‘We’re Doomed!’ a Critical Assessment of Risk Framing Around Chemical and Biological Weapons in the Twenty-First Century

Giulio Maria Mancini and James Revill

Abstract ‘Risk’ and ‘risk assessment’ rhetoric has become pervasive in twenty-first century politics and policy discourses. Although a number of different meanings of ‘risk’ are evident, the concept frequently purports to be an objectively, quantifiable and rational process based on the likelihood and consequences of adverse events. However, using the example of chemical and biological weapons (CBW), this chapter argues that security-related risks are not always objectively analysable, let alone quantifiable. Moreover, the process of risk assessment is not always ‘rational’. This is, first, because efforts to quantify CBW-related risks normally require a body of data from which to inform assessments of probability when in fact there are limitations in data pertaining to the human dimension of CBW terrorism; with considerable gaps in knowledge of CBW incidents and a need for caution because of the emotive power of allegations of association with CBW. Second because the consequences of a CBW event are often informed by a wide range of variables, which make such weapons highly unpredictable. Third because conclusions that are drawn from any dataset often depend on the questions asked and the assumptions and values that ‘subjectify’ risk calculations, not least depending on if and how ‘expertise’ on risk is defined. This is not to say that risk assessment is not important, but that CBW risks might require a combination of a more rational phase of risk characterization with a more ‘subjective’ process of risk evaluation that acknowledges uncertainty of probabilistic modelling, deals with ambiguity, and opens-up the questions and assumptions that inform the risk assessment process to wider scrutiny and to the consideration of social and other factors.

The content of this chapter does not reflect the official opinion of the European Union. Responsibility for the information and views expressed in the chapter lies entirely with the author(s).

G.M. Mancini (✉)
Directorate-General of Migration and Home Affairs of the European Commission, Brussels, Belgium
e-mail: giulio.mancini@ec.europa.eu

J. Revill
Harvard Sussex Program, SPRU, University of Sussex, Brighton, UK
e-mail: j.revill@sussex.ac.uk

M. Martellini, A. Malizia (eds.), *Cyber and Chemical, Biological, Radiological, Nuclear, Explosives Challenges*, Terrorism, Security, and Computation,
DOI 10.1007/978-3-319-62108-1_15

Keywords Biological weapons • Chemical weapons • Risk • Uncertainty • Risk assessment • Bioterrorism • Chemical terrorism • Security • Threats • Scientific advice

1 Introduction

'Risk' and 'risk assessment' rhetoric has become pervasive in twenty-first century politics and policy discourses whether it is being applied to appraisals of science and technology, security, or their interactions.[1] For scholars such as Beck and Giddens the growing salience of risk is rooted in a tendency towards 'rational' decision-making processes in postmodern Western cultures. Indeed, although a number of different meanings of 'risk' are evident [2], the concept frequently purports to be an objectively, quantifiable and rational process based on the likelihood and consequences of adverse events [3, 4, 5]. This process is normally portrayed as undertaken by specialists and thereby presented as reflecting an expert analysis of the evidence resulting in reliable results. As such, risk is founded on positivist assumptions, with models derived from quantitative risk assessment applications in the nuclear and other engineering safety sectors [6], and looks at risks as largely an objectively observable, natural phenomenon. This approach to risk is used as a powerful tool in shaping policy options and validating policy decisions in relation to both science and security, as Williams notes "Risk has come to capture the minds of policy makers and public alike" [7].

However, using the example of chemical and biological weapons (CBW), this chapter argues that risks are not always objectively analysable, let alone quantifiable. Moreover, the process of risk assessment is not always 'rational', but frequently a combination of rationally comparable analysis *and* socially-mediated activity in which risks are socially constructed, and their "importance" subjectively evaluated or constructed. That is not to suggest that "anything goes" and risks are plucked out of the ether; but that the process of assessing risks is a human activity and informed by socially mediated assumptions, interests and (the limits of) knowledge. In this context, whilst some hazards will involve known risks that can be characterized in terms of probabilities and impacts, there will also be cases where there is uncertainty as to the 'likelihood' of a risk, ambiguity as to its potential consequence, and/or "ignorance, where we don't know what we don't know, and the possibility of surprise is ever-present" [8].

