8.8 (as summarised in Figure 3) and the conceptual model presented in Section 4, they are clearly consistent with each other. Subsequent work reported in PRACTICE Deliverables D8.9 and D8.10 has shown that the Four Factors are key *generic* variables that make a substantial contribution to explaining the emotional and behavioural responses of members of the public to CBRN incidents but also that they may take effect in very different manners (i.e. varying weights of individual factors) depending on various contextual variables and the interplay between each of the Four Factors.

Whilst it is outside of the scope of Project PRACTICE to undertake further detailed scientific analysis in this field or to develop and test further models of Public vulnerability, there are indications of broad relationships between the Four Factors (see D8.8 and Sjöberg 1996, 1998 & 2000). These have been developed and used in indicative ways in the Model (described in Section 5.1) such that they will direct knowledgeable users of the Model to areas requiring further work.

The Model presented here recognises that within PRACTICE there will be limited opportunity to gather large amounts of data directly from the public about their perceptions of threats and the other Factors identified by D8.8 but that it is possible to ask what arrangements are in place (by responsible authorities and organisations) for addressing them and how good those arrangements are. By using the relationships discussed above, the Model shows how the relative strengths and weaknesses of these arrangements could contribute to public vulnerability.

In this way, it is possible to measure how well supported the Public are by organisations (e.g. Government, Emergency Services) and how capable they are likely to be in dealing with the Public during such an incident. It also reflects the relationships between the Public and these organisations through mechanisms such as trust. The way that these relationships are represented in the Model is presented in Section 5.1.1

5.1 Implementation of Psychosocial Modelling

The following sections discuss the way that the Four Factors from Figure 2 are represented in the Model and the dimensions that are used in the effects matrices. Annex III presents more detailed support for the equations and modelling methods used.

The four key Factors in the model are shown in Table 1, which clearly maps to Figure 3.

Table 1: The Four Factors and their acronyms used in the Model

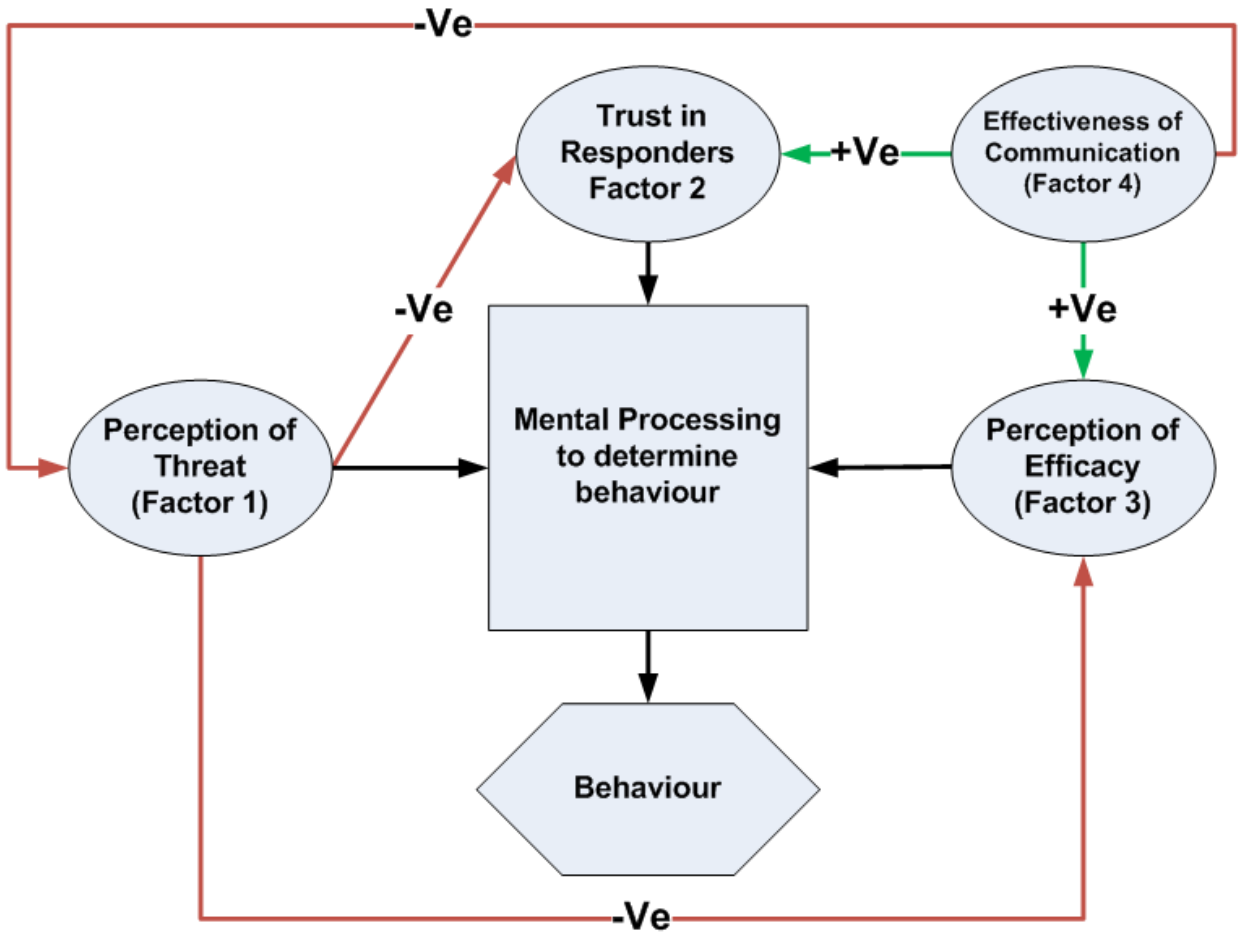
Factor Number	Factor Name	Acronym
1	Perception of Threat	PoT
2	Trust in Responders	TiR
3	Perception of Efficacy	PoE
4	Effectiveness of Communication	EoC

5.1.1 *Interaction of Factors*

Within the Model, Figure 3 (from D8.8) has been implemented as shown in the Influence Diagram shown in Figure 4 (overleaf).

Although the influence diagram reflects many of the inter-relationships discussed in D8.8, it is important to note that it differs in some respects. The most significant difference between the influence diagram of this Deliverable and Table 1 of D8.8 is that Perception of Threat in the former implicitly excludes any direct assessment of Trust in Responders or Perception of Efficacy, whereas in the latter these are listed as elements of the Perception of Threat discussed. For the Model, this relationship has been inverted; Perception of Threat is shown to destructively relate to Trust in Responders and to Perception of Efficacy[8]. As the overall goal of the model is to predict or measure vulnerability as a function of the Factors shown then the overall effect is maintained – the modelled relationship could be viewed as saying "All other things being equal, the higher the psycho-social impact of a threat, then the greater the Trust in Responders and Perception of Efficacy that is required to maintain the same level of Resilience". This simplification requires a careful framing of the questions used to populate the Model (or the Tool used to implement it) to keep these Factors separate.

[8] See Figure 4 for explanations of constructive and destructive dependency.



Notes to Figure 4:

Dependencies are shown by the Green and Red Links.

- Destructive dependencies are shown in Red and are labelled as "-Ve". These show that an increase in the item at the foot of the arrow is modelled as leading to a decrease in the item at the head of the arrow (e.g. Poor use of communications can lead to an increased level of threat perception) and vice versa.

- Constructive dependencies are shown in Green and are labelled as "+Ve". These show that an increase in the item at the foot of the arrow is modelled as leading to an increase in the item at the head of the arrow (e.g. good use of communications can improve perception of responders efficacy) and vice versa.

The mathematical form of the dependencies is shown in Annexe AII.1.

Figure 4: Influence Diagram for the Factors

The 'mental processing' element of Figure 4 and its contributing Factors is based upon the Extended Parallel Processing Model as discussed in Section 5.1.2. The modelling of the Effectiveness of Communications is discussed in Section 5.1.3.

5.1.2 Factors 1, 2 and 3 - The EPPM Model

D8.8 notes that the Factors that influence public vulnerability are, at least in part, developed from Protection Motivation Theory (see D8.8 Section 4.3). This theory has been built upon and refined in the Extended Parallel process Model (EPPM) – see Maloney et al and Annex I. The EPPM is widely used as the basis for the formulation of messaging campaigns where a particular action (e.g. the use of condoms) is desired from a population in order to mitigate a certain threat (e.g. AIDS). The messages are known as 'fear appeal' messages. An equivalent desired action in a CBRN environment could be to "remove your clothes and shower" and the corresponding threat could be "otherwise you will remain contaminated and be harmed".

The EPPM suggests that perception of a threat and of the efficacy of the proposed action combine through a fear appraisal to produce a response. Moreover it suggests that if that fear appraisal is significant then the response can be maladaptive[9]. **This prediction of Behaviour Type (i.e. either Adaptive or Maladaptive) is taken as the predictor of Vulnerability in the Model.**

Figure 5 shows how the EPPM model has been conceptually combined with the Influence Diagram suggested by Figure 4.

