COLLECTED ESSAYS

CBRN risks in maritime and land containers transport

Edit by Valerio Cartocci, Matteo Gerlini, Anna Giovanetti

Italian National Agency for New Technologies,
Energy and Sustainable Economic Development

CBRN risks in maritime and land containers transport

Collected essays

Edited by Valerio Cartocci, Matteo Gerlini, Anna Giovanetti

2017 ENEA
National Agency for New Technologies, Energy and
Sustainable Economic Development

ISBN: 978-88-8286-347-0

Copy editing: Giuliano Ghisu

Cover design: Cristina Lanari

Printing: Laboratorio Tecnografico ENEA – Frascati

Table of contents

Foreword 5

Facilitating the Interface between Science and Policy Regarding CBRN 7
Janet K. Benini

The Main Problems of Public Understanding of CBRN 11
(Chemical, Biological, Radiological, Nuclear) Risks
Sylwia Mrozowska

Using Container Status Messages to improve targeting of 17
high-risk cargo containers
Aris Tsois, Jose Antonio Cotelo Lema, Michail Makridis, Enrico Checchi

Swedish Experiences regarding CBRN Risks in Maritime and Land 23
Container Transport – with focus on the Radiological (R) and
Nuclear (N) aspect
Helmuth Zika

CBRN Transport System Security Decontamination Strategies and Solution 29
Renato Bonora, Stefano Mioriotti

Addressing Bio and Chemical Risk 37
Anna Giovanetti

Foreword

Containers could be compared to barcode as a material tool of globalization's process. Answering to standardization's requirements that every industrial and commercial economy met, containers became the basic unity of delivering in any international goods markets. The movement of containers has revolutionized the world of logistics and has reduced the cost of transport for every kind of goods. Over 11 million containers arrive in USA alone, every year. But the movement of containers in the seaports entails the risks of illicit trafficking as well as CBRN threats and malicious acts. The sealed nature of the containers means that there is a growing appreciation for the risk of prohibited or dangerous material being shipped around the world as contraband items.

The CBRN threats need globally dedicated procedures of response, as well as the collection and filtering of shipping data to identify high risk sources and separate intelligence. For the future, the aim in this field must remain increasing volumes and variety of screening. If in the past, the focus may have been on explosive materials, now there is growing interest in nuclear and bio-terrorist threats. Whilst there is recognition that the authorities have neither the technology nor the resources to screen every container for every kind of known threat, this remains the final aim for a comprehensive container security.

Moreover, the screening methods with existing testing (chemical, biological, radiological) (i.e. large scale X-ray, gamma ray machines and radiation detection devices) still need for new screening methodologies (i.e. non-intrusive inspection). According to the pilot study of 2002 (Detecting Nuclear Material in International Container Shipping: Criteria for Secure Systems. Stanford Study Group Center for International Security and Cooperation Stanford University), the detection of special nuclear material was the main target for container screening. So, while the RN detection is still the advanced sector of CBRN detection's technologies, the pursuit of a reactive component that can track data for epidemic trails (Ebola, Anthrax, etc.) would be a good research in order to address bio risk in container exchange, in particular for aliments transportation.

With the aim of discussing these topics, an interdisciplinary approach is needed. For these reasons the editors will convey articled of experts from the various fields involved in the technics and in the related international policies. Detection technologies, regulatory frameworks, emerging threats, and many other topics shall be discussed to approach the movement of containers. The aim of this work is to gather experts in a high-quality discussion in order to increase public awareness and raise governmental and international organizations engagement as well as to promote future adoption of a harmonized security approach.

This publication contains a selection of presentations gave in the NATO Science for Peace and Security Advanced Research Workshop “CBRN Risks in Maritime and Land Containers Transport – Global good transportation and future non-conventional challenges” held in Rome from the 25th to the 27th of May 2016. The presentations were part of the discussion of the first panel “Comparing experiences: land, maritime and container security”, the second panel “CBRN threat vectors”, and the fourth panel “Bio and chemical threat response”.

The Machiavelli Center of Florence and the University Mohamed V of Rabat organized the workshop in partnership with the NATO SPS Defence College Foundation. After the workshop, the editors welcomed the offer by ENEA to publish a selection of papers from the participants. This final outcome shall be a collection of scholarship on a field hopefully useful for experts and professionals.

Facilitating the Interface between Science and Policy Regarding CBRN

Janet K. Benini

George Washington University, jbenini@starpower.net

Abstract

There are always challenges when policy makers attempt to work in a technical sphere. The detection and exclusion of nefarious chemical, biological, radiological and nuclear materials is both extremely important and extremely complicated, when trying to balance security with the economic benefits of the global supply chain. Preparedness and response for CBRN events are also more complex than for natural disasters. This chapter addresses some techniques for securing borders against these threats, and builds upon emergency response and policy from the United States to provide practical ideas for developing workable policies and procedures for collaboration and flexibility to both prevent CBRN incidents to respond to these incidents when necessary.

Introduction

Stopping CBRN transport

Fortunately, the global experience with incidents involving chemical, biological, radiological and nuclear (CBRN) exposures is limited. One strong mitigation measure to ensure this continues to be true is to deny the transport of CBRN materials across international borders.

The connection between transportation and terrorism is clear. Transportation can be the means to accomplish a terrorist's objective, such as with truck bombs or the airplanes used in the attacks of 9/11. Transportation can provide the opportunity to impact crowds of people, such as during the bombing of the Brussels Airport in 2016. The disruption of transportation can also be the goal of terrorists, such as IRA attacks in the 1970's. Relevant to this discussion, transportation is the mechanism for bad actors to move their dangerous cargo to their targets. However, transportation also is the mechanism that allows the global supply chain to operate, and world economies to function and grow. This poses the requirement to establish and maintain, through varying threat levels, a continuum of throughput and security.

There are three general strategies to achieve the security goal in transportation. First is to inhibit access – guards, gates and technology to deny access to unauthorized people and CBRN shipments. The second strategy is passive surveillance. These includes sensors and cameras – the limitation of these techniques includes lack of real-time information and false positives. Active surveillance is the most labor intensive and therefore usually used as a surge capability based on threat. There are great opportunities to improve each of these strategies, as further chapters in this report detail. But in addition to the technical capabilities, parallel policy and response plan development is necessary to assure rapid, accurate and coordinated response if CBRN is detected.

Responding to CBRN incidents

Due to the rarity of CBRN incidents, policy makers and technical experts must extrapolate from known events policies and procedures to develop appropriate responses.

The United States, over the last decade, developed increasingly detailed and comprehensive plans and mechanisms for addressing potential CBRN incidents; these mechanisms may be useful for other nations and provide a foundation for coordinated international responses.

Challenges with CBRN Event [1]

There are several particular challenges with preparing and responding to CBRN events. Although people frequently consider them as a package, the differences among chemical, biological, radiological and nuclear events are profound and require different mitigation, preparedness, response and recovery measures. Falling into the category of low probability/high consequence events, it is difficult for CBRN to be perceived as a priority for busy policy makers and emergency managers. Particularly for biological and radiological events, the triggering incident may be difficult to recognize and the impacts widespread before detection occurs. Lingering effects of the events could extend well beyond the response period, requiring long-term recovery efforts.