The chapter seeks to illustrate the relevance and limitations of risk assessment in relation to CBW through the application of critical thinking around risk assessment of emerging technologies – as developed by Andy Stirling and others- to the processes of looking at risks surrounding CBW in the twenty-first century. The first

[1] As Edmunds points out, the UK 2012 National Security Strategy (NSS) employs the term 'risk' no fewer than 545 times [1].

section of this chapter outlines some of the limitations in efforts to quantitatively model the risks posed by CBW, drawing attention to the limitations in available aggregate data, the challenges of determining consequences in a meaningful manner, the difficulty in effectively quantifying likelihood, and the limits of 'experts' in risk assessors. The chapter then elaborates on the social construction of security-related risks generally, and CBW risks specifically. The chapter then discusses possibility of amalgamating these two approaches to risk assessment, suggesting that an integrative, rather than exclusive, approach could be explored. In this model, the two approaches are not seen as mutually exclusive but complementary, with rational risk characterization and constructed risk evaluation forming the process of risk assessment. Essentially this would apply expert judgement through Bayesian techniques, and could be valuable in generating meaningful assessments of CBW risks which could be used to inform decisions around risk mitigation measures, even in the absence of a precise estimation of the baseline risk level. It should also be taken into account that the relative weight of the two framings within each assessment could vary. It is noted however that to maintain a minimal rational value, not all risks could be described with a sound characterization, largely depending on the level of uncertainty on likelihood estimation based on unknown factors related to the context or an intelligent threat,[2] even when impact can be relatively more clearly characterized basing on 'objective' characteristics of the hazards.

2 Risk in the Security Discourse

Over the course of the Cold War the process of conducting a threat assessment was relatively easy, as Dasse and Kessler state: "The enemy was known, its military capability was identified and its intentions understood – or so it was believed" [9]. Since the collapse of the Soviet Union and the easing of bipolar tensions, it is risks, rather than 'threats', which have grown in salience in both academic and policy discourses.

Indeed, in terms of the academic literature, risk has emerged as a nascent field of study within IR, influenced by the work of Beck on the concept of the risk society and the preoccupation in late modernity with the question of "how the risks and hazards systematically produced as part of modernisation can be prevented, minimised, dramatized, or channelled".[3] In terms of the policy discourse, Williams

[2] In the chapter "threat" is used to mean an intelligent (potential) perpetrator with intention to cause harm, i.e. a person or group of people, including a State or non-State actor.

[3] Beck's "risk society" is the post-industrial one that self-creates, through modernization, new risks that despite being created are less predictable than "classical", external risks. The "constellation in which new knowledge serves to transform unpredictable risks into calculable risks, but in the process it gives rise to new unpredictabilities, forcing us to reflect upon risks" is what Beck called "reflexivity of uncertainty" [10]. At the same time it is a society that no longer relies on the guidance of traditional or natural laws. The risk society uses decision-making tools such as risk assessment or risk mitigation. Furthermore, with the evolution from the "risk society" to the

suggested that "as a result [of 9-11] America became paranoid about possible security risks … transatlantic relations truly entered the age of risks" [7]. As much is evident in the praxeology of a number of Western institutions in the twenty-first century, NATO for example has shifted from looking at nation-State threats (in the form of the Soviet Union) to "security challenges and risks", with the Alliance's 1991 strategic concept explicitly stating "[i]n contrast with the predominant threat of the past, the risks to Allied security that remain are multi-faceted in nature and multi-directional" [7]. In Europe, discourses largely dominated by specific conceptualizations of "threats" have evolved to integrate images of security risks. The European Security Strategy suggested that threats faced by Europe were "more diverse, less visible and less predictable"; and that threats, such as terrorism and the proliferation of WMD, put Europe and Europeans "at risk" [11]. Later, the EU Internal Security Strategy considered "threats" (terrorism, organised crime, cybercrime, as well as adverse events of a largely safety nature but with security implications) and "challenges" with the potential to generate risks for the Union and its citizens. The 2015 European Agenda on Security [12] employs risk framing in relation to border security, radicalisation, and disasters.[4]

2.1 Quantitative Security Risk Assessment?

Indeed, risk language and 'risk assessment' have become a preoccupation amongst policy makers seeking to respond to phenomena that could lead to adverse events, and which must be identified and measured for probability and consequence. In this approach to risk assessment, a risk can be considered as a function of the likelihood and consequences of a specific adverse event associated with specific (natural) hazards and/or (human) threats [3, 13, 14, 15]. The model of risk identification and characterization by Kaplan and Garrick is based on a trio of "fundamental questions", including: what could go wrong? How likely is it that that will happen? If it does happen, what are the consequences? In this sense, the first question relates to risk identification, and is a creative activity of exploring possible undesirable

"world risk society", Beck introduced a series of innovations specific for the international nature of risk society in the twenty-first century, including risk as (globalized) anticipated catastrophe and, especially relevant for the security discourse, transnational terrorism as an entire new category of global risk subverting calculations with "intention" in the place of "chance". A type of global risk that is even more peculiar when coupled with cutting-edge technologies that are continuing, as predicted 20 years earlier, to contribute to uncertainty. "Those responsible for well-intentioned research and technological development will in future have to do more than offer public assurances of the social utility and the minimal 'residual risk' of their activity. Instead, in the future the risk assessments of such technological and scientific developments will have to take into account, literally, intention as well as chance, the terrorist threats and the conceivable malicious uses as well as dangerous side effects" [10].