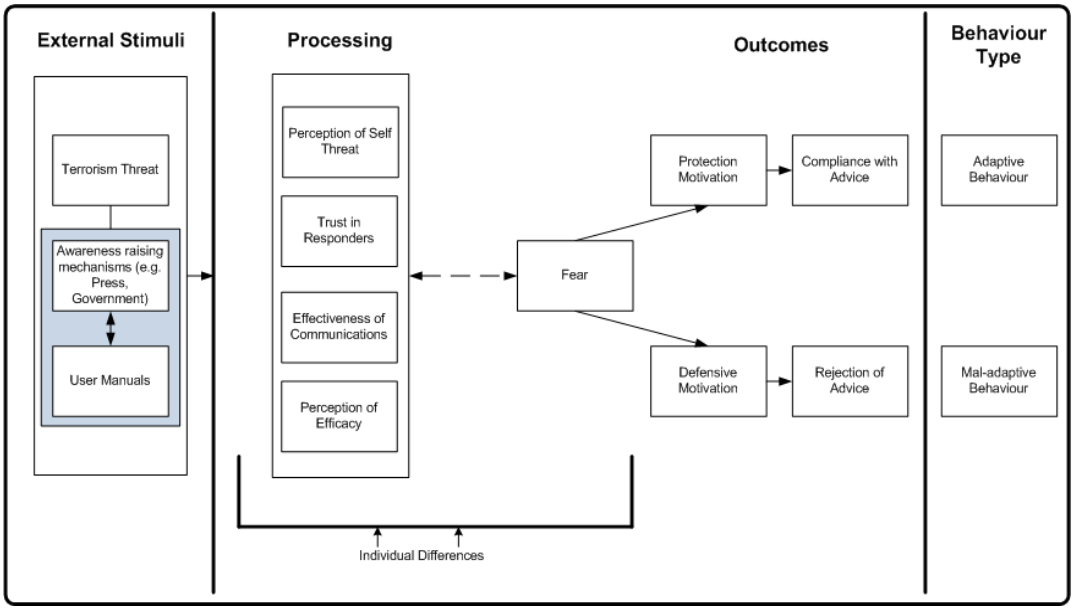


Figure 5: EPPM Model and the RM Model Merged (adapted from Maloney et al)

[9] Maladaptive behaviour refers to types of behaviour that inhibit a person's ability to adjust to particular situations. This type of behaviour is often used to reduce one's anxiety, but the result is dysfunctional and non-productive. For example, avoiding situations because you have unrealistic fears may initially reduce your anxiety, but it is non-productive in alleviating the actual problem in the long term . Adaptive behaviour means dealing with the threat in a way that directly addresses it – in the cases considered here that means following the prescribed advice.

Whilst, in the traditional EPPM model the "fear appeal" is deliberately generated by those wishing to change a response, in the case of project PRACTICE the "fear appeal" would be a combination of both terrorism in general and messages from first responders and the like[10].

Further work by Witte et al (1995) suggested that the key factor influencing the type of behaviour that results from the fear appeal message was the balance between perception of the Threat (PoT) and perception of Efficacy (PoE) as shown on Figure 6 (the definitions of PoT and PoE are essentially the same as those adopted for the Factors listed in Section 5.1.1 and noted in D8.8.

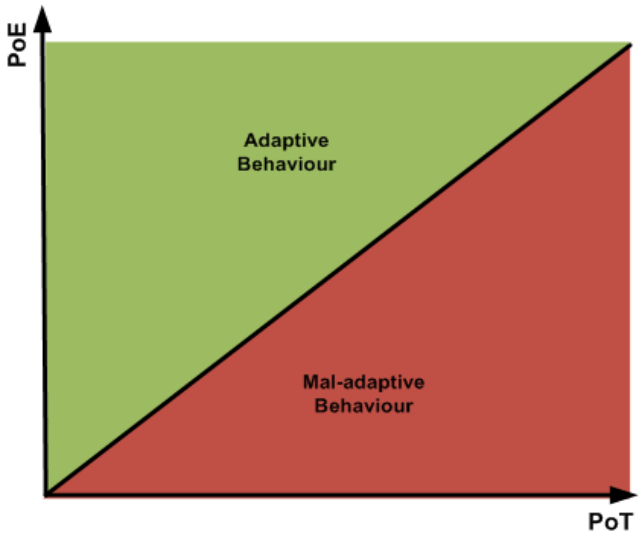


Figure 6: The EPPM Relationship between behaviour and Perception of Threat and Efficacy

Because of the potential reliance of the public on First Responders in the threat situations considered in Project PRACTICE, in the Model, PoE has been replaced by a Factor referred to as Total Efficacy (TE) which also includes a contribution from Trust in Responders. The representation of TE in the Model is presented in Annex III.2[11].

TE is modelled as a function of both PoE and TiR *(1)*

Maloney et al and Witte et al have noted that the first step that the Public takes (not necessarily consciously) in determining what response, if any, they will adopt to a Threat is to engage in a subconscious type of threat assessment to determine whether or not they perceive that the threat is severe enough and their own susceptibility to the threat is high enough to warrant further action. If people do not perceive the threat to be high, they will not experience fear. In this case the personal assessment comes to an end and people will not respond to the message.

[10] In this case, the fear appeal is composed of both deliberate controlled messages (in this example from first responders) and uncontrolled messages (from the general background of a terrorist threat, perhaps via news media and the like).
[11] The fact that the Responders are not present at all times is accounted for in the Model by the addition of a timescale dimension which is discussed in Section 5.2.1.

This implies that the relationship shown in Figure 6 only applies once Fear[12] is greater than some Threshold Value (TV) and that below that value no response will be achieved (or at least it will not be as predicted). In the Model, Fear is represented as a function of PoT and TE such that increasing PoT leads to increasing Fear and increasing TE leads to reducing Fear. The actual form of relationship used is presented in Annex AIII.2

Fear is modelled as a function of PoT and TE *(2)*

Given the simplicity of the model and the way that responses may change from individual to individual, the relationship shown in Figure 6 is modified in the Model to account for uncertainty about the region where behaviour changes from adaptive to maladaptive. Thus, within the Model, Figure 6 is modified as shown on Figure 7 (the region of uncertainty is shown in orange on this Figure)

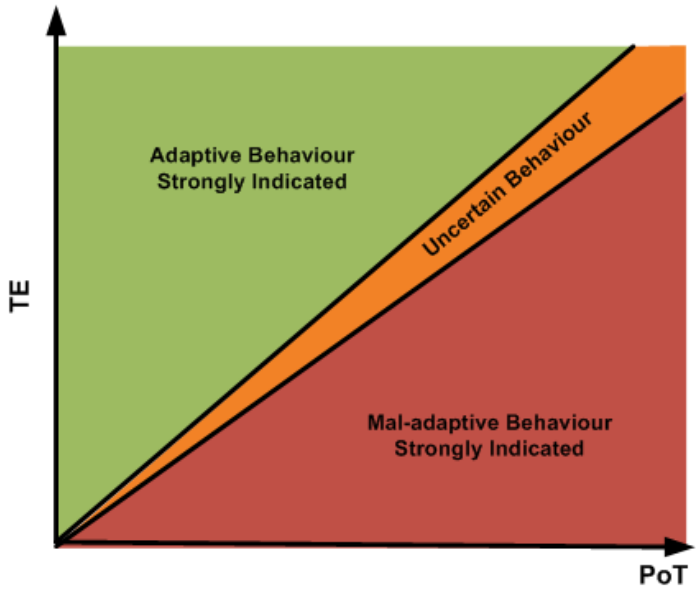


Figure 7: Relationship between TE and PoT in the Model.

In summary the Model uses a relationship which may be expressed as

If Fear is greater than TV then the type of behaviour that the model indicates is determined by the balance between TE and PoT as shown on Figure 7. If Fear is less than TV then the model indicates that no response (maladaptive or adaptive) is certain. *(3)*

The Ratio TE/PoT is referred to here as the Behaviour Index (BI) *(4)*

[12] Maloney et al describe Fear as "an internal emotional reaction comprising psychological and physiological dimensions that may be aroused when a serious and personally relevant threat is perceived"

5.1.3 Factor 4 - Effectiveness of Communication (EoC)

The Fourth Factor incorporated into the model is Effectiveness of Communications. This differs from the other Factors in the model in so far as it is a pure input variable; examination of Figure 4 shows that this Factor has no inputs from the other Factors shown.

Deliverable D8.8 notes that;

> *"although good risk communication cannot always be expected to improve a situation, poor risk communication will nearly always make it worse" and*
>
> *risk communication "is vital for facilitating and encouraging appropriate protective actions, reducing rumours and fear, maintaining public trust and confidence, and reducing morbidity and mortality" and*
>
> *"The flipside entails the negative consequences of poor communication: For instance, contradictory, multi-source messages can increase uncertainties and fear, as well as undermine trust in risk managers.".*

This effect is modelled by the use of a Simple Dependency Model (see Annex AIII.2) and an appropriate weighting factor (of the form shown in Figure AIII.1 c). This exaggerates the effects on the other Factors of a poor score for EoC whilst providing for only a moderate positive effect from a good score for EoC.

The degree to which EoC may influence the other Factors may differ between phases – for example, in an environment of a low background threat level, communications are likely to attract little attention from the public and to have short "shelf life" whereas once a threat is materialising or the threat level is growing it is probable that the public will seek out information and start to rely on communications for support (see D8.4). Furthermore, D8.8 notes that "Communicating with the public is particularly important in pursuit of greater preparedness and resilience of members of the public in the event of a CBRN incident".

These two effects are also reflected in the model through the use, respectively, of the Threshold Value (noted in Section 5.1.2) and through the use of a timescale dimension as noted in Section 5.2.1.