US Policy and Procedure Evolution

Brought into the White House staff following the attacks of 9/11 as the Director for Response and Planning of the Homeland Security Council (2003-05), I had the opportunity to establish two baseline programs that form the foundation for US CBRN preparedness efforts.

First, we developed the National Planning Scenarios[2], designed to describe the minimum number of potential circumstances that would help the nation scope the range of response resources potentially required. Plausible CBRN incidents are included among these scenarios.

Second, we combined the national plans for terrorism, natural disasters, disease outbreaks and radiological incidents into one National Response Plan[3] with an overarching policy and response coordinating mechanism used in all types of events. Evolved over the subsequent years, this Plan now represents the core of the National Response Framework, which also incorporates mitigation and recovery at the national level.

These documents are now augmented by the National Strategy for CBRNE Standards[4], which has three areas of focus. First, it identifies an interagency policy group to coordinate the standards. It calls for both performance and interoperatibility standards for equipment used and for a testing and evaluation protocol for the equipment. Standard operating procedures for preparedness and response are covered as well as a training and certification program for responders.

Lessons Learned

The US recognized several gaps in our policies and preparedness following the Fukushima nuclear plant meltdown. As articulated by MG Julie Bentz, these areas for improvement are:[5]

- Governments need to develop a mechanism for intra-government coordination for low-probability, high-impact events. This includes the legal framework for a domestic response verses an international response.
- The US needs an improved mechanism for sharing technical data that is useful, timely, and meets the needs of all responding entities.
- We need to define metrics for success and consequence management.
- All nations need to develop policies to evacuate their personnel and citizens from a region struck by a CBRNE event. These policies should coordinate with national response efforts.

Guidance for Policy Development

Build on Existing Policies and Plans

There are two reasons why this is important. First, because CBRN events are rare, it is important that organizations respond using patterns already developed for natural disasters, humanitarian incidents and other events that occur more frequently. Speed is of the essence and governments do not have time to develop and test new systems for CBRN exclusively.

Secondly, using existing mechanisms is important because nations must take advantages of ongoing international relationships and protocols during a CBRN incident, which has a high probability of being an international event.

Coordination is Key

Many people and organizations will be involved in a CBRN response – some of whom do not work together normally. Communications between governments and the private sector is critical, as well as communicating classified information when needed. Establishing mechanisms to accomplish this before an event occurs will greatly speed needed communication when necessary.

Build in Flexibility

An axiom in the emergency management field is, "It will never go according to the plan." Therefore, flexible plans, policies and procedures should be formulated, to provide opportunities to reduce, re-scope, or increase response measures when emerging facts present themselves.

Incident Response Considerations

While CBR and N are grouped together as threats that are potentially high consequence/low probability, their characteristics and therefore appropriate responses are quite different. Chemical, radiological and nuclear events may affect a small to large geographic area, but that area has boundaries and one of the first response activities is to limit access to the area. Chemical events likely have a short duration, but radiological and nuclear ones can have impacts over years to decades. Biological incidents can further be categorized as persistent or non-persistent, contagious or non-contagious; and whether they start naturally or intentionally they are likely widespread by the time first detected. With over 1 billion people travelling across international borders annually, a disease outbreak quickly becomes a global event.

These characteristics themselves are generalized – some radiological sources have short half-lives while others persist for much longer – so responses must be developed based on a functional approach rather than scenario-based. For example, the capability to conduct evacuations is important, as well as the ability to shelter-in-place. Policy leaders and technical experts, coordinating carefully, can guide responders to implement the functions applicable to a particular situation.

Conclusions

While the probability of an extreme event involving CBRN cannot be determined, it is greater than zero, and the impacts could be catastrophic. Therefore prudent governments, companies and technical experts must include these contingencies in their suite of plans. By developing consistent yet flexible emergency preparedness doctrine, coordination mechanisms, and response plans, organizations can build on their ability to respond to higher probability events by including considerations for CBRN potentials.

The unusual characteristics of a CBRN event, including complicated technical information, possible terrorism nexus, and probable international response all require additional focus in national and international preparedness planning and operations.

References

[1] Brian Lewis, in National Research Council, An All of Government Approach to Increase Resilience for International Chemical, Biological, Radiological, Nuclear, and Explosive (CBRNE) Events, National Academies Press, Washington DC 2014

[2] Federal Emergency Management Agency, accessed 1.11.17 at: https://emilms.fema.gov/IS800B/lesson5/NRF0105060t.htm

[3] Department of Homeland Security, National Response Plan, accessed 1.11.17 at: https://www.dhs.gov/xlibrary/assets/NRP_Brochure.pdf

[4] https://www.whitehouse.gov/sites/default/files/microsites/ostp/chns_cbrne_standards_final_24_aug_11.pdf accessed 11/16/16

[5] MG Julie Bentz, in National Research Council, An All of Government Approach to Increase Resilience for International Chemical, Biological, Radiological, Nuclear, and Explosive (CBRNE) Events, National Academies Press, Washington DC 2014

The Main Problems of Public Understanding of CBRN (Chemical, Biological, Radiological, Nuclear) Risks

Sylwia Mrozowska

University of Gdansk, Faculty of Social Sciences, s.mrozowska@ug.edu.pl

Abstract

During the recent terrorist attacks in France and Belgium once again government institutions faced the challenge of how to effectively communicate a terrorist threat to the general public. The need to take action in this field has been reinforced by the fact that the international community and leaders of many countries in the world have believed that there is a high probability of the use of CBRN material by terrorists. One of the challenges for the construction of a model of effective communication in this area is the issue of social understanding of a terrorist threat. This is a complex and multifaceted issue, although its recognition has a high practical value. This paper presents the most important determinants of public understanding of CBRN threats, including issues such as the perception of risk; the level of knowledge; the knowledge of procedures and standards of behaviour in the face of a terrorist threat and, on the other hand, the level of political communication or the quality of media political discourse.

Introduction

CBRN materials are used every day for the good of humanity, but they are perceived primarily through the prism of hazards and risks. Especially after 11 September 2001, the international community and leaders of many countries have believed that there is a high probability of the use of CBRN material by terrorists. As a result, citizens began to press their governments to take immediate and extensive action to minimise this risk. In response, many countries and international organisations have adopted enhanced security procedures. Terrorist groups have shown interest in acquiring CBRN materials, but so far we can observe few successful attacks with their use [1].

The term CBRN itself arose from the notion of "weapons of mass destruction" in the period of the emergence of asymmetric conflicts [2]. Due to the fact that in the conflict which is not symmetrical, it is unacceptable to use any means affecting human life, health and the environment, the letter (E) from the word explosives has been added to the acronym CBRN and now we more often talk about a CBRNE threat. The dynamic process of shaping collective threats caused another modification of the definition and currently the CBRNE threats also include public scale threats and those of an other than military nature, consisting e.g. in the contamination of water, food and the environment, used as a means of asymmetric combat or to make gain. The term CBRNE remains associated with public threats to human communities [3]. CBRN incidents are connected with the occurrence of several potential phenomena: mass casualties; loss of life; long-term negative effects for health and the environment; and the extent and the cross-border nature of the incident.

In this article an attempt is made to present the main factors influencing the public perception of threats, including CBRN, from the perspective of social sciences. The attention was focused primarily on complex patterns of the interpretation of risk in the public sphere.