[4] As a mere indication, the word "risk" was used 4 times in the 2003 European Security Strategy, 15 times in the 2010 Internal Security Strategy, and 31 times in the 2015 European Agenda on Security.

scenarios, [13] that would be consistent with other work that has sought to apply the same framework to chemical, biological and other risks [16, 17, 18]. The second and third questions in the model would correspond to risk characterization, looking respectively to likelihood and impact.

Purportedly "scientific approaches" to risk all seem to share this vision. Although scholars such as Stirling associate the event itself with its impact, in other explanations the "adverse event" is distinguished from the "impact/consequences" it can have. As Kates and Kasperson note, "risks are measures of the likelihood of specific hazardous events leading to certain adverse consequences" [4]. A risk assessment process would start by identifying all the reasonably foreseeable possible adverse events, in order to answer the question "what could go wrong?" [3] This is the process of risk identification and would be followed by a process of risk characterization in which an analysis would be undertaken of all the factors that may influence the likelihood and/or consequences of the identified adverse events. Popular ways to perform this analysis include assigning values to the various factors and Multi-Criteria Decision Analysis (MCDA), which characterizes, relatively, various risks factors using qualitative definitions.[5]

Such purportedly "rational" or "objective" risk framings have been applied to assess a number of natural hazards as well as security-related risks associated with the deliberate misuse of science and technology by actors (person, group or nation-State) intending to cause harm, including using chemical and biological weapons. For example risk characterization related to chemical and biological weapons would include an analysis of factors pertaining to the nature, mode and context of dissemination [5]; the nature of the target [19]; and the motives [20], intensity [21], known values and beliefs [22], skills and objectives of possible perpetrators.[6]

The appeal of such approach is, in part, that it purports to be founded upon rational, 'sound science', 'expert analysis' or, in the case of the UK, "Subject-matter experts, analysts and intelligence specialists" – described by the then Prime Minister David Cameron as "all the relevant people" – who frequently serve as the definitive authority for decisions taken; and in part because the process serves to reduce complex political problems into 'single "definitive" technical or expert interpretations' upon which policy makers can act – and be seen to be acting – in a 'rational' manner [23].

Such a practice is evident in the development of the UK National Security Strategy which formed the "first ever National Security Risk Assessment (NSRA)" in which the UK's National Security Council identified: "the full range of existing and potential risks to our national security which might materialise over a five and 20 year horizon. All potential risks of sufficient scale or impact … were assessed, based on their relative likelihood and relative impact." Upon the unveiling of the National Security

[5] Methods are used to inform decisions in situations of limited and evolving knowledge from multiple sources. MDCA methods are based on weighted sum algorithms of multiple factors evaluated against each other [18].

[6] Such objectives include can include killing but also economic sabotage, media attention and prestige, ıncapacitation, crime, destabilization, disruption, deterrence and denial.

Strategy in the UK, Cameron suggested, "We have had a proper process-a national security process" and that: "the review has been very different from those that went before it. It has considered all elements of national security, home and abroad… It has been led from the top with all the relevant people around the table" [23].

In some respects the NSS was different in the sense that it recognizes the hazards and dangers posed by environmental change and new wars as well as the limitations of military means alone in responding to such challenges. Yet in other respects the National Security Strategy, continued to pursue an approach based on national security which used the language and practice of risk to mask the socially mediated assumptions, interests and (the limits of) organisational knowledge that were at play in the determination of the UK's National Security Risks [24].

3 Challenges with CBW-Related Risks Assessment

Looking at risks and trying to make sense of hazards is no bad thing. One of the issues with the approach to risk framing outlined above however is that there are significant limits as to how "true" and "reliable" the results of the seemingly rational analysis are; and by implication, the appropriateness of ensuing risk mitigation measures. Risk framing is often associated with 'sound science' and terms such as rational, objective, quantitative, probabilistic. Yet while these approach share a vision of "representing reality" they may actually mean different things and reflect different levels of confidence and certainty in part because of the limits of data sets of relevance to CBW and in part because of the limits of 'experts'.

3.1 Limits of Datasets

Indeed, efforts to quantify CBW-related risks normally require a body of data from which to inform assessments. This is relatively straight forward in areas such as engineering failures or car accidents where there is an aggregate body of data on events from which to inform probabilities; but even then data is often simplified, masking complexity and a certain amount of uncertainty (or ambiguity) as different and complex parameters are reduced and aggregated [25]. With new complex systems or little-known chemical or biological agents, this becomes even more difficult as there is frequently going to be a lack of aggregate data from which to meaningfully determine probabilities. In the absence of sufficient data risk assessment can become vulnerable to whimsy.