5.2 Dimensions of the Effects Matrix

A fundamental aspect of the Model is that results obtained are presented in summary form in a matrix format, where the dimensions of the matrix (i.e. the rows and columns) are such that comparison of scores across them reveals additional information to the user (by revealing relative strengths and weaknesses or patterns). These matrices are referred to as Effects Matrices.

The choice of dimensions for the Effects Matrices clearly depends upon on the subject area being analysed and on the types of Threats being considered. The dimensions chosen for the Model are the timescales of the incident and the maturity of the knowledge and experience of those implementing response measures as discussed in the following Sections 5.2.1 and 5.2.2 respectively. The Effects Matrices are presented in Section 5.2.3.

5.2.1 Timescales

Public vulnerabilities clearly exist both before during and after an incident. Accordingly the Model has dimensions representing the following[13];

The Preparedness Phase (Pd): The phase that exists prior to any specific incident occurring that directly impacts upon the population under consideration. This may be considered to be the baseline phase.

The Present Phase (Ps): The phase that exists during an incident (i.e. when the emergency services may be attending an incident or when public perceptions may be heightened because of raised awareness, for example).

The Post Phase (Pt): The phase that exists after the Present Phase, when the immediate impact has subsided but there may remain heightened perceptions (above the baseline Preparedness phase).

In the modelling discussed up to this point, no account has been taken for the relative importance of each of the Factors in each of these phases. D8.8 notes however that some of the Factors may be more important than others at different phases. The Model therefore includes a set of parameters used to reflect these potential variations. These parameter values are set in a parameter table, as discussed in Annex III.2.5, which provides relative weights to the Factors, for each timescale phase.

5.2.2 Knowledge Phases

Since public vulnerability will not just be a function of the knowledge held by those responsible for their welfare (or vulnerability) but will also depend upon how that knowledge has been applied and tested, the Model also includes the 'Knowledge Phase' dimensions shown in Table 2;

Table 2: Knowledge Phases

Phase	Description
Knowledge (K)	Relates to how well the subject organisation has gathered and adopted current knowledge and best practice.
Action (A)	Relates to how well that knowledge has been transcribed into action
Effectiveness (E)	Relates to how well the action has been demonstrated to be effective

[13] These correlate to the Preparedness, Response and Recovery phases noted in PRACTICE Deliverable D3.1 (Bastings et al)

In this way, the model has the potential to identify the issue that is sometimes referred to as the 'knowledge gap' or the 'doing gap' (see Pfeffer J and Sutton R.I for example). This refers to the gap between an organisation possessing knowledge about a subject but not effectively implementing that knowledge across the organisation.

5.2.3 Effects Matrices

The Model provides for the answers (and assigned scores) to its questions to be grouped by Factor and summarised in Effects Matrices which have the dimensions of Pd, Ps, Pt by K, A, E as noted in 5.2.1 and 5.2.2. The Model also uses a colour coding scheme to show whether the scored values represent 'good' practices (in Green), poor practices (in Red) or somewhere in between (Orange hues). For example, an Effects Matrix, for a particular Factor, might look like;

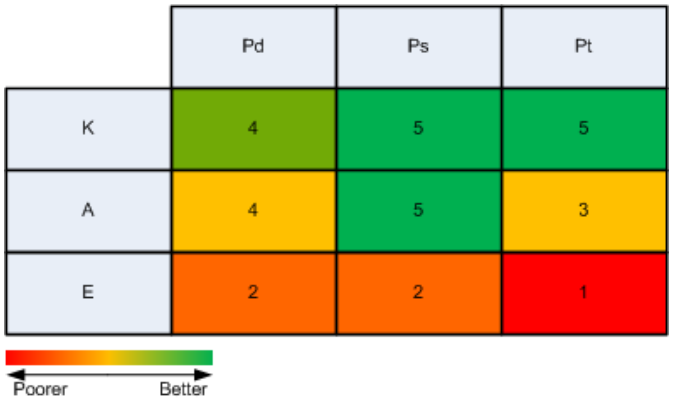


Figure 8: Example Effects Matrix for a Factor

Which, in this case would illustrate that the responses are generally good in respect of Knowledge and Action but less so in respect of Effectiveness, especially in the later stages of an Incident (Ps and Pt).

5.2.4 Behaviour Effects Matrix

Each of the Effects Matrices for each of the Factors is combined using the relationships and parameters discussed above to produce an overall Behaviour Effects Matrix where the values in this case are the BI values which indicate the type of behaviour that may result given the information scored in the Factor Effects Matrices. An example Behaviour Effects Matrix is shown in Figure 9 (Note that the entries for each of the KAE dimensions have been summed at this stage, as a simple equally weighted sum, but this can be varied in the Model).

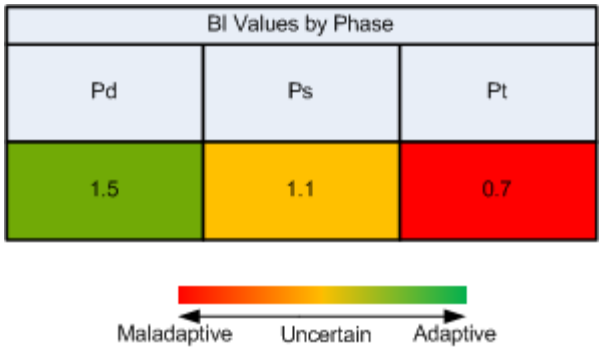


Figure 9: Example Behaviour Effects Matrix

5.3 Scoring

The Model assumes that answers to the questions are scored against simple Likert type scales (Likert R) which can be turned into numerical values to enable its computational aspects.

Accordingly all of the questions are cast as how well are the things covered/understood/managed.

All questions are framed so that they may be scored according to the following structure[14].

Likert Scale Point	Example Meaning
Low (Left End)	Little emphasis on the Factor, it has not been recognised or implemented
Mid-Point	Moderate Emphasis, Some of the areas noted in the guidance are covered
High (Right End)	There is a detailed treatment, all of the known issues are addressed and gaps are recognised

5.4 Questions and Guidance

The exact form of the Questions to be used in the implementation of the Model is discussed further in Section 7 “The Way Ahead”. The following structure is proposed as a taxonomy for the questions, to be used as the basis for their development during D8.16. Perception of Threat (PoT) is taken as the exemplar but a similar approach is possible for all of the Factors.

The Questions will also be supported by Guidance notes which will provide more specific guidance about the types of metrics that should be used to judge performance.

[14] Although the foregoing has discussed scoring using discrete point values – based upon Likert type scales - the scores could equally well be presented by probability distributions, without any loss of generality. The Model presented here would, in that case, be equivalent to using the mean or most likely data point from the distributions.

Table 3: Example Structure of Questions for the Model

	Factor: Perception of Threat		
	Phase		
Knowledge	**Pre**	**Present**	**Post**
Questions	In preparing for a particular Threat, (e.g. a chemical release) how well does the Source Organisation understand the role played by the Factor in Public vulnerability?	During a particular Threat (e.g. during a chemical release), how well does the Source Organisation understand the role played by the Factor in Public vulnerability?	In the period following a particular Threat (e.g. following a chemical release), how well does Source Organisation understand the role played by the Factor in Public vulnerability?
Guidance	*It is important to understand what Affected Groups know about the Threat, whether these views are accurate and the likely effect these views could have on the vulnerability of the Affected Group. It is also important to understand the extent to which the Source Organisation "buys into" the importance of the Affected Group's perceptions and how it addresses itself to understanding and responding to them.* *e.g. Does the Source Organisation acknowledge that the Affected Group's perception of the Threat may affect their vulnerability? (Strategy/policy)* *e.g. Does the Source Organisation's strategy include maintaining an understanding of the Affected Group's perceptions? (Strategy/policy)* *e.g. Who is responsible for understanding the Affected Group's perceptions of the Threat? (Roles and responsibilities) e.g.. What steps has the Source Organisation taken to ascertain and understand the Affected Group's perceptions of the Threat? (Situation awareness, Information and Knowledge, organisational connectivity)* *e.g. How are the Affected Group's perceptions communicated within the Source Organisation? (Communication and relationships)* *e.g. Have the Affected Group's perceptions of the Threat been included in the Source Organisation's risk analysis? (Risk Analysis)* *e.g. What steps has the Source Organisation taken to change the Affected Group's perceptions of the Threat? (Risk Analysis/Planning)*		
Action			
Questions	In preparing for a particular Threat, (e.g. a chemical release) how well does the Source Organisation address the Affected Group's perceptions of that Threat?	… during a particular Threat? (e.g. during a chemical release)	… in the period following a particular Threat? (e.g. following a chemical release)