The article recalls the concept of social amplification of risk. In the second part we referred to the latest opinion polls conducted in the European Union in terms of the perception of the threat of terrorism. The example of the European Union was chosen for two reasons: the established opinion among EU citizens about the increasing risk of the use of CBRN materials by terrorists; the recent occurrence of terrorist attacks on its territory, and Europeans' heightened expectations for undertaking broader action in relation to the fight against terrorism.

Incidents involving CBRN materials are very rare, and the public has limited knowledge about how to respond to such events. General people have certain expectations for rescue operations and emergency services, partly based on films or television. These expectations are often unrealistic. It is assumed that the increase in the level of knowledge, engagement of the public in taking protective measures, skilful management of social expectations regarding the process of responding to such incidents or an attempt to understand the main problems of public perception of the risks connected with the use of CBRN materials could lead to a reduction in social unrest and an increase in public trust in emergency response procedures.

From Public Understanding of Science and Technology to Public Understanding of Risk

Issues of public understanding of science and technology (Public Understanding of Science Technology – PUS or Science, Technology, Society – STS) were raised on a larger scale in the 70s of the twentieth century. A review of the results of previous studies in the area of PUS and STS enables us to distinguish the most important psychological and social factors, which are particularly important in shaping attitudes towards science and technology and affect the perception of risks associated with them. Social assessment of the risk of the use of a given technology is essential for its acceptance or rejection. In contrast to the expert risk assessment, it cannot be predicted on the basis of the profit and loss account, in accordance with the paradigm of the theory of rational decision-making, because the cognitive assessment is influenced, among others, by emotions. Sometimes seemingly trivial threats focus disproportionately greater attention than the risks well documented in science and much more serious. An example is nuclear technology, which is so strongly associated with risk that it is socially stigmatised [4]. Psychologists and sociologists call the situation of unfunded risk assessment associated with it the loss of the sense of reality, irrational fear, a collective psychosis, a phobia or a paradoxical attitude to nuclear technology, particularly to nuclear power engineering.

In explaining these types of behaviour psychologists evoke the role of affect and availability heuristics. The affect heuristic describes people's tendency to make judgments based on their emotions. Studies by Paul Slovic and his colleagues demonstrated that a person’s affect, how a person feels about a social issue or technology, is an important predictor of how that person assesses the risks and costs associated with a specific technology [5].

Another important cognitive shortcut that influences our judgments is the availability heuristic. Kahneman [6] wrote in his book "in social context, all heuristics are equal but availability is more equal than the others”. Others often agree [7]. The availability heuristic describes people's tendency to rely on easily available, salient examples, images, and data.

Media's role in shaping easily available context and content is obvious. An example of this role is the so-called availability cascade, described by Kuran and Sunstein.

This cascade is a self-sustaining chain of events. It may start with a media report of relatively minor event and lead to public panic and government intervention. Media stories about the possibility of risk related to an action or technology can catch the attention of some viewers and readers; they may react with fear and negative emotions, which may lead to more media coverage, and this - as a cascade - creates more emotional distress among the public and more emotional reactions. In summary, studies on heuristics shed light on how people rely on simplistic rules and cognitive shortcuts when evaluating social phenomena. This area of research highlights the role of cognitive distortions in risk perception and how cognitive distortions could be related to affective responses (and vice versa) [8].

Social amplification of risk framework (SARF)

An interdisciplinary concept of social amplification of risk by Jeanne X. Kasperson and Roger E. Kasperson presents complex patterns of the interpretation of risk in the public sphere. Social amplification draws attention to the fact that social and political interpretation of risk is in fact a process of communication, in which a large role is played by social actors and institutions. In its course the risk undergoes decoding involving values and symbolic interpretation models [9].

Several arguments support the social recognition of risk. Firstly, the risk of a social or a political issue [10]. Secondly, it is connected with the socio-cultural context: people perceive risks differently because they come from different backgrounds and cultures [11]. Assuming that science and politics are in the framework of culture, we know that cultural diversity influences risk assessment. Thirdly, the risk is constructed in strategies and discourses (also in media ones), and the social control and the functioning of society are shaped by means of it [12]. The aim of SARF is to map complex patterns of interpretation of risk in the public sphere. The authors of the concept [13] emphasise that certain threats seem more dangerous than others due to the adopted heuristics, which are products of culture, and a broad framework of expectations, characteristic of the public, often enable appropriate risk identification, but sometimes seemingly trivial threats focus disproportionately higher attention than a threat well documented in science and much more serious.

The authors of the model assume that information about a threat can be "manipulated" by increasing or reducing the power of "signals", their filtering and highlighting selected aspects (the use of patterns of interpretation). It leads to strengthening or disregarding selected pieces of information on threats. Many actors and institutions (broadcasters) are involved in this process: groups of researchers; risk managing institutions; the media; activists and groups protecting the environment; peer groups; government agencies, and consecutive phases (stages) of information amplification: signal filtering; signal decoding; processing of risk information; binding information with social values in order to draw conclusions on the issue of risk management and current policy; interacting between cultural and peer groups to interpret and confirm signals; formulating an intention to tolerate a specific threat or to undertake action to eliminate it or targeted against risk managers; involvement in individual or collective activities aimed at accepting, ignoring, tolerating or changing the risk [14].

Terrorism Communication

The possibility of a deliberate attack using CBRN materials is a serious challenge for those responsible for communicating the incident and first of all it requires getting to know factors responsible for the public perception of risks.

The literature analysis [14] of terrorism communication has led to the specification of the following challenges for communication and the communication practice. In the first area it is pointed that terrorism evokes strong emotions and creates a high level of fear. Fear and uncertainty lead to many types of irrational and unexpected behaviour of general people. There is a risk of loss of confidence in and credibility of the institutions responsible for countering terrorism. A media discourse about terrorism, which can lead to conflicts in the society, also becomes an important problem. Moreover, a discourse developing in social media is difficult to monitor. There is a noticeable tendency to transfer the responsibility to the authority. Little knowledge on a wide range of hazardous materials is a problem in the case of crises connected with the use of CBRN materials. This is confirmed by studies conducted in the US [15]. In addition, obtaining knowledge on CBRN materials requires continuous updating, among others, due to the technological progress. In the second of the mentioned areas a challenge is to prepare immediately available and updated sources of knowledge on CBRN for general people.

Consistency of information from various sources and their credibility is one of the factors affecting the trust in the information source. The need to maintain and build trust in the source of information is indicated as another important factor influencing the effectiveness of communication about risks [16]. Another problem is the cooperation between the public health sector and rescue services. With regard to communication activities it is a challenge to have competence in the field of social media, particularly in the area of monitoring and methods of interpretation of data, which can be an important factor influencing the effectiveness of the communication strategy. In the event of crises connected with the use of CBRN materials the issue of communication in the area of health and strengthening of social resilience is an important challenge. A characteristic feature of such crises is the durability of the effects, so a challenge will be not only communication before and during the crisis, but also when the crisis is over [17].

Europeans and the fight against terrorism

Europeans have experienced many types of terrorism in their history. Today, despite undertaking a number of activities in the field of countering terrorism by both the European Union and the Member States, terrorism is indicated as one of the most important challenges and threats in the security strategies of EU countries. Recent terrorist attacks in France and Belgium have strengthened Europeans' belief that terrorism still threatens the security and values professed by democratic societies and the rights and freedoms of European citizens.