This is compounded by limitations in data pertaining to the human dimension of CBW terrorism, specifically information about motives, means and objectives of different groups. There have been several datasets of such information created, including public datasets such as the Global Terrorism Database (GTD) developed by the START consortium and various chronologies of the use of

CBW. Such datasets are useful sources of information on past cases of chemical and biological weapons adoption or use. However, a number of issues remain with these and indeed any dataset pertaining to CBW.

First, there remain considerable variations in definitions & assumptions surrounding CBW and CBW-related incidents. For instance, what is a chemical or biological weapon? Do such weapons include only pathogens and toxins, and only when explicitly optimized for a hostile purpose, or do they include any chemical compound or biological organisms that is used to cause some sort of harm? Are "munching insects" such as Thrips Palmi, or invasive species that can cause economical damage, biological weapons? Does an attack on chemical facilities, or the throwing of acid at people, constitute chemical weapons? An overly broad a definition of chemical and biological weapons can render the term meaningless. An overly narrow definition can also be unhelpful as it skews the focus around only those more significant incidents which in themselves may be anomalies in how chemical or biological weapons have been adopted or used.

The second factor is that there remain considerable gaps in knowledge of CBW incidents; more comprehensive datasets, such as the GTD or the POICN database, seeking to capture a broad range of incidents have acknowledged as much, with significant percentages of certain variables, including on inter alia the perpetrators, the agents used, the motivations and indeed the validity of some reported cases, omitted. Datasets also frequently omit or overlook seemingly validated events that are perhaps useful, but fall outside of key criterion or time frames. For example the use of CBW against animals or plants as was the case with the Mau Mau in 1950 [26] and the reported threat to use biological agents against crops by the Tamil Tigers circa 1982 [27], are not always included in datasets, despite providing useful illustrative examples of how CBW could be used.

Third, there is a need for caution in some of the cases included. Non-events or naturally occurring phenomenon have been mistaken for – or deliberately misrepresented as – chemical and biological weapons use. Fourth there is a need for caution in the reliability of datasets that are largely based on past data as past events are not necessarily useful in predict future ones, particularly as biotechnology evolves and chemical and biological sciences converge. Whilst scenario building exercises can be useful in this regard, there are challenges with departing from known events and moving from facts to fictions in risk appraisal.

Fifth, and yet perhaps most significant, is that there is a need for caution with data on CBW-related adoption because of the emotive power of allegations of association with CBW. Some reported incidents of CBW use in criminal or terrorist contexts are just that – reports which are unvalidated and in some cases unlikely, but nonetheless serve the interest of powerful actors as they can be used to demonise individuals, groups or countries. In this regard it is worth noting Robinson's remark that "Accusations of association with [CBW] have for centuries, even millennia, been used by well-intentioned as well as unscrupulous people to vilify enemies and to calumniate rivals" [28]. This presents major issues for those seeking to undertake in objective risk assessment drawing on past data, as it requires careful separation and a degree of judgment in separating reality from powerful 'alternative facts'.

3.2 Limits of Quantifying Likelihood

Such factors necessitate that the aggregate data required to quantify the 'likelihood' of chemical and biological weapons can prove difficult to acquire and potentially misleading. Even basic calculations of the frequency of CBW events become highly contested (and contestable) depending on definitions and data selected: for example, the inclusion of failed cases of agro-bioterrorism and the use of acid as a weapon, will generate very different frequency calculations to a data-set focusing on successful lethal biological attacks against humans. Even in circumstances where there is agreement on definitions and criterion, there will remain uncertainty over certain cases in open source datasets, and most likely closed, classified information on cases too. To some extent, uncertainty could be acknowledged and mitigated by the integration of uncertainty factor into calculations of frequencies, however this potentially creates another potentially subjective factor in the calculation.

3.3 Limits of Quantifying Consequences

Yet it is not only the likelihood of risks which are difficult to assess, so too are the consequences of a CBW event. CBW are frequently capricious weapons and vulnerable to factors such as *inter alia*, atmospheric stability, convective forces, ground cover (mist or fog), mechanical forces (terrain roughness) and rainout [29]; not to mention the public health, immunity and detection and response capacity of the target population factors. Such factors mean that the impact of the use of an agent can vary by orders of magnitude depending on the environment. Such issues of predictability are more than academic musing, but had a bearing on the selection of agents in Cold War CBW programmes.