Guidance	*It is important to understand the steps the Source Organisation takes to improve the Affected Group's perceptions of Threat and/or the Source Organisation's understanding of those perceptions.* *e.g. How does the Source Organisation decide on the actions (if any) it takes to change the Perceptions of the Affected Group? (Leadership, Management and Governance, Planning)* *e.g. How does the Source Organisation decide on the actions (if any) it takes to improve the understanding of the Perceptions of the Affected Group? (Leadership, Management and Governance, Planning)* *e.g. How are priorities decided? (Leadership, Management and Governance, Planning)* *e.g. What steps (actions) has the Source Organisation taken to change the Affected Group's perceptions of the Threat? (Risk Analysis/Planning)* *e.g. What steps (actions) has the Source Organisation taken to improve its understanding of the Perceptions of the Affected Group? (Risk Analysis/Planning)* *e.g. Who is responsible for the Source Organisation's actions? (Roles and responsibilities)* *e.g. Are there systems in place to ensure good awareness within the Source Organisation (e.g. all employees) of the actions taken? (Situation awareness, Communication and relationships)* *e.g. How are the actions (e.g. "awareness events") communicated to the Affected Group? (Communication and relationships, Organisational Connectivity, Situation awareness)* *e.g. How well understood are the anticipated effects of the actions taken by the Source Organisation? (Planning, Strategic vision and outcome expectancy)*		
Effectiveness			
Questions	In preparing for a particular Threat, how well known is the effectiveness of the Source Organisation's actions on the Affected Group's perceptions of that Threat?	… during a particular Threat? (e.g. during a chemical release)	… in the period following a particular Threat? (e.g. following a chemical release)
Guidance	*Having taken action to improve the Affected Group's perceptions of the Threat and/or the Subject's understanding of those perceptions, it is important to understand the effects of the* Source Organisation's *actions.* *e.g. What were the effects of the Subject's actions on the Affected Group's perception of Threat? (Strategic vision and outcome expectancy, connectivity awareness)* *e.g. What metrics or range of indicators are used to measure the levels of success of each action? (Planning)* *e.g What were the effects of the actions on the Subject's understanding of the Affected Group's perception of Threat? (Situation awareness)* *e.g. Were the effects anticipated? (Strategic vision and outcome expectancy, Planning)* *e.g. Who is responsible for evaluating the effects of the Subject's actions on the Affected Group and the Subject? (Roles and responsibilities, Leadership, Management and Governance Structures)*		

	e.g. Are there systems in place to ensure good awareness within the Subject (e.g. all employees) of the effects of the actions taken? (Situation awareness, Communication and relationships)

6. Use of the Tool

The way in which the Model overall is applied is shown in Figure 10 (overleaf) and a simple example tool implementation of it, excluding the recording of evidence, is shown on Figure 11 (overleaf).

For the present Deliverable a simple spreadsheet model has been developed. It is intended that through application of the model during the PRACTICE validation exercises, it will be further developed and refined using feedback from those exercises. It is envisaged that there will then be a tool which will then be in a form where it will be usable on a practical and commercial basis.

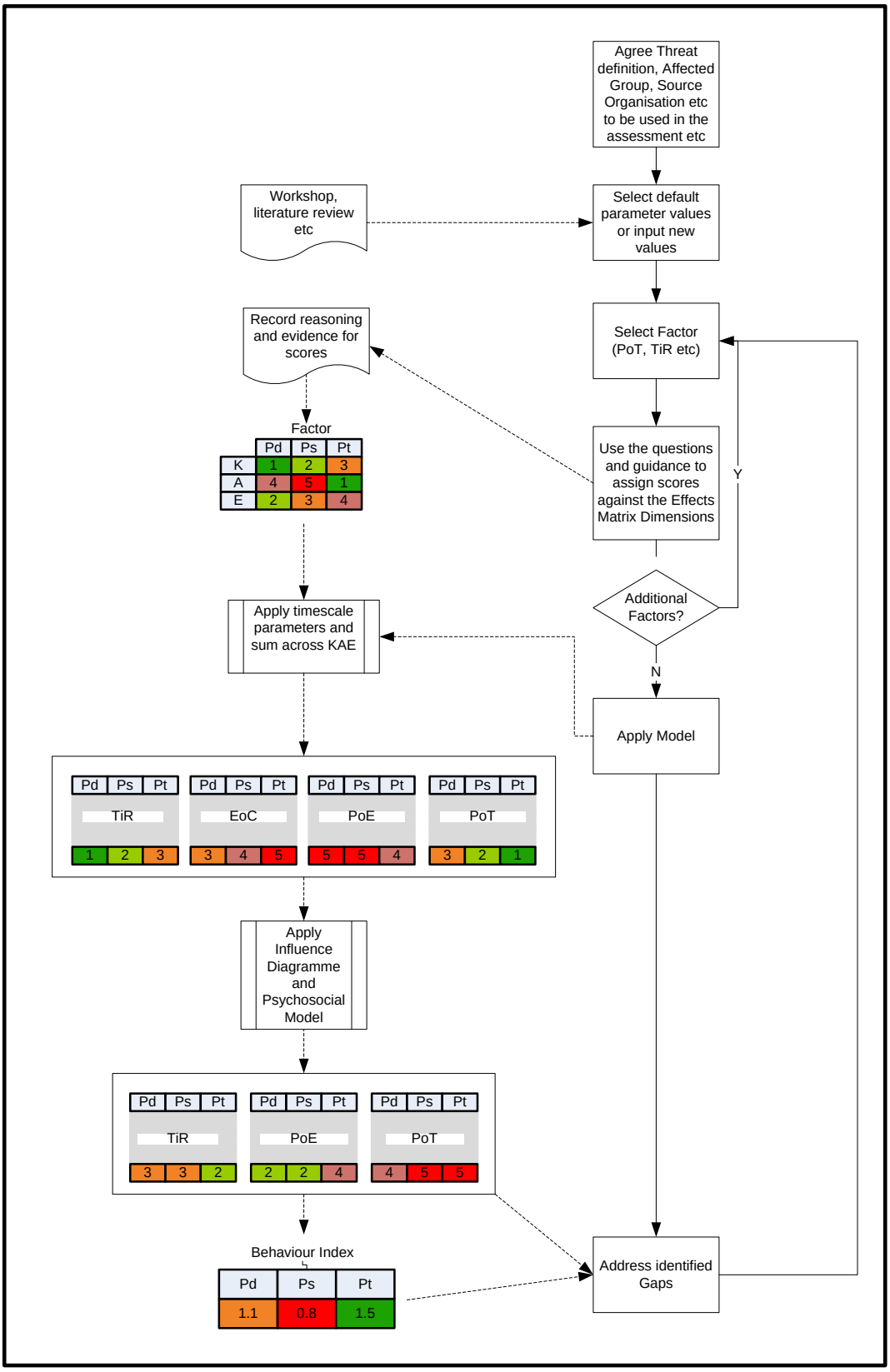


Figure 10: Implementation of the Model

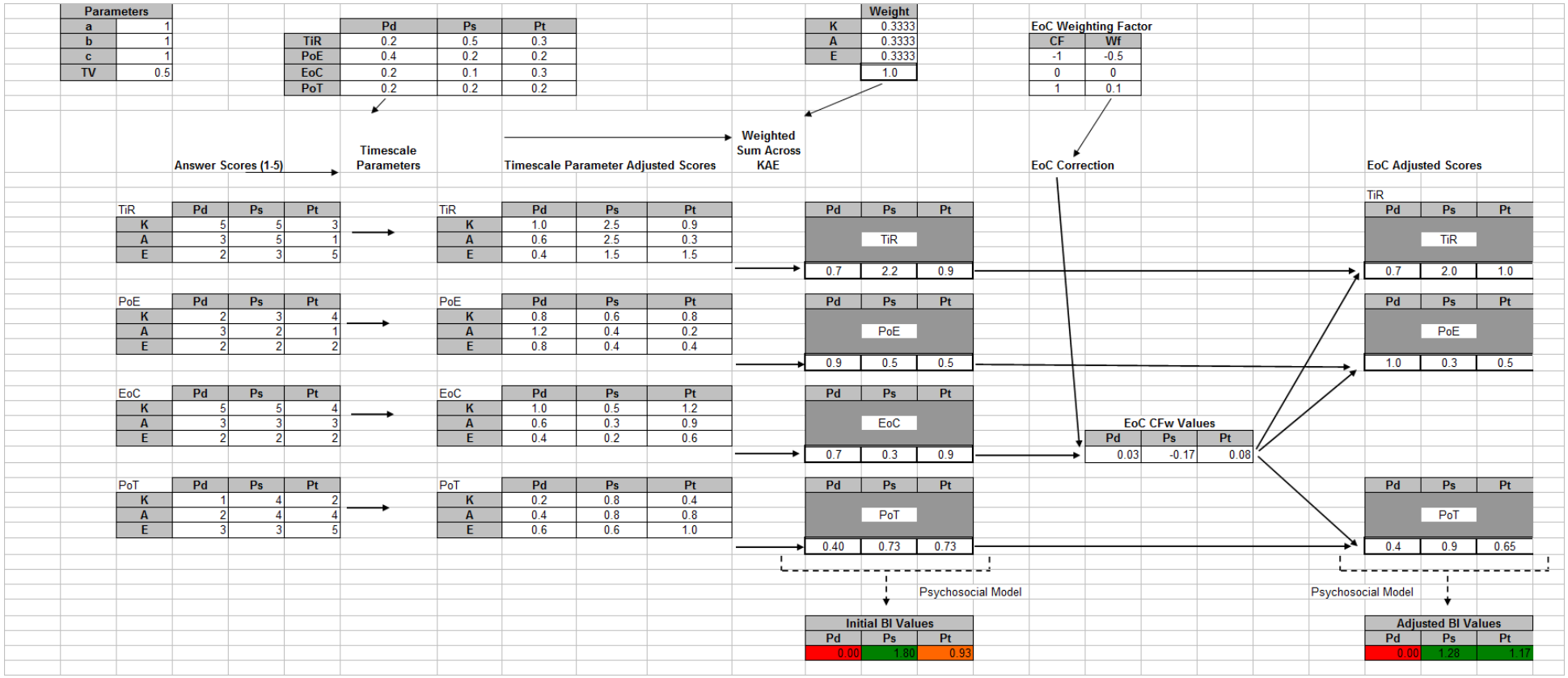


Figure 11: Example Model Application (excluding recording of evidence)

7. The Way Ahead

All future work on the development of the matrix will be linked to the preparation and evaluation of the exercises by close co-operation between WP8 and WP6. Also because the tool will form part of the PRACTICE Toolbox, WP5 will also be closely involved. Details of the work to be undertaken are presented below.