The special issue of the European Parliament Eurobarometer entitled Europeans in 2016: Perceptions and expectations, the fight against terrorism and radicalisation presents the opinion of Europeans in relation to the areas in which EU action is seen as insufficient and where broader action is expected. In the area of foreign policy, security and defence policy and European values, EU action is considered inadequate, among others, in relation to the fight against terrorism. 69% of respondents believe that EU action is not sufficient, 82% would like the EU to undertake large-scale action, 40% of respondents believe that the risk of terrorist attacks is high, at the national level an absolute majority of respondents believe that the risk of attacks is high in France (64%), the UK (55%) and Belgium (50%). Europeans enumerated the most important measures which according to them are most urgent in order to combat terrorism at the European level.

Among them there were, in descending order: the fight against the financing of terrorist groups, the fight against the roots of terrorism and radicalisation, strengthening of border controls, better cooperation between the police and intelligence services of the Member States and Europol, an EU agency for police cooperation, the fight against smuggling of weapons within EU, preventing radicalised citizens of the Union from joining terrorist organisations and better anticipation of their return to the European Union [18].

The terrorist attack that took place in 2016 in France and Belgium have confirmed that contemporary terrorism, particularly its Islamic version, focuses on maximizing the scale of psychological influence on the attacked community by shocking with vastness of casualties and determination of terrorists. Europeans expect increased preventive action on the part of state and European Union institutions, insufficiently caring for their education in terms of safety procedures and correct ways of behaviour in case of terrorist incidents. The analysis of social behaviour during the recent terrorist incidents confirms the fact that the level of knowledge of general people will play a more and more important role in minimising the number of casualties of terrorist attacks, which directly translates into the ability to read messages from the institution of crisis management.

Conclusions

The variety of incidents with CBRN materials, uncertainty, high dynamics of information about it, the impossibility to determine the exact boundaries of time and space of hazards associated with them, the lack of knowledge and diverse information needs of different social groups (the public) pose a serious challenge to the institutions of crisis management. Currently, contamination with hazardous chemical, biological, radiological and nuclear (CBRN) agents is still a serious threat to the environment and to the human life and health. This threat can result from potential acts of war, but also from the threat of terrorist acts with the use of CBRN materials, as well as from industrial or transportation failures and disasters. Actions taken by governments and international organisations after the 11 September 2001 focused primarily on intelligence analysis programmes; programmes to prevent illegal dissemination of CBRN materials; systems of responding to the threat with the use of CBRN weapons, or the creation of specialised units for nuclear, radiological terrorism, bioterrorism or chemical terrorism with the use of explosives. Much less attention is devoted to public understanding of CBRN risks.

The article showed a connection between the public perception of threats and the effectiveness of communication about the risk and risk management. Effective communication has the potential to mitigate the risk, supports the implementation of protective measures and may contribute to minimizing the negative social effects, including psychological ones. Effective communication translates directly into the efficient implementation of protective measures by those directly threatened by the effects of incidents and prevents panic among these groups that are not directly endangered. As a result, it leads to the preservation of public trust in institutions.

References

[1] The Global Terrorism Database, www.start.umd.edu

[2] M. Kadlor, New & Old Wars. Organized Violence in a Global Era, Standford, 2007

[3] L. Górniak, D. Kalisz, K. Młynarczyk, Zagrożenia chemiczne zamierzone, redukcja podatności i kultura bezpieczeństwa chemicznego, *Chemik*, vol. 69, no. 4, pp. 201-208, 2015

[4] J. Flynn, P. Slovic, H. Kunreuther, (eds.), Risk, Media and Stigma. Understanding Public Challenges to Modern Science and Technology, London, 2001

[5] P. Slovic, M. L. Finucane, E. Peters, D.G. MacGregor, Risk as analysis and risk as feelings: Some thoughts about affect, reason, risk, and rationality. *Risk Analysis*, vol. 24(2), pp.311-322, 2004

[6] D. Kahneman Thinking, Fast and Slow. Macmillan, 2011

[7] L. Sjöberg, Factors in Risk Perception. *Risk Analysis*, vol. 20(1), pp. 1-12, 2000

[8] T. Besta, The Role of Shared Group Beliefs, Framing Effect, Affect and Reasoning in Perception of Technology In S. Mrozowska (Ed.), Social Sciences and Energy Issues, pp. 109-119, Kraków 2016

[9] [14] J. Arnoldi, Risk, Cambridge, 2009

[10] U. Beck, Społeczeństwo ryzyka. W drodze do innej rzeczywistości, Warszawa, 2002; Społeczeństwo światowego ryzyka. W poszukiwaniu utraconego bezpieczeństwa, Warszawa, 2012

[11] M. Douglas, Risk and Blame, London, 1992

[12] M. Foucault, Governality, In G.Burchell, C.Gordon, P. Miller (red.), The Foucault Effect, London, 1991

[13] J.X. Kasperson, R.E. Kasperson, The Social Contours of Risk, London, 2005

[14] A. Rugierro, M. Vos, Terrorism Communication: Characteristic and Emerging Perspectives in the Scientific Literature 2001-2012, *Journal of Contingencies and Crisis Managment*, vol. 2, no. 3, pp. 153-166, 2012;

[15] R.J. Wray, S.M. Becker, N. Henderson, D. Glik, K. Jupka, S. Middleton, C. Henderson, A. Drury, E. Mitchell, Communicating with the Public about Emerging Health Threats: Lessons from the Pre-Event Message Development Project, *American Journal of Public Health, vol.* 98, *no.* 12, *pp.* 2214–2222, 2008

[16] M.B. Rogers, R. Amlôt, G.J. Rubin, S. Wessely, K. Krieger,Mediating the Social and Psychological Impacts of Terrorist Attacks: The Role of Risk Perception and Risk Communication, *International Review of Psychiatry*, vol. 19, no. 3, pp. 279–288, 2007

[17] A. Ruggiero, M. Vos, M. Mykkänen, P. Palttala, CBRN Communication Scorecard. In S. Schmidt, M. Vos (Eds.), Behavior and communication in CBRN crisis: Findings and recommendations in case of chemical, biological, radiological, and nuclear attacks on society, pp. 106-139, Pabst-Science Publishers**,** 2015

[18] J. Nancy, Europejczycy w 2016r.: wyobrażenia i oczekiwania, walka z terroryzmem i radykalizacją postaw. Wydanie specjalnie Eurobarometru Parlamentu Europejskiego, Biuro Analiz Parlamentu Europejskiego, PE570423, 2016

Using Container Status Messages to improve targeting of high-risk cargo containers

Aris Tsois, Jose Antonio Cotelo Lema, Michail Makridis, Enrico Checchi

European Commission, Joint Research Centre - Space, Security and Migration Directorate, Aris.Tsois@ec.europa.eu

Note: This is a short version of the original paper presented at the WCO TI Forum held in Rotterdam in October 2015. The risk indicators examples, illustrated in the original paper, have been redefined and adapted to CBRN[1] threat scenarios.