For example, Anthrax is arguably the archetypal biological weapon and has been considered in many state biological weapons programs in part because of the relative hardiness of the spores and the considerable knowledge of the agent. Yet for all the data on the characterisation of anthrax, the extrapolation of lethality data from animal test subjects to humans proved difficult in the case of the US program. This was compounded by the apparent variance in estimates of LD50 of Anthrax with LD50 calculations for humans ranging from 1000 to 6000 spores. As such, Anthrax was standardised not for use in strategic weapons, but as a weapon for use by special forces (the M2 munition). The US had greater success with the Tularemia based M210 Biological Warhead for the MGM-29 Sergeant Missile, however as Kirby has illustrated, the limitations on the weapon were considerable, with logistical factors, such as the half-life decay of the agent, and environmental conditions spelling the difference between mass effect, and negligible effect [29].

One could argue that highly contagious biological agents could mitigate such logistical and environmental difficulties. Yet such weapons too are limited in their predictability. As has been noted "epidemics involve two dynamics; the first is the

course of the disease in the individual, and is biomedical. The second is the spatial contact process among individuals, and is social". The latter in particular makes predictability difficult "random effects can be dramatic, spelling the difference between large-scale epidemics and abortive ones that never take off" [30].

Chemical weapons provide relatively more predictable effects, yet chemical weapons too are influenced by environmental factors. As Carus has remarked:

> Chemical agents are highly unpredictable. They are very sensitive to weather conditions, including temperature, wind, and atmospheric pressure. Even with high quality weather forecasting it is difficult to ascertain accurately the specific conditions that will exist at a particular place. [31]

For example, Botulin ranks amongst the most lethal agents know to humans and has been considered in several state chemical (and biological) weapons programs. However, devoid of complex stabilisation processes, botulin was highly unpredictable with "[e]xtremes of temperature and humidity will degrade the toxin … Depending on the weather, aerosolized toxin has been estimated to decay at between less than 1 % to 4 % per minute".

The point is not that consequences can or should somehow be ignored in risk assessment. Nor is this to suggest that the consequences cannot be estimated under certain conditions. However, any attempt to neatly quantify the consequences of biological and to a lesser extent chemical weapons needs to be heavily caveated; and for all the advances in science and technology, precisely predicting the outcome of CBW attacks is "the prerogative only of the ignorant" [32].

3.4 Limits of "Expertise"

The realist approach to risk typically places much greater importance on "experts", a category delineated from "lay people"; with the former regarded as neutral actors employing an objective and replicable measurement of risk, and the latter often viewed as unable to correctly assess risk and led by whimsy. As much is implicit in what Erik Millstone has termed the 'technocratic model' of science advice in policy making that has served as the dominant narrative for much of the last 60 years [33]. In this model, "policy is based (only) on sound science", with technocracy implying "that public administration by impartial experts should replace governance by those with particular interests because only the experts possess the relevant understanding and knowledge" [33]. The underpinning assumption of this model is that "the relevant scientific knowledge is objective, politically neutral, readily available and sufficient" [33]. However, as Millstone and others have indicated, knowledge is often "incomplete, uncertain or equivocal"; and experts are not always impartial and immune to bias [33] (Fig. 1).

Indeed, the technocratic model of scientific advice to policy makers has begun to weaken in several issue-areas over the last couple of decades, in part because of the recognition of uncertainty and in part because of the rise of freedom of infor-

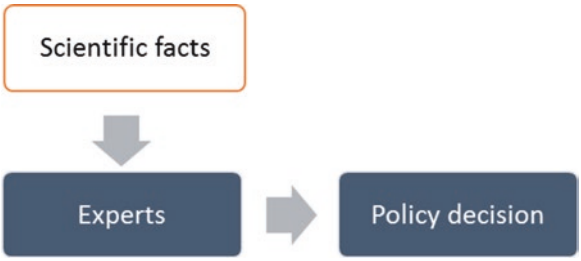

Fig. 1 The technocratic model: 'policy is based (only) on sound science' (Adapted from Millstone 2009)

Fig. 2 A 'decisionist' model of science advice for policy makers (Adapted from Millstone 2009)

mation act requests. Certainly, in relation to the former, uncertainty is increasingly recognised in scientific assessments. For example US legislation related to food and drugs has "acknowledged scientific uncertainties and provided federal agencies such as the US Food and Drug Administration (FDA) with guidance on how they should interpret and respond to such uncertainties" [33]; similarly European bodies, such as the European Food Safety Authority (EFSA), have recognised that "Methodologies for integrating (weighing) evidence and assessing uncertainties are of utmost importance to ensure that scientific assessments are transparent, robust and fit for purpose to support decision-makers" [34]. Regarding the latter, Millstone suggest that freedom of information request related to the use of expert advice over GMO decisions, "entailed the disclosure of sufficient information on the science used to support policy to reveal that the science was often profoundly uncertain" [33].