7.1 Parameters

In the Annexes, the model includes the following parameters which the user must set or accept default values for;

1. a and b - the weighting factors for the calculation of Total Efficacy (TE)
2. c - a weighting factor for the calculation of Fear
3. BI_U and BI_L - the upper and lower bounds for the uncertainty region relating to prediction of Maladaptive or Adaptive behaviour
4. Timescale Parameter values – i.e. weighting factors that indicate the relative importance of the Factors in each of the four Phases.
5. KAE weights – the weights to be used when calculating the weighted sum across the KAE phases.
6. The form of Figure AIII.1 b and c (i.e. the dependency models)

It is proposed that all of the above will be provided with default values or forms based upon internal Project workshops and discussions. It is proposed that these workshops will use techniques such as the Analytic Hierarchy Process (Saaty et al), the ranked "pairwise" comparison technique (Canter L.) or the Delphi technique (See Linstone and Turoff), for example. The choice of methodology will be made after internal WP8 discussions. Thus, the default values will represent the expert views of the Project team at the time of analysis[15].

These parameter values will be derived prior to the first validation exercise in 2013 and prior to the production of the first drafts of the WP8 User Manuals.

7.2 Semi-Empirical testing in Validation Exercises

The applicability of the Model in general and the values of the parameter will be examined prior to, during and after the validation exercise by interviews, focus groups, questionnaires etc (as indicated by the developing findings of the Project) with participants (both Public and Responders).

[15] As the Project team is represented by members from across the European community, efforts will be made to solicit views from across that community.

As for the identification of Parameters discussed above, the actual methods to be used will be selected by internal WP8 discussion.

The overall model validity will also be judged by WP8/6 review following each exercise to establish if further refinement will be required.

It is also proposed that comparison of the results across the three exercises will help to refine some of the modelling aspects with respect to the relative impacts of different types of scenarios and agents. This may lead to the inclusion of a further parameter set in the Model to reflect these variations.

As the three exercises will take place in three geographically different locations and will thereby include different responding agencies and arrangements, the exercises will also provide the opportunity to identify the impact of such exogenous variables.

7.2.1 Potential Difficulties

Whilst the exercises are clearly anticipated to provide useful feedback, they will be limited in their potential to provide real indications of fear as those attending will not experience any real threat to their wellbeing during the incident which naturally only uses simulated injects.

The development of appropriate questionnaires will also require careful co-ordination between WP8 and WP6.

7.3 Questions & Guidance

It is proposed that the questions and guidance which the Model contains and which the user of the model uses to help populate it, will be more fully developed to specifically list and refer to existing knowledge and best practice as the remainder of the WP8 deliverables become available in approved form. Again, the exact form of these will be determined by internal WP8/WP6 workshops which will, where possible, include representatives drawn from, for example, emergency services.

7.4 D8.16 “Updated Resilience Matrix –After Validation Exercises”

D8.16 will present the model arising in conclusion of all of the work presented here and to be undertaken as described immediately above. It will be comprised of three parts:

Part 1: A working model

Part 2: A resume of the updates to the model since this Deliverable (incorporating the items listed above) and will therefore effectively be an addendum. It will therefore, provisionally, have sections reporting on the following:

- Updates to default Parameter Values
- Revised Questions and Guidance
- Updates to the dependency models

- Lessons learned from Validation Exercises

Part 3: Will be a detailed user manual for the Tool so that it may be incorporated into the PRACTICE Toolbox. It will, inter-alia, include the following, in common with the other PRACTICE Tools:

- Nature of the tool (using the Staccato Taxonomy [see ASD])
    - To be able to reference correctly the tool along the functions
- Complete description of the tool in different languages
    - Complete product sheet
    - Complete Usage Guide
- Description of the Various Operational conditions
    - constraints
    - limitations
    - ...
- Description of all the interfaces at various levels
    - Public
    - Eventually Private for further developments...
- Availability policy, legal constraints, licences policy, ethical issues…
- Sensitivity aspects (user restrictions…)

8. Conclusions

During the process encapsulated in 8.3, 8.6 and 8.7 the Resilience Matrix model has been adapted to focus on vulnerability indicators. This reflects the switch from focusing on the resilience of an organisation to the vulnerability of the people (whether members of the public, decision makers or first responders).

The vulnerability indicators are encapsulated within the Four Factors being “Perception of Threat”, “Trust in Responders”, “Perception of Efficacy” and “Effectiveness of Communications”.

The resulting maladaptive or adaptive behaviour that these four factors indicate become the predictors used in the Model.

Therefore the conceptual, practical and mathematical process for assessing and calculating the vulnerabilities of people is now developed, thereby creating a template to be populated (as part of D8.16) with detail relevant to a CBRN event in a public place, via interviews and mini workshops in close liaison between WP6 and WP8. This will assist the process of ensuring that the user manuals focus on the actual concerns of the people, whether their role in the event is as an innocent bystander or an active participant.

9. Literature

ASD (AeroSpace and Defence Industries Association of Europe), *Deliverable D1.2.2, STACCATO Final Taxonomy*, online at http://www.asd-europe.org/site/fileadmin/user_upload/STACCATO_final_taxonomy.pdf

Bastings I., Peters C., Wevers J., Vink J. (2012), *D3.1 Survey Methodology*, Project PRACTICE WP3, D3.1, TNO

Canter L.W. (1997), *Environmental Impact Assessment (Second Edition)*, McGraw-Hill inc.

Drake K & Wildavsky A. (1990) *Theories of Risk Perception: Who Fears What and Why?* Daedalus 119: 41-60.

Glik D, Drury A, Canavaugh C & Shoaf K. (2008) *What not to say: Risk communication for botulism*. Biosecurity and bioterrorism: Biodefence Strategy, Practice, and Science 6: 93-107.

Henderson J.N, Henderson L.C, Raskob G.E and Boatright D.T, *Chemical (VX) Terrorist Threat: Public Knowledge, Attitudes, and Responses*, in Biosecurity And Bioterrorism: Biodefense Strategy, Practice, and Science, Volume 2, Number 3, 2004

Krieger K, Rogers B M (2012), *Systematic review of existing projects- Public Perceptions and Risk Communication in Times of Crisis , Project PRACTICE WP8, D8.8*, KCL

Likert R (1932), *A Technique for the Measurement of Attitudes*, Archives of Psychology 140: 1–55.

Linstone H.A, Turoff M, *The Delphi Method, Techniques and Applications*, available at http://is.njit.edu/pubs/delphibook/delphibook.pdf, accessed April 2012.

Luthar, S.S (2003), *Resilience and Vulnerability: Adaptation in the Context of Childhood Adversities,* Cambridge University Press, The Edinburgh Building, Cambridge Cb2 2RU, UK.

Maloney E.K., Lapinski M.K., Witte K., *Fear Appeals and Persuasion: A Review and Update of the Extended Parallel Process Model*, Social and Personality Psychology Compass 5/4 (2011): 206–219

National Trust Measures, Table on trust in specific domains, from European Social Survey Round 4. (2008). http://www.europeansocialsurvey.org/index.php?Itemid=80&option=com_docman. Last Accessed February 2012.

Poortinga W and Pidgeon N.F , *Exploring the Dimensionality of Trust in Risk Regulation*, in Risk Analysis, Vol. 23, No. 5, 2003.

Saaty, T.L.; Peniwati K (2008). *Group Decision Making: Drawing out and Reconciling Differences.* Pittsburgh, Pennsylvania: RWS Publications. ISBN 978-1-888603-08-8

Sjoberg L. (1996) *A discussion of the limitations of the psychometric and cultural theory approaches to risk perception*. Radiation Protection Dosimetry 68: 219-225.

Sjöberg L. (1999*), Consequences of perceived risk: Demand for mitigation* p139, in Journal of Risk Research 2 (2), 129–149 (1999)

Sjöberg L. (2000) , *Factors in Risk Perception,* in Risk Analysis Vol 20, No 1, 2000, Society for Risk Analysis

Turner B.L, Kasperson R.E and others, *A framework for vulnerability analysis in sustainability science, http://www.pnas.org/content/100/14/8074.full#aff-1 accessed January 2012.*

Usher D, Kelly D (2012), *Summary Report for the Project PRACTICE Public Stakeholder Workshop*, CBRNE Ltd.

Vinchon C, Carreño M-L, Contreras-Mojica D.M, Kienberger S, Schneiderbauer S, Alexander D, Barbat A.H, Cardona O.D, Decker B, Eidsvig U, Papathoma-Köhle M, Miniati R), Pratzler-Wanczura S, Ulbrich T, Vangelsten B.V, and Welle T, *Methods for the Improvement of Vulnerability Assessment in Europe : Assessing vulnerability to natural hazards in Europe: from principles to practice Manual on methods and concepts* ,

Witte K, McKeon J. Cameron K., Berkowitz J., (1995), The Risk Behaviour Diagnosis Scale (A Health Educator's Tool), Michigan State University, East Lansing MI48824.