Abstract

Customs authorities consider the transportation route as an important factor for the profiling and targeting of high-risk cargo containers. In most of the cases, authorities have incomplete information. On the other hand, ocean carriers collect, store and own Container Status Messages which describes the status and movement of the containers. In this paper we present how semantic information can be extracted from the CSM data in the form of Container-Trip Information (CTI) and Vessel-Stop Information (VSI). These new information elements can be used to build route-based risk indicators for the automated analysis of the routes. Finally, we present the visual analytics tool we have implemented to analyse and visualize CSM and CTI data.

Introduction

The vast majority of non-bulk cargo worldwide is transported in containers. The World Shipping Council estimates[2] that more than 18 million of containers were active in 2011, transporting in 2014 more than 171 million TEU (Twenty-foot Equivalent Unit) of goods. Due to the high volumes of containerized trade, authorities can physically check only a small fraction of it, limiting their capacity to detect illegal activities and security threats.

Increasing the number of controls by a large factor, at any single point of the supply chain, would result in disproportional large increases in the costs of these controls. Therefore, the only alternatives are: a) the distribution of the controls along the supply chain and b) the improvement of the efficiency of each control.

Customs can distribute the controls by collaborating with other customs authorities (for example at the origin of the goods – the Customs-to-Customs pillar of WCO SAFE) or by collaborating with the supply chain industry by including them within the control structure (i.e. the Authorized Economic Operators (AEOs) programs – the Customs-to-Business pillar of WCO SAFE).

On the other hand, for improving the efficiency of the controls, which is the subject of this paper, the authorities can count on (among others) better data or better tools that process the data they have available. Customs-To-Customs and Business-to-Customs collaborations can both bring better (and more) data but then it is up to each customs' authority to make the best use of the available data.

In this paper, we focus on improving the processing of just one of the information elements used by authorities, namely the ***routing of the goods***. The efficient usage of this information can significantly improve the identification of illicit trade, including the detection of shipments posing safety or security threats. In fact, WCO SAFE defines data elements through which customs authorities can collect information on the origin country, the countries of routing, as well as the final destination.

[1] Chemical, Biological, Radiological, Nuclear.
[2] World Shipping Council, Container supply review. World Shipping Council, Berlin, Heidelberg, 2011.

Unfortunately, poor quality information regarding the actual route followed by a container is quite common in Customs' declarations. However, authorities may collect much more valuable and detailed information on the routes followed by the containerized goods through a different data element: the Container Status Messages (CSM). WCO SAFE already foresees the collection of CSM data and US is collecting since 2010 CSM data for all containers destined to arrive in the US with its 10+2 rule. In Europe a recent EU legislation[3] has empowered EU customs to systematically collect and use CSM data for anti-fraud purposes.

This paper explains how CSM records can be used to enable route-based risk analysis and assist the profiling and targeting of suspicious containerized cargo.

1. Container Status Messages

The Container Status Messages are electronic records used by the logistic industry, and mainly the ocean carriers, to keep track of their fleet of container and monitor the progress of their transportation. They may contain a big variety of data elements, however, for the purpose of using them for route-based risk analysis we identified that just the following 7 data elements are enough: Container identifier, Event description, Location identification, Data and time of the event, Vessel (if any), Load status (empty/full/etc.), and Carrier.

CSM data is generated from multiple parties and different standards / encoding schemes are used for the various data elements. This means that the characteristics of the above data elements are not uniform across all CSM data and requires appropriate data transformation and cleaning before it can be used for further analysis and processing[4].

When all the data quality issues are taken into account, and appropriately dealt with, the resulting set of "cleaned" CSM records can be very valuable for route-based profiling of shipping containers. The events described in these CSMs indicate the locations and dates when the various operations took place. They indicate how long a container remained in a particular location and how long it took to be transported from one location to the next.

A human examiner can derive the complete route of the container at the detail-level reported by the corresponding CSMs. The CSM-revealed information could also be checked against other data sources available to customs, like the import declarations, to identify inconsistencies or to complement them with the details of the complete route followed.

2. Container-Trip Information

Customs authorities consider the complete route of the cargo an important factor of the risks assessment process in both import and export control. Such route-based risk analysis can be done by appropriate use of the relevant CSM records. However, the full set of CSMs of a given container is not the most appropriate for this analysis. One needs to focus on the subset of the CSM that describe the movement and events of the container only while carrying the corresponding goods. This subset of CSMs can be analysed so that the required information on the transportation of the goods are extracted.

ConTraffic has implemented a machine learning algorithm based on Conditional Random Fields[5] to extract semantic information on the container route from the sequence of CSMs records describing its movements and events. In particular the algorithm detects the sequence of CSMs that describe the movements and events of a container while carrying the goods from their origin location to the final destination and extract semantic information from them.

[3] Regulation (EU) 2015/1525 of 9th September 2015 amending Regulation (EC) 515/97
[4] The list of issues for CSM data quality is described in the original paper.
[5] More details about the algorithm are in the original paper.

ConTraffic defines container-trip each transportation of goods from their origin location to the final destination by one (and only) cargo container. The Container-trip information (CTI) is the data structure defined to store the container-trip information needed in the route-based risk analysis. ConTraffic defines 5 phases for a CTI:

1) **Stuffing**: when and where the goods get stuffed into the container.
2) **First-load**: when and where the container started its deep-sea maritime transport.
3) **Transhipment** (if any): when and where the container transhipped.
4) **Final-discharge**: when and where the container ended its deep-sea maritime transport.
5) **Stripping**: when and where the goods get stripped from the container.

Each of the 5 phases contain information on the location involved, the time period covered and the vessel(s) involved (if any). The CTIs allow customs authorities to perform much more advanced and automated route-based risk analysis than what is possible by using just the CSMs.

3. Vessel-Stop Information

If a container remains on-board the vessel, while other containers are loaded and discharged at a container terminal, then no CSM is generated for that container at that terminal. Therefore, by looking only at the CSMs of the container one may not discover the locations where the container has been while being carried on-board a vessel. This additional information, which is not contained in the CTI defined above, can be calculated if we have available the routes of the vessels and details about all the ports they called and the dates during which they remained at the ports. For presentation reasons we call a *vessel-stop* any such call at a port by a container vessel.

The details of vessel-stops can be obtained from various databases that record the movement of vessels. However, by analysing CSMs it is possible to compute these vessel-stops. At each port where a vessel-stop took place some containers were loaded and discharged and therefore CSM records were generated to describe these events. Such CSMs can be used to derive (precisely enough) information about the vessel-stops. The Vessel Stop Inference (VSI) algorithm that we designed and implemented tackles this issue: computation of vessel-stops based on the total set of CSMs. More specifically, VSI identifies, for each vessel, the locations where load and discharge events happen, along with the corresponding dates of the events. The aggregation and analysis of the above-mentioned information leads to the calculation of the sequence of vessel-stops. Each vessel-stop defines the port called by the vessel along with the relevant time period during which the vessel was at that port.

4. Applying route-based risk analysis for profiling containers

The purpose of computing CTI and VSI is to enable advanced processing and analysis of the CSM data for profiling containers. This information records can be used together to analyse the routes of the cargo containers and identify risks that these routes may reveal. We call route-based risk indicators the indicators that can be constructed by taking into account the CSM, CTI & VSI data, which reveal the route followed by the cargo from its source to the final destination.