The experience with food safety governance, is clearly different to that of CBW where the evidence base for risk assessment is frequently secreted and sensitive. Nonetheless, the acknowledgement and efforts to "develop a more sophisticated understanding of scientific uncertainty and its treatment" [35], along with experiences, such as the Iraq War (Chilcot) Inquiry and the Butler report in the UK, and WikiLeaks to some extent diminished faith in models of expert advice to policy makers relying exclusively on technocratic or scientific input, unmediated by social, political, ethical, economic and cultural factors. Moreover, it highlights how "risk are routinely predicated on assumptions, which inform the scientific deliberations, but which are not themselves scientific" but rather "hybrid judgements" that draw on scientific as well "normative considerations" [33] (Fig. 2).

4 From Technocratic to 'Decisionist'

As a result of the limitations in technocratic models of risk assessment in other issues areas, the provision of scientific advice shift from a technocratic to a two stage "decisionist model" in which scientific risk assessment was followed by non-scientific process of risk management.

Similar two-phase approaches have been popularised in the US through work of the National Research Council, such as on *Risk Assessment in the Federal Government: Managing the Process.* This model proved highly influential and has been applied by a number of organisations. As Millstone notes "deliberate decisions have been taken to create separate pairs of institutions, with one of the pair labelled as responsible for 'risk assessment', having a scientific mandate, and the other labelled as having responsibility for 'risk management' policy decisions" [33].

More recently an advanced version of this form of risk assessment has been undertaken for Gain of Function research using models draw from the nuclear sector [36] but populated by data on lab incidents and epidemiological data that were passed to NSABB to inform decisions [37] in a manner consistent with the decisionist or "red book" model.

One of the problem with both the decisionist (or "red book") and technocratic models is portrayal of "scientific representations of risk" as if they were entirely free from all social, economic or policy influence, when in fact it is widely now understood as "representations of risk are inevitably hybrid judgements, dependent on both scientific and normative considerations". Several scholars have demonstrated this, illustrating how expert can reach starkly different conclusions from the same body of data because of the different framing assumptions, or as Millstone notes "often because they are asking and answering different questions" [33]. Looking beyond the Gryphon report, the more recent controversy over Gain of Function study also perhaps illustrates how different framings can lead to different conclusions with security and scientific communities – whilst not monolithic – tending towards different conclusion. Indeed, Ron Fouchier, a virologist at the centre of the Gain of Function controversy has remarked "Even if they could be quantified, the weighing of risks and benefits will be a personal (subjective) issue" [37].

5 Towards a Co-evolutionary Model

Millstones' remedy for the limitations of the technocratic and decisionist models, is the notion of a "co-evolutionary model" of science in policy making. The model does not exclude scientific consideration in the form of expert risk assessment, but seeks to contextualise this, by preceding such expert risk assessment with a more explicit process of outlining a risk assessment policy in which socio-economic consideration are used to inform the framing assumptions that feed into expert

Fig. 3 A co-evolutionary model: reciprocal links between science and policy (Adapted from Millstone 2009)

risk assessment. This could include information such the historical incidents of CBW use which informed assumptions and specifics of the questions asked of assessors. Moreover, rather than the scientifically informed expert risk assessment directly determining risk management policies, policy decision making (risk management) is explicitly informed by technical as well as economical, and political considerations. Put otherwise, "scientific risk assessments are… sandwiched between up-stream framing considerations and down-stream interpretative judgements" [33] (Fig. 3).

6 …And CBW Risk Assessment?

There are significant differences between appraisal of risks related to climate change or GMOs on the one hand, and the risks of chemical and biological weapons on the other. Whilst all these topics are clearly political sensitive, with Climate change and GMOs the body of evidence can largely be made available for external actors to scrutinise. In the case of CBW, much of the information is likely to be security sensitive. This makes it much more difficult to open up CBW risk assessment to form a more discursive, participatory process as has been proposed for other issue areas.

Nonetheless this does not discount the possibility of alternative approaches to addressing CBW related risk that acknowledge that the process of risk identification and characterization are, in part, socially constructed; a notion advanced variously, on risk in general, by Beck, Giddens and Douglas. Under such as model quantitative and qualitative approaches could co-exist combining a more rational phase of risk characterization with a more 'subjective' process of risk evaluation within a ("co-evolutionary") risk assessment process.

In this model the weighting of rational and subjective elements could be determined by the levels of uncertainty and the nature of the risks addressed. In circumstances of increasing uncertainty the employment of qualitative measures could be weighted more heavily; in cases where risks were better characterised quantitative approaches could be given greater weight and the "representations of risks are portrayed as hybrid

judgements constructed out of both scientific and non-scientific considerations" [33]. In both cases, reasonably foreseeable risks could be somehow ranked, as studies by Marris et al. indicate, the integration of constructivist or even relativist considerations into objective or quantitative risk assessments doesn't preclude that risks can be categorized and ranked according to a number of factors [38].