Zimmerman, M. A., and R. Arunkumar. 1994. *Resiliency research: Implications for schools and policy*. Social Policy Report 8 (4): 1-17.

I Annex I: Overview of the Resilience Matrix Method

Resilience Matrix Overview - D Kelly and N Hale (CBRNE Ltd)

Background Theory – From a Paper by CBRNE Ltd

Life is not linear, most outcomes are dependent upon many variables and these variables are seldom entirely independent of each other.

We often use the separation of variables approach to approximate solutions to the real world – i.e. we assume that the variables act independently or linearly although we know that they do not in all cases. Moreover, people do not generally behave in this way.

These simplifying assumptions often lead to solutions that are only valid for a small part of the solution space or which are valid for small perturbations from the starting conditions. For example, on Figure A1.1, the red line is the true behaviour of a system (S) dependent upon variable x and the blue line is the simplified solution which is valid or approximately valid for only a small part of the total solution space as shown[16].

In a complex system (C) it is sometimes only possible to model responses by building up the model from many sub-systems such as the one modelled above – with the inherent simplifications (see Figure A1.2).

Organisations often have processes, arrangements and procedures that are built up in this way and which are valid for everyday use but which may not be valid in more extreme situations.

Resilience

The overall behaviour of an Organisation can be viewed as a matrix of systems and sub-systems such as those discussed earlier, some of which are connected to others and some of which are not. In Figure A1.3, each of the nodes is a system and the lines show how they are connected to other systems and the thickness of the lines shows the strength of the connection. The connections can be seen as some form of supportive grid that keeps the organisation whole.

[16] Furthermore, we sometimes need to assume that solutions are only dependent upon a selected range of variables or that some of the variables do not contribute significantly to the solution (i.e. extending the example above there could be a third dimension to the problem – the Z dimension – but these extra dimensions have been ignored to make things easier).

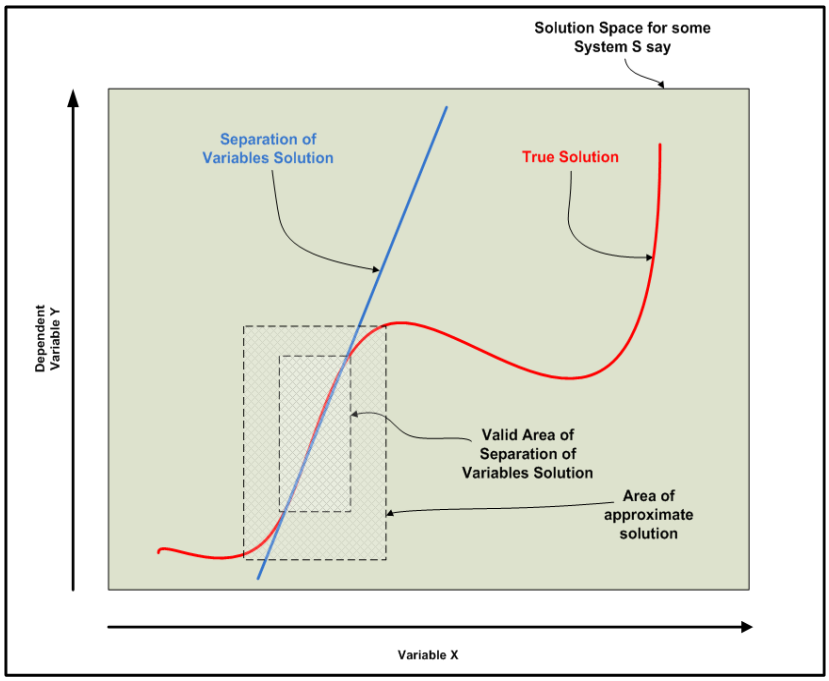


Figure A1.1: Approximation of behaviour by separation of variables

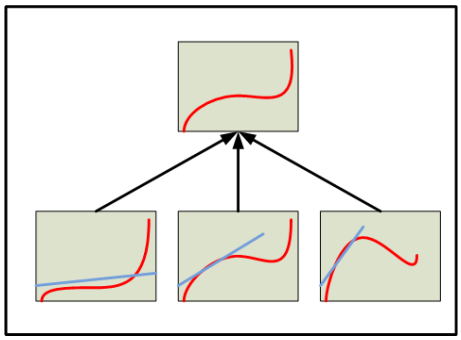


Figure A1.2: Complex system (C) modelled as composite of simplified systems

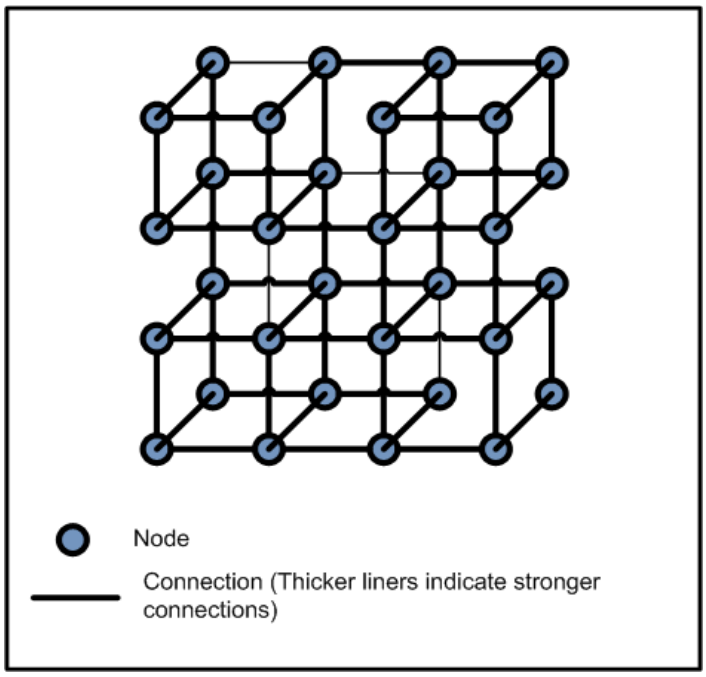


Figure A1.3: Organisational Arrangements and Interconnections

When any one of the connected systems is disturbed by some external influence the overall system may respond in several ways, such as shown in Figure A1.4 (where, in each case, the node in Red is the one that has been disturbed); response (A) is well "behaved" and the response may be considered to be first order - although the overall system is challenged it remains essentially intact and functional; in response B the system that is perturbed becomes completely independent of the remainder of the overall system, which nevertheless remains otherwise functional; response C by contrast represents a gross collapse of the overall system with second and third order effects such that it cannot reasonably continue to perform in this form for any significant period of time.

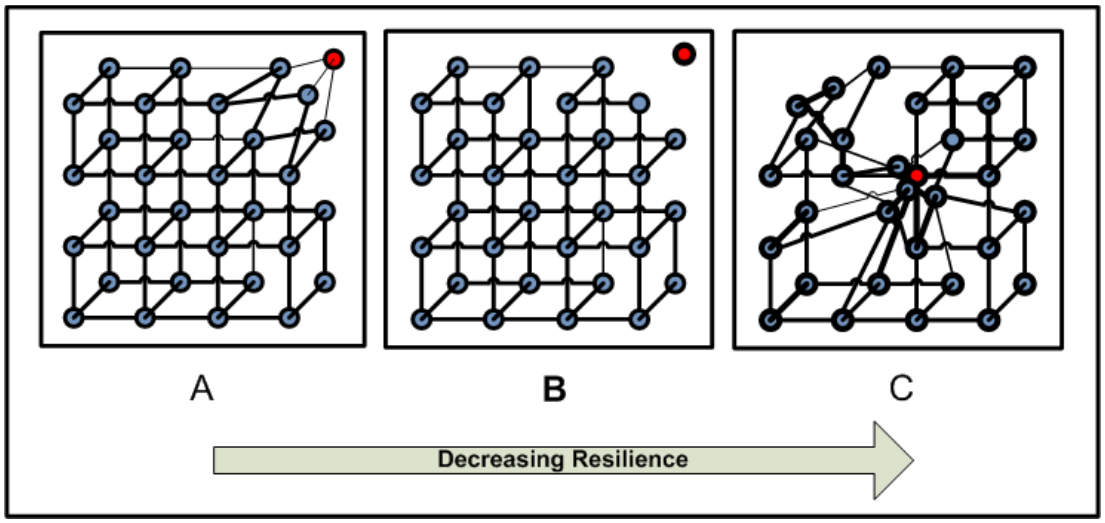


Figure A1.4: System Responses to Perturbation

If Resilience is the capability of a system to continue to operate (or recover) following a perturbation then the system in Figure A1.4A could be seen as more resilient than that in Figure A1.4B and that one more so than Figure A1.4C. The validity of this conclusion however depends upon the significance or importance of the system that is disturbed to the dimensions in which the overall system needs to operate post disturbance.

The Resilience Matrix Method

Traditional techniques for assessing Resilience use, for example, checklists and questions to establish what arrangements are in place within organisations for dealing with a prescribed list of Threats or potential perturbations i.e. they establish what the existing systems are and how well each of them will respond to a perturbation by challenging the system in a linear 1st order way. They then try to impose a simple overall model such as that shown in Figure A1.2 in order to interpret the results of this assessment.