A risk indicator is a mathematical formula that returns a numerical risk value in the range 0 to 1. Higher values indicate higher risk. The formulas use as input a database of CTI and VSI records and a number of reference data (usually the date and place when/where the container entered the jurisdiction of a customs authority and the vessel that brought it) that identify the shipment (container / goods) to be examined.

4.1. Risk indicator based on the ports in the route

Through the CTI and VSI records that are related to a particular shipment of goods it is possible to reconstruct the full list of ports visited by the goods during the transportation. This list of ports can then be

used to calculate a total route's risk based on a predefined (static) table of risky ports. The formula could even take into account the handling time at the port, if operations took place at the port, or the fact that the container just remained on board.

An alternative way to define such a risk indicator is to compare the computed list of visited ports with the data declared in pre-arrival declarations (like the Entry Summary Declarations in Europe) and identify if risky ports are not mentioned in the pre-arrival data.

In the following sections we provide two hypothetical examples of risk indicators related to CBRN threat[6] scenarios. Note that they are just example formulas to illustrate the usage of CTI records and not a proposal for risk indicators to be used in practice by authorities.

4.1.1. Example 1: "Hijacked" container risk indicator (shipper not involved)

In this *modus operandi,* a container is intercepted at some point along the logistics chain and opened illicitly. Weapon is inserted and container is closed/re-sealed. In this scenario the shipper and carrier are not aware and not involved with the illicit activity. For this reason the formula takes into account for a predefined percentage (F_{static}) the absolute risk of each location/country touched (R_{Ds}) based on a static predefined table of risk plus the complementary percentage ($1 - F_{static}$) of the same static risk multiplied by the abnormality of the length of the stay in the location ($RHstd_s$)[7]. The final value is the average value computed for all the locations/countries of the container trip. The final formula is then:

$$Risk = AVRG(F_{static} * R_{Ds} + (1 - F_{static}) * R_{Ds} * RHstd_s)$$

The locations touched by the container, in the relevant container-trip are taken from the corresponding CTI record, which is identified, based on the reference data. The value of F_{static} can be used to adjust how the weight is distributed in the formula between the location static risk and the abnormal handling time indicator.

4.1.2. Example 2: "Trojan Horse" container risk indicator (shipper involved)

In this *modus operandi,* terrorist establishes "legitimate" export business, builds trading record and trust through legitimate operations over a period of time. Because of the involvement of the shipper, the model consider as important only the risk of a CBRN weapon insertion in the container $R_{Worigin}$ at the estimated stuffing/departure location of the trip and the number of transhipments (TR_{number}), because they may be used as a way to hide the real origin of the transportation. As in the previous case, a factor F_{static} for composing the two aspects is used. The formula is the following:

$$Risk = F_{static} * R_{Worigin} + \frac{1 - F_{static}}{7} * MIN(TR_{number}, 7)$$

This formula represents a route-based analysis result as it can be computed based on the CTI information that includes both the total number of transhipments $\mathbf{TR_{number}}$ and the estimated stuffing/departure location. The $\mathbf{R_{Worigin}}$ values are obtained from a pre-computed static table of risks.

5. Visual analytics

Apart from the systematic use of CSMs, and of the derived CTIs & VSIs, for computing risk indicators, the same information can be used for manual investigations and analytical work. Such analytical work may aim to understand the flows of containers, examine hypothesis and scenarios and discover interesting facts. This

[6] It's the possibility that a terrorist group uses a container to deliver a CBRN (Chemical, Biological, Radiological and Nuclear) weapon.

[7] $RHstd_s$ can be computed for each phase of the container-trip, as the comparison of the reported time spent in the location/port (HT_s) against its first order statistic (mean value M_s and standard deviation σ_s). See the original paper for a detailed description.

analytical work is needed to identify or better understand illegal activities in which shipping containers are involved.

Given the massive volume of containerized cargo we expect that customs analysts will have access to very large databases of CSM, CTI & VSI records. With a visual analytics tool the analysts will be able to explore the data, to efficiently search and to understand large results sets through appropriate visualizations.

In order to demonstrate the value of this approach, along with the analytical power provided through the CTI records, we have developed a visual analytics prototype within the ConTraffic website[8]. The current tool allows the user to interactively explore the CSM and CTI data in the ConTraffic database, perform various search operations and display the results on geographical maps, timelines and text tables. The ConTraffic database is appropriate for such a demonstration as it contains billions of CSMs and millions of calculated CTIs.

Although the developed tool is just an initial prototype it has the power to select CSM records based on properties of the CTI records to which they correspond. For example, one can ask to see the CSM records that correspond to container-trips (CTI) that have as first loading port a particular location or with final destination in a particular country, or with X or more transhipments, or even with a duration of more than Z days.

The results are shown on maps aggregated by location, with the size of the circles indicating the relative number of records that correspond to each location and colours to indicate the type of records at each location. The maps are interactive with not only the typical zoom/pan capabilities but also with information pop-ups that give more details when the user moves the mouse over the various circles and lines. Double-clicks on particular items would also start new visualizations.

While maps are very good to understand the geography of the information, something very important for the movement of containers and goods, timelines are very appropriate to focus on the time dimension and the sequence of events / operations. Timelines show naturally the duration of the various phases of the container-trip; for example the duration of transhipments.

[8] https://ec.europa.eu/jrc/en/scientific-tool/container-traffic-monitoring-system

6. Conclusions

In this paper we presented how Container Status Messages can be efficiently used for manual and automatic route-based risk analysis in support of containerized cargo profiling and targeting. We have identified the pre-processing needed on CSM records in order to improve their values; we have presented why it is important to have container-trip and vessel-stop information and how that can be extracted and computed from the CSM records.

Finally, through the presented route-based risk indicators and the prototype visual analytics tool we have demonstrated the usefulness of this approach and indicated a number of techniques that can be applied. Our conclusion is that route information alone is not enough for container profiling but when combined with other customs data and risk information it can be very valuable.

We believe that the results of this research work can be used both as evidence for the value of using CSM data in the domain of container profiling and targeting as well as to facilitate the implementation of the relevant IT tools that authorities will require.

The presented results are far from exhaustive and research work can continue in various directions. For example the visual analytics tool can be enhanced with a plethora of additional functions, the algorithm for CTI computation can be further improved and applying unsupervised machine-learning methods on CTIs for outlier detection may bring further results.

References

1. A. Tsois, J. A. Cotelo Lema, M. Makridis, E. Checchi. Using container status messages to improve targeting of high-risk cargo containers. *In Research Track at the 5th World Customs Organization Technology & Innovation Forum, Rotterdam*, Netherlands, 2015.
2. P. Chahuara, L. Mazzola, M. Makridis, C. Schifanella, A. Tsois, M. Pedone. Inferring itineraries of containerized cargo through the application of conditional random fields. *In Proc. of the 2014 IEEE Joint Intelligence and Security Informatics Conference*, pp. 137-144, Washington DC, USA, 2014. IEEE Computer Society.
3. E. Camossi, T. Dimitrova, A. Tsois. Detecting anomalous maritime container itineraries for anti-fraud and supply chain security. *In Proc. of the 2012 European Intelligence and Security Informatics Conf., EISIC '12*, pp. 76-83, Washington DC, USA, 2012. IEEE Computer Society.
4. World Shipping Council. Container supply review. *World Shipping Council,* 2011.
5. V. Donati, E. Kotsakis, A. Tsois, F. Rios, M. Zanzi, A. Varfis, T. Barbas, J. Perdigao. Overview of the ConTraffic system. *In Technical report, JRC. Joint Research Centre*, 2007.
6. United Nations Conference on Trade and Development. Review of the Maritime Transport 2015. *United Nations Publications*, 2015.
7. World Customs Organization. SAFE Framework of standards to secure and facilitate global trade. *World Customs Organization,* 2015.
8. P. Villa, E. Camossi. A description logic approach to discover suspicious itineraries from maritime container trajectories. *In GeoSpatial Semantics: Proc. of the 4th Int. Conf., GeoS 2011*, France, pp. 182-199, Berlin, 2011. Springer.