However such a process needs to acknowledge "the prospect of radical surprise" or "unknown unknowns" which evade risk identification process – and which obviously cannot be ranked – to avoid generating a false sense of security. Moreover, in seeking to rank risks, assessors would need to acknowledge that "probabilistic reasoning under uncertainty cannot yield a single objectively aggregate value" and open up the framings that inform the process of risk assessment in circumstances where the consequences of an adverse event may be problematic and ambiguous [39]. The latter requires articulating the specific details of the questions that were asked of risk assessors. For example, articulating who (the EU, the Member State, military forces, citizens) or what (human health, welfare, economy, livestock) is at risk; from what (non-state actors, terrorist, states, criminals). Such a step would open-up the process and subject previously hidden assumptions, values and beliefs to reasonable scrutiny rather than black boxing the framings employed. Whilst governments can legitimately withhold details of the data used to inform risk assessment process, there are less grounds for withholding details of the *questions* put to risk assessors and some details of the information that informs assumptions of risk assessors *can* be synthesised and made public.

From the perspective of observers of the risk assessment process and results, it will important to recognise that difficult decisions need to be taken over which risk mitigations measures to pursue to deal with CBW risks in the absence of complete information pertaining to the initial likelihood or consequences of an event. Put otherwise, 'paralysis by analysis' is not an option for policy makers that need to respond – and be seen to respond – to risks, particular for what Slovic refers to as 'dread' risks. It is also needs to be acknowledged that certain CBW mitigations measures can and have lower likelihood and/or even impact in the absence of complete information. Indeed, even when risk assessment is cynically seen as an instrumental tool to justify certain mitigation measures, it does not necessarily mean that the measures themselves are not helpful in mitigating the given risk, also when the exact initial baseline is not known or reliable [40, 41].

7 Conclusions

Risk assessment has become increasingly important in relation to chemical and biological weapons in the twenty-first century with greater emphasis placed on efforts to objectively calculate the likelihood and consequences of adverse CBW events. However, whilst discussion around CBW related risk is important, it needs to be recognised that risks – including CBW risks – are not always objectively analysable, let alone quantifiable and that risk assessment is not always

'rational', but frequently a combination of rationally comparable analysis *and* socially-mediated activity in which risks are socially constructed, and their "importance" subjectively evaluated or constructed.

This is not an argument for giving up on CBW risks assessment. However it does suggest that decision-makers need to be aware of the limits of quantitative (only) risk assessment; and those involved in risk assessment need to be more forthcoming in the uncertainty of probabilistic reasoning and acknowledge that the consequences of adverse CBW-related event may be problematic and ambiguous. It also needs to be recognised that there is a need for caution in claims that all risks have been assessed, a notion that can leave us ever more vulnerable to surprise from unknown unknowns.

References

1. Edmunds, T.: British civil-military relations and the problem of risk. Int. Aff. 88, 265–282 (2012)
2. Slovic, P., Weber, E.U.: Perception of Risk Posed by Extreme Events. (2002)
3. Kaplan, S., Garrick, B.J.: On The Quantitative Definition of Risk. Risk Anal. 1, (1981)
4. Kates, R.W., Kasperson, J.X.: Comparative risk analysis of technological hazards (A Review). Proc. - Natl. Acad. Sci. USA. 80, 7027–7038 (1983)
5. Hohenemser, C., Kates, R.W., Slovic, P.: The Nature of Technological Hazard. Science (80-.). 220, 378–384 (1983)
6. Starr, C.: Social Benefit versus Technological Risk. Science (80-.). 165, (1969)1232-8.
7. Williams, M.J.: NATO, Security and Risk Management: From Kosovo to Khandahar. Taylor & Francis (2008)
8. Leach, M., Scoones, I., Stirling, A.: Pathways to Sustainability: an overview of the STEPS Centre approach. (2007)
9. Christopher Daase, Kessler, O.: Knowns and Unknowns in the `War on Terror': Uncertainty and the Political Construction of Danger. Secur. Dialogue. 38, (2007)
10. Beck, U.: World at Risk. Polity (2013)
11. Council of the European Union: European Security Strategy., Brussels (2003)
12. European Commission: The European Agenda on Security., Strasbourg (2015)
13. Kaplan, S.: The Words of Risk Analysis. Risk Anlaysis. 17, (1997)
14. Garrick, B.J.: Quantifying and Controlling Catastrophic Risks. Elsevier Inc. (2009)
15. George E. Apostolakis: How Useful Is Quantitative Risk Assessment? Risk Anal. 24, (2004)
16. World Health Organization: Laboratory biosafety manual Third edition. (2004)
17. Gormley, Á., Pollard, S., Rocks, S., Black, E.: Guidelines for Environmental Risk Assessment and Management - Green Leaves III. (2011)
18. Caskey, S., Gaudioso, J., Salerno, R., Wagener, S., Risi, G., Kozlovac, J., Halkjær-knudsen, V., Prat, E.: Biosafety Risk Assessment Methodology. (2010).
19. Isukapalli, S.S., Lioy, P.J., Georgopoulos, P.G.: Mechanistic Modeling of Emergency Events : Assessing the Impact of Hypothetical Releases of Anthrax. Risk Anal. 28, (2008)
20. Brown, G.G., Cox, L.A.: How probabilistic risk assessment can mislead terrorism risk analysts. Risk Anal. 31, (2011)
21. Depoy, J., Phelan, J., Sholander, P., Smith, B., Varnado, G.B., Wyss, G.: Risk assessment for physical and cyber attacks on critical infrastructures. MILCOM 2005 - 2005 IEEE Mil. Commun. Conf. 3, 1961–1969 (2005)
22. Keeney, G.L., Winterfeldt, D. Von: Identifying and Structuring the Objectives of Terrorists. Risk Anal. 30, 1803–1816 (2010)