The Resilience Matrix approach recognises that the real world is more complex and that under extreme perturbations reliance may be placed upon known dependencies or that these may naturally result in supportive practices that would not otherwise occur. With reference to Figure A1.4, this is equivalent to saying that the perturbation may itself lead to increases or decreases in some of the strengths of the connections between nodes.

The basic propositions behind the Resilience Matrix approach are that;

1. Organisations that -

i) have systems that make optimal use of their resources;
ii) have identified (either deliberately or through culture) their dependencies and opportunities for cross support following and incident;
iii) have established practices for addressing incidents,

are more likely to be able to adapt to severe perturbations and are therefore more likely to be Resilient.

2. Resilience is an emergent property of an Organisation and its presence is indicated by the principles embodied in proposition 1.

Establishing Dimensions

The Resilience Matrix approach firstly asks questions about the solution space that needs to be modelled, i.e. we first ask what the dimensions of the problem are. This question relates to the following types of question;

- What types of threat are of concern?
- What taxonomy of threat is best suited to analysing the organisation?
- Are some threats of more concern than others?
- What types of resources does the organisation have to respond to perturbations or what type of resources does it want to be able to use?
- What is important to the organisation, post disturbance?

Establishing Connections and Dependencies

For certain types of organisations it is possible to identify typical processes and linkages such that it is also possible to interrogate those systems in a way that draws out both the actual degree to which those dependencies have been accounted for and also how well the degree to which they could be beneficial following a perturbation has been accounted for. (i.e. with reference to Figure A1.4, how well are the linkages understood and have their potentially supportive benefits been recognised).

Typically these dependencies are identified in the Resilience Matrix as weighting factors between the chosen types of Threat and also between the questions used to identify how well the organisation can deal with the threat. Furthermore, dependencies between two items A and B (say) can be established as being either positive (i.e. a positive response to A supports the response to B, OR B supports A) or bi-supportive (A supports B AND B supports A). The way in which the dependency is modelled can be changed (i.e. the exact mathematical model can be changed). The models can be adjusted to exaggerate strengths or exaggerate weaknesses or to give a neutral (linear) adjustment.

Overall Resilience

Typically for the Resilience Matrix approach, the effectiveness of an organisation is scored in some way by an assessor (using responses to questions asked) and then the Resilience against each threat is shown as a matrix, one for each Threat, such as that shown in Figure A1.5. In this instance the chosen dimensions of importance to the organisation are how well it uses its Physical assets, its People and its Processes, and where these are targeted in terms of Prevention, Preparation and Protection[17]. It is implicit in this particular instance of the technique that a Resilient organisation will score well across the whole of the matrix's dimensions, i.e. that maximal use will be made of its Physical, People and Process assets at each stage of Prevention, Preparation and Protection.[18]

In the RM method these dependencies are used to scale the raw scores (i.e. those assigned by the assessors) to produce adjusted scores. The differences between these two scores and the distribution of the scores across the matrix is where the additional information and value is provided.

A resilient organisation would be expected to have matrices where the raw scores are consistently to the left (i.e. in the green area) and the adjusted scores would be close by. In the example of Figure A1.5, the populated effects matrix for Threat A indicates that the organisation's use of its people resource in the Preparation and Protection aspects of its business is perhaps not as resilient as might be indicated from a simple examination of its arrangements and that when dependencies are accounted for (perhaps on other aspects of the business's arrangements) its resilience is likely to be less good. The data from which these matrices are drawn can be identified by drilling down into the detailed responses to questions and the assessor's comments.

[17] These matrices are referred to as Effects Matrices. Although the dimensions of Physical, People etc shown in Figure A1.5 are those used in the model initially developed other dimensions could be equally well used. The dimensions of the effects matrices need to be orthogonal or as near orthogonal as practicable.

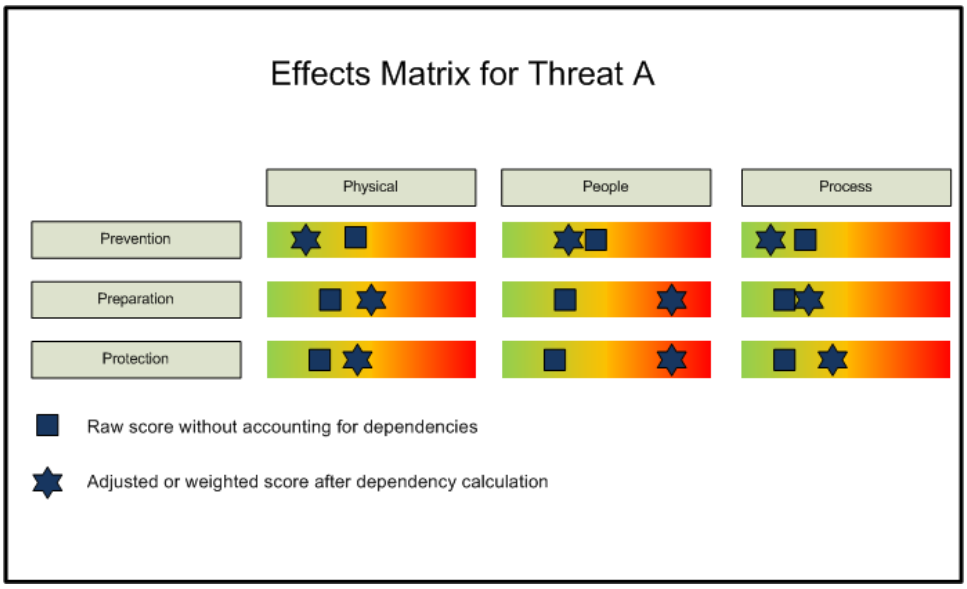


Figure A1.5: Effects Matrix Example

Overall Resilience is indicated by combining the results of the individual effects matrices; typically this takes into account an organisation's own perception of the importance of each threat to them (this is usually identified during initial discussions with the organisation and during the definition of the Threat Taxonomy). Again, the way in which the effects matrices are combined can be changed. The combination of the Effects Matrices is the Resilience Matrix.

References

Much of the background to the development of the Resilience Matrix was derived from the personal experience of the authors in managing organisations, in the delivery of services during the response and recovery phases of incidents, in the performance of physical vulnerability assessments and more generally risk assessments across a broad industry base. As such it represents original work.

There are parallels between the Resilience Matrix approach and methodologies such as Structured Equation Modelling (see for example, Principles and Practice of Structural Equation Modeling , Third Edition, Rex B. Kline August 2010), Attack Trees and Threat Trees (see http://en.wikipedia.org/wiki/Attack_tree) and to Building Vulnerability Assessment (see for example, FEMA 426 Reference Manual to mitigate Potential Terrorist Attacks against Buildings, 2003), among others, but it is different from each of these.

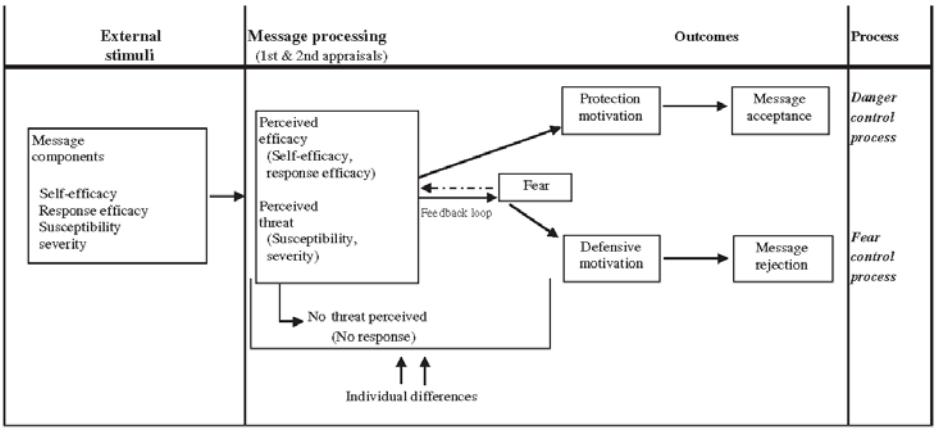
Resilience Matrices as used in child welfare (see for example, Using the resilience matrix to make sense of assessment information and evaluate children's needs, http://www.scotland.gov.uk/Topics/People/Young-People/childrensservices/girfec/Practitioners/ToolsResources/UsingResilienceMatrix) but these are less sophisticated than the approach outlined here and for a different purpose.

The use of Taxonomies is consistent with Luiijf, E. 2005/2006 “Threat Taxonomy for Critical Infrastructures and Critical Infrastructure Risk Aspects at EU-level”, the VITA Consortium. PASR-2004-004400. and Van de Voort, M., O'Brien K.A., Adnan, R. and Lorenzo, V., “Seacurity - Improving the Security of the Global Sea-Container Shipping System” RAND Europe 2003. ISBN: 0-8330-3440-5, among many others.

Adapted from earlier work by NH and DK, for presentation to the WP8 members at the initial kick-off meeting.