Swedish Experiences regarding CBRN Risks in Maritime and Land Container Transport – with focus on the Radiological (R) and Nuclear (N) aspect

Helmuth Zika

Swedish Radiation Safety Authority

Abstract

Sweden has an extensive nuclear program including power reactors along its coastlines, a fuel fabrication plant, nuclear waste storages and other radiological facilities. Transports of nuclear materials and other radioactive sources are done frequently. The Swedish Radiation Safety Authority (SSM) is as the guardian of the Act on Nuclear Activities and the Radiation Protection Act responsible for licensing and supervision of radioactive transports. They need also to comply with all the international transport regulations (ADR, IMDG-Code etc.) for dangerous goods. SSM cooperates with other national authorities in the supervision and enforcement of the requirements in the form of joint inspections and information exchange.

Key words: Coast Guard, Customs, Emergency preparedness, Field exercises, Legal aspects, Mobile X-ray scanners, National Police, Operative authorities, R/N detection, Transport Safety Inspectors (R/N).

Introduction

Transport containers such as sea containers are widely used in Sweden to transport ordinary cargo but also dangerous goods of all classes (1- 9) by sea and on road/railway. The large number of container movements across the national border to and from EU member states and third countries makes control of the shipments difficult. Prohibited articles and high taxed consumer goods may not be declared at all and be hidden amongst other ordinary goods. Undeclared dangerous goods may also impose an increased safety risk both during the handling of the containers and for example passenger ferry safety. Pyrophoric materials, flammable liquids and compressed gases may have catastrophic consequences if they catch fire on the car deck of a ferry, by accident or intended. Radioactive materials such as contaminated scrap metal or consumer items produced from radioactive contaminated metal ingots may cross the border undetected and be a threat to public health.

Legal aspects

Regarding radioactive materials that also includes nuclear substances the main legal requirements aside EU Regulations are incorporated in the Act (1984:3) on Nuclear Activities and in the Act (1988:220) on Radio Protection. These two acts together with their underlying Government ordinances and regulations issued by SSM are the basic legal pillars regarding control, handling etc. of radioactive materials in Sweden. In addition, the Act (2006:263) on Transport of Dangerous Goods reflects the IAEA Transport Regulation SSR 6 in its current version. Relevant EU directives are incorporated in these mentioned acts.

Authorities involved

The competent authority for licensing practises with all radioactive materials, including transport and supervision of those activities is SSM. Inspections of dangerous goods in common is done primarily by the border controlling authorities such as Customs and the Coastguard at harbours and other entry points to Sweden, but also at ordinary road controls by the Police. The Swedish Transport Agency (TS) and the Swedish Work Environment Authority are mainly involved in so-called joint inspections as described under the next heading, but the railway department of TS does container inspections at rail/road terminals. If transports of radioactive materials has to be controlled during routine checks, SSM could provide support through their duty officer 24/7.

Authority cooperation

Dangerous goods in accordance with the international transport regulations (ADR, RID, IMDG etc.) including their carriers could be inspected by several authorities regarding different aspects of the goods and the legal competence of the authority.

To optimize the inspection work and act as a deterrent joint unannounced inspections are performed at mainly harbours and other border crossing points by mixed teams. The cooperation has the acronym SAMTIL that stands for “cooperation in legal enforcement”.
At the time being the following authorities take part in the SAMTIL work within their legal competences:

- Swedish Customs
- National Police
- Coast Guard
- Swedish Radiation Safety Authority (SSM)
- Transport Agency
- Swedish Work Environment Authority.

At regular meetings between representatives of the involved authorities inspection plans are being prepared and decided, and information exchanged. Normally the inspections are coordinated by a rotating leadership among Customs, Police and Coast Guard. The number of planned joint inspections are about one every month on top of the common enforcement activities by the Parties.

Selected containers in harbour moved for control by joint inspection team (Photo: SSM)

Inspection activities

The purpose of the SAMTIL border inspections are to cover all types of dangerous goods (IMDG etc. Class 1 – 9), search for contrabands, check the stowing and latching of cargo in- and outside shipping containers and control of vehicles, drivers and passengers. Alcohol level checks of drivers and vehicle conditions are very effective in accident prevention involving dangerous goods.

Swedish Customs mobile X-ray scanner in action (Photo: SSM)

Mobile X-ray scanning equipment used by Customs units is an extended option to stationary devices and enables a more effective use of the resource and it´s special trained personnel. Special software is used to identify suspect objects within the cargo department, container or vehicle. Manual search by officers could then be limited mainly to these areas. Specially trained sniffer dogs might then be assigned to check certain interesting areas. The selection of trucks and cars to be X-rayed is limited due to the rather time consuming procedure. If the vehicles comes to the border point by ferry a combination of check of the ferry`s manifest together with Customs intelligence will determine which vehicles will be selected for a more thorough search.

R/N detection

SSM is the competent authority for Class 7 Radioactive Materials regarding transports, and also issues package certificates, validations of foreign certificates and license use and transport of RAM according to the Nuclear Act and Radiation Protection Act. During SAMTIL inspections the SSM team normally uses handhold fast search instruments and calibrated dose rate measurement instruments. SSM has a 24/7 officer on duty who can provide assistance and also mobilise the emergency preparedness organisation of SSM if needed. Well-equipped own measurement teams and also contract laboratories all over Sweden could give assistance. The Customs, Police and Coast Guard have their own instruments and are partly trained by SSM.

Cobalt-60 contaminated commercial goods and radioactive scrap metals are of concern. Radioactive sources such as level gauges or other abandoned sealed sources hidden in the scrap metal can be difficult to easily detect due to shielding effects from surrounding metals. If they are not detected at border checks but later at a commercial smelters portal monitors, they might regenerate high costs for waste handling as orphan sources. The worst case scenario is that they are not detected and charged into a smelter. That might produce many tens of tons of contaminated ingots that has to be handled as radioactive waste with very high costs and maybe airborne radioactive contamination of part of the plant. Cesium-137 is here of special concern as it may be very volatile and rather longlived, about 30.2 years half-life.

Scanning of truck at border crossing with a GR-110 search device (Photo: SSM)

SSM mobile measurement team truck (Photo: SSM)

Training

Exercises

SSM has in the past organised a number of field exercises together with the University of Lund with the aim to find stolen or lost radioactive sources and handling dirty car bombs, bomb labs with RAM and other scenarios. International participants and observers were invited. Military gunning ranges and CBRNE facilities in Southern Sweden were used for the exercises, which were set up in a station system of logistic reasons.