23. Hansard (UK): Strategic Defence and Security Review. In: Oral Answers to Questions, Tuesday 19 October. Hansard, London (2010)
24. Ritchie, N.: Rethinking security : a critical analysis of the Strategic Defence and Security Review. Int. Aff. 87, 355–376 (2011)
25. Stirling, A.: Chapter 2: Risk, uncertainty and precaution: some instrumental implications from the social sciences. In: Berkhout, F., Leach, M., and Scoones, I. (eds.) Negotiating Environmental Change New Perspectives from Social Science. Elgar
26. Yeh, J.-Y., Park, J.-Y., Cho, Y.S., Cho, I.-S.: Animal Biowarfare Research: Historical Perspective and Potential Future Attacks. Zoonoses Public Health. 59, 1–9 (2012)
27. Carus, W.S.: Bioterrorism and Biocrimes - The Illicit Use of Biological Agents Since 1900. (February 2001 revision)., Washington, D.C. (2001)
28. Robinson, J.P.P.: Alleged Use of Chemical Weapons in Syria, HSPOP 4. (2013)
29. Kirby, R.D.: The Sergeant: A Biological Missile. Eximdyne (2014)
30. Epstein, J., Cummings, D., Chakravarty, S.: Toward a containment strategy for smallpox bioterror: an individual-based computational approach. Gener. Soc. Sci. Stud. agent-based Comput. Model. (2006)
31. Carus, W.S.: Chemical weapons in the Middle East. Policy Focus. 15 pp (1988)
32. SIPRI: The Prevention of CBW. The Problem of Chemical and Biological Warfare: Volume V. SIPRI, in association with Oxford University Press (1971).
33. Millstone, E.: Science, risk and governance: Radical rhetorics and the realities of reform in food safety governance. Res. Policy. (2009)
34. Dorne, J.L.C.M., Bottex, B., Merten, C., Germini, A., Georgiadis, N., Aiassa, E., Martino, L., Rhomberg, L., Clewell, H.J., Greiner, M., Suter, G.W., Whelan, M., Hart, A.D.M., Knight, D., Agarwal, P., Younes, M., Alexander, J., Hardy, A.R.: Weighing evidence and assessing uncertainties. Eur. Food Saf. Auth. J. 14, 1–13 (2016)
35. Parliamentary Office of Science and Technology: Handling Uncertainty in Scientific Evidence. (2004)
36. Gryphon Scientific: Risk and Benefit Analysis of Gain of Function Research: Final Report—April 2016. (2015)
37. Reardon, S.: US plan to assess risky disease research takes shape. Nature. October, (2015)
38. Marris, C., Langford, I.H., Riordanz, T.O.: A Quantitative Test of the Cultural Theory of Risk Perceptions: Comparison with the Psychometric Paradigm. Risk Anal. 18, (1998)
39. Stirling, A.: Opening Up the Politics of Knowledge and Power in Bioscience. PLoS Biol. 10, (2012)
40. Comıté Européen De Normalısatıon (CEN): CEN Workshop Agreement - Laboratory biorisk management, Brussels (2011)
41. Caskey, S. and Sevilla-Reys, E.E. IN: Caskey, S., Gaudioso, J., Salerno, R., Wagener, S., Risi, G., Kozlovac, J., Halkjær-knudsen, V., Prat, E.: Biosafety Risk Assessment Methodology. (2010)