© CBRNE Ltd

II Annex II: Overview of the EPPM Model



Quotes from Maloney E.K et al

The EPPM postulates that motivation to take action in response to a fear appeal message depends solely on the degree to which the message increases perceptions of a threat; the type of action individuals take depends upon the degree of perceived efficacy to avert the threat. If a threat is perceived, the fear appeal message will be successful in motivating people to engage in the recommended protective behaviours if it successfully increases people's confidence that they are capable of engaging in the recommended behaviour, and that this behaviour is an effective means of avoiding the threat.

At its most basic, the model can be summed up as follows. First, under the condition that perceived threat is not high enough to produce fear, individuals will take no action in response to a fear appeal message. Second, if perceived threat is high enough to produce fear, when perceived efficacy is higher than perceived threat, individuals will engage in the response recommended by the fear appeal message; when perceived efficacy is lower than perceived threat, individuals will not engage in the response recommended by the fear appeal message, but instead will either avoid thoughts of the hazard altogether, or they will engage in behaviours that put them even more at risk of the hazard.

The authors specified that when individuals are in danger control (adaptive behaviour), high threat, high efficacy messages will be the most successful to reinforce behaviour used to avert the threat. Conversely, a negative discriminating value means that the individual is engaging in fear control (mal-adaptive behaviour). Under such conditions, Witte et al. (1996) recommended high efficacy messages with no mention of threat. This approach will increase the probability that individuals engaging in fear control processes will begin to perceive greater efficacy than threat, and will begin working to reduce their danger, rather than their fear, of the threat.

Another consideration for the criterion of openness is the degree to which a theory is compatible with other theories in the field. Cho and Salmon (2006) conducted research guided by Prochaska and DiClemente's (1983) stages of change model to demonstrate that individuals in different stages are likely to react to fear appeals differently. Results of this study suggested that the stages of change moderate the EPPM such that individuals in the early stages of change are likely to react to high threat fear appeals using fear control processes whereas those in later stages are likely to engage in danger control processes when confronted with a high threat fear appeal. Similarly, Hullett and Witte (2001) integrated the EPPM with the predications or uncertainty and anxiety management theory to predict intercultural adjustment.

III Annex III: The RM Model

AIII.1. The Simple Dependency Model

The general Model used for dependencies between two variables X and Y, where X and Y are both measured against the same scale interval (I) - e.g. from 0 to 5 - with the upper and lower bounds (X_U and X_L or Y_U and Y_L respectively) having the same meaning - e.g. 0 is poor and 5 is good – is as shown below;

If I_0 is the point on the interval I which is considered to be acceptable (e.g neither good nor poor) and X is scored at X_1 and Y is initially scored at Y_1 then the unweighted correction factor Correction Factor to Y_1 (CF say) is

$CF = (X_1-I_0) / (X_U-I_0)$

And the weighted correction factor CF_w is

$CF_w = W_f * CF$

Where W_f is a weighting factor that permits the adjustment of the strength of the interaction.

and

$$Y1' = Y1 + CF_w \qquad \textbf{...(1)}$$

Various forms of W_f can be specified depending upon whether the user wishes to emphasise the implied strengths or weaknesses. Some typical examples are shown below;

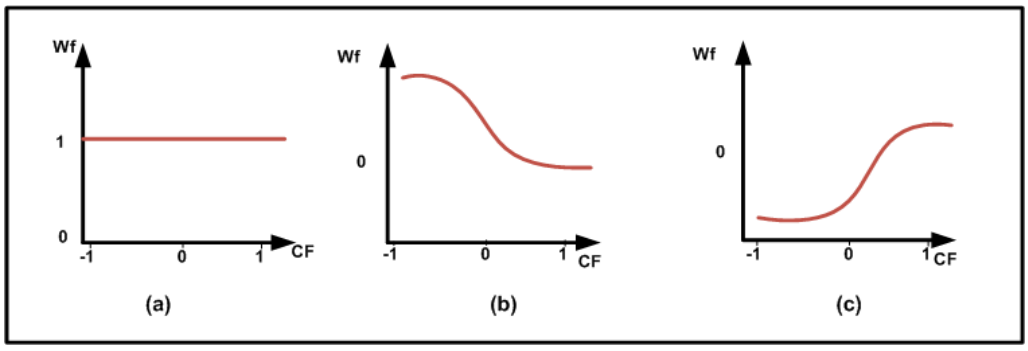


Figure AIII.1: Example Forms of Weighting Factor (Wf)

Notes to Figure AIII.1

Type (a) is used where the weighting factor is constant for all CFs – i.e. there is no relationship between CF and Wf

Type (b) is used where a large value of CF is considered to be disproportionately significant to a lower value.

Type (c) is used where a lower value of CF is considered to be disproportionately significant to a higher value.

The shapes of the curves and their intercepts with the axis can be adjusted.

AIII.2. Implementation of the EPPM Model

The following sections outline the equations and parameters used in the Model, which is also shown on Figure 11 in the main text.

AIII.2.1. Total Efficacy (TE)

TE is a combination of PoE and Trust in Responders (TiR). In the Model TE is simply evaluated as a linearly weighted average;

$$TE=(a.PoE +b.TiR) / (a+b) \quad \ldots (2)$$

Where a and b are simple weighting factors – the default values of a and b are unity such that the default value of TE is the simple average of PoE and TiR. The values of a and b are external to the Model and are entered as datum values by the user[19].

AIII.2.2. Fear

Fear is modelled as how much greater the perception of Threat is than the perception of Total Efficacy. This modelled as;

$$Fear = c.PoT / TE \quad \ldots (3)$$

Where c is a weighting factor, with a default value of unity. As noted above, this can be evaluated externally by the user and entered as a datum value.

AIII.2.3. Prediction of Behaviour

Figure 6 (The EPPM Relationship between behaviour and Perception of Threat and Efficacy) and the accompanying text is represented in the Model by the following equation;

IF *(Fear > TV* ***AND*** *TE> PoT)* ***THEN*** *Adaptive Behaviour will result* ***ELSE*** *Maladaptive Behaviour will result.* …***(4)***

Where 'no response' which occurs below the Fear threshold is considered to be Maladaptive.

More fully (substituting for Fear from (4), and TE from (3));

IF *(c(a+b).PoT/(a.PoE +b.TiR) >TV)* ***AND*** *[(a.PoE +b.TiR) / (a+b) > PoT]* ***THEN*** *Adaptive* ***ELSE*** *Maladaptive* …***(5)***

Given the simplicity of the model and the uncertainties surrounding the datum values, the main text argues that it is appropriate to modify Figure 6 to account for uncertainty about the region where behaviour changes from adaptive to maladaptive. This is done by the inclusion

[19] These could, for example, be estimated using techniques such as the Analytic Hierarchy Process (AHP – See Saaty and Peniwati) but this facility does not form part of the Model.

of an upper and a lower bound for the changeover region as shown in Figure 7. If a parameter called the Behaviour Index (BI) is introduced such that

BI=TE/PoT …**(6)**

Equation (5) is modified to

IF *(c(a+b).PoT/(a.PoE +b.TiR) >TV)* ***AND*** *[BI > BI_U]* ***THEN*** *Adaptive*

ELSE

IF *c((a+b).PoT/(a.PoE +b.TiR) >TV)* ***AND*** *[BI < BI_L]* ***THEN*** *Maladaptive*

ELSE

Uncertain …***(7)***

Where BI_U and BI_L are the upper and lower bounds of the uncertainty region.

AIII.2.4. Effectiveness of Communications

EoC is modelled as an independent variable that has an impact upon the values assigned to the other variables in isolation.

As shown in Figure 4 (Influence Diagram) and discussed in the main text, the influence of EoC is modelled using the simple dependency model described in Section AIII.1 and a weighting factor of the form of Figure AIII.1 (c) .

AIII.2.5. Variation of the Model with Timescales

Equation (6) is the general form of the Equation used in the Model to predict likely types of behaviour. However, it does not account for the variations in the relative importances of Factors between phases.

To allow for the modelling of these variations, the Model includes a set of values of the form shown below (

Table AIII.1) which allows the user to specify these relative importances[20]. As noted for the other variables and parameters, the exact datum values are left for the user to enter but they could be determined using Analytic Hierarchy Process (Saaty et al) or similar techniques. The default values for the importances are 0.25 (i.e. they sum to unity in each Phase).

[20] The alternative is to specify separate equations for each of the phases but it is considered that the timescale variable included in the Model is more intuitive and easier to understand.

Table AIII.1: Timescale Parameter Values

Factor	Relative Importance of Factor in the Phase		
	Pd	Ps	Pt
Perception of Threat (PoT)	α	ε	ρ
Trust in Responders (TiR)	β	ζ	ς
Perception of Efficacy (PoE)	γ	η	σ
Effectiveness of Communications (EoC)	δ	θ	Φ
Sum	1	1	1

The Scores assigned to each of the Factors in each of the Phases are multiplied by the importances in the table before evaluation of the equations (2), (3), (6) and (7) listed above.

AIII.2.6. Summation across KAE

After application of the Timescale Parameter Values to the initial scores, they are summed across the KAE dimensions so that an initial set of Behaviour Index values can be calculated.

These are calculated as a simple equally weighted sum, for each phase. But the weightings may be changed if desired by the user.

AIII.2.7. Overall Behaviour Effect Matrix

After application of the Phase Matrix, the adjustment for EoC and summation Across KAE, an overall Behaviour Effects Matrix of Behaviour Index values is calculated using the relationships set out in equations (2), (3), (6) and (7).