Powerful radiation sources such as blood irradiators together with less potent sealed sources and also liquid radioactive sources were used. The strong blood irradiators, mainly Co-60 were hidden in wooden boxes and shielded in a way that they could beam upwards in a collimated beam to produce so called sky-shine. The sources were operated remote controlled outside a restricted safety zone. The purpose was to show the uninformed exercise teams how difficult it is to do measurement on a source when only indirect radiation could be measured from a safety distance. The unexpected sky-shine really confused many of the search teams.

Other exercises involved short-lived nuclides such as F-18 and was spread out in a dirty bomb scenario for more realism. Fully equipped search teams had to survey the involved car wrecks. Other exercises involved search teams that went “per pedes”, used cars, helicopters and an aircraft with long dedicated tail for geological survey to complete their mission.

Exercise REFOX-11. Swedish Customs R/N measurement vehicle together with a Danish EPR team and a Swedish Army CBRN APC tracking lost gamma sources (Photo: SSM)

In the year 2015 an exercise called Pilot-2015 simulated a full scale terrorist attack on a nuclear cargo ship (M/S Sigrid, an INF-3 type vessel). She is mainly used to transport spent nuclear fuel (SNF) from Swedish nuclear power stations situated along the North Sea and the Baltic Sea to the interim storage for spent nuclear fuel (CLAB) that lays close to Oskarshamn in the Southern Baltic Sea. This ship has special features regarding physical security, but the exercise gave also a good picture of the challenges an law enforcement action against a captured ordinary container ship loaded with dangerous goods would meet. International observers were able to watch part of this exercise that involved the National SWAT team in action.

Dangerous goods such as radioactive uraniumhexafluoride(UF_6) in steel cylinders are commonly shipped in sea containers as an overpack or in special racks. An antagonistic act that would rupture this type of cylinders with radioactive content would both give a radioactive release but probably worse a chemical cloud of very poisonous hydrogenfluoride (HF) when the content in the cylinders react with water or moist in the air and decomposes. Remediation efforts will be difficult and time consuming. Specially trained personnel will have to handle such a situation.

Fissile uraniumhexafluoride (UF6) in 30B cylinders on a rack (Photo: SSM)

Conclusions

Transport containers are from a logistic standpoint very effective for sending all types of cargo. Closed containers protects the cargo from environmental impacts especially during sea transports on dedicated container ships that could take month to reach their final destination. The containers should comply with standards for this type of overpacks, i.e. they should be robust for their purpose to protect the content. Containers can be fully loaded with goods. From a control aspect, this fact makes it difficult for authorities to check their contents for contrabands and dangerous goods. A container ship arriving to a harbour in Sweden can have up to 15 - 20 000 sea containers as cargo. International and national cooperation such as sharing Customs and Police intelligence with each other, to involve other authorities and use sophisticated measurement equipment is a tool for success. The Swedish model with joint authority inspections at mainly border points both works well and is successful.

References

1. Seminar on REFOX exercise (2012) held August 27 – 29, 2013 at Park Inn Hotel Solna, Stockholm hosted by the Swedish Radiation Safety Authority. NKS activity NordEx-12

2. Integrated Regulatory Review Service (IRRS) Mission to Sweden, 6 to 17 February 2012. IAEA-NS-IRRS-2012/01

3. Travel report from ENSRA Meeting in Brussels 2014 by Mr. Tommy Nielsen. Swedish Radiation Safety Authority, document registry index 14-3090

4. Marine joint exercise (MS 14) at Berga Naval Base, Sweden. CBRNE exercise organised by the Swedish Customs 24 – 27 November 2014 in cooperation with the University of Lund. Swedish Customs registry index 2014-26

5. Joint authority inspection at Norrköping harbour, Sweden on 26 February 2016. Swedish Radiation Safety Authority registry index SSM2016-676, document 16-560

CBRN Transport System Security Decontamination Strategies and Solution

Renato Bonora[1], Stefano Miorotti[2]

[1]*University of Padua, Department of Industrial Engineering, renato.bonora@unipd.it*
[2]*Subject Matter Specialist, Cristanini SpA, cristanini@cristanini.it*

Abstract

This article analyses the Chemical, Biological, Radiological or Nuclear (CBRN) risks for the international maritime and land transport system due to terrorist organizations and, within incident management, how planning the decontamination measures helps to minimise the effects of a CBRN event whether deliberate or accidental. First responders shall be trained and equipped to respond to all CBRN hazards.

As part of the planning process for CBRN, decontamination organisations should consider actions to be less dependant from initial ambiguity and/or delay in determining the type of material involved in CBRN incident.

Historically, decontamination has been viewed and used as a defensive measure, normally as part of military force protection. In the last three decades state and non-state actors have long sought to acquire and use CBRN weapons. The threat is increasingly serious and complex, as these weapons are now more readily available and harder to detect. With the development and the evolutions in decontamination technology, decontamination systems and methods are refined to be used for the reduction of threat vulnerability.

Introduction

Containers are the basic unit for delivering goods through any international market. Every year million containers reach the seaports around the world and million of them travel along the road, on land. The movement of containers brings a risk of illicit trafficking, as well as CBRN threats. Sealed containers pose a growing risk of prohibited or hazardous material to be shipped worldwide.

The impact of CBRN attacks perpetrated by terrorist to containerized transport reaching economic, psychological and personal targets can be devastating for the maritime and land containers transportation sector.

The security problems in the chain container transport are mainly related to internal freight integrators, carriers operating in the starting and ending links of the chain.

Whereas a CBRN incident occurs (accidentally or intentionally), effective response and recovery plans must be activated. An action for the resolution of incidents will be taken, depending on the location of the incident itself, either public or shipping/logistics company; the essential matter for the transport companies is to be aware of the problems associated with the incident response and recovery.

The preparedness phase takes place before an incident; planning, tools and procedures will help to take action faster, thus providing a more efficient in response.

To contain a CBRN incident, the first consideration should be to reduce the impact of contamination above all. Decontamination efforts are essential to mitigate the effects of hazards in order to enhance effectiveness of post-event restoration. Typically, decontamination should be performed as soon as possible to maximize effectiveness.

The areas exposed to CBRN agents should be considered contaminated, with a presumption of validity until the contrary is demonstrated.

This is why the decontamination and clean-up must be carried out in order to reduce or avoid exposure to CBRN materials for first responders and staff, thus avoiding the risk of an uncontrolled spread.

Historically, decontamination has been viewed and used as a defensive measure, normally as part of military force protection on the battlefield, but most experts agree that future threats are more likely related to urban or semi-urban environment and to critical infrastructures. An agile adversary also may seek to develop complex CBRN incidents that may involve a combined chemical and biological or radiological release, or any combination thereof.

Speed of response and multifunctional solutions are an intrinsic part of a new philosophy to help overcoming these challenges. This has a huge impact on training, operational procedures, logistics and supporting capability management and relating cost benefits, but above all it brings a real improvement at the operational level. If a respirator and suit can protect the operator against multiple types of hazards, why should decontamination be any different? R&D can work to refine processes and develop creative solutions for those who need them. Saving of life is the priority and decontamination must be timely provided.

With the development and the advances in decontamination technology, decontamination operations are refined to be used for the reduction of threat vulnerability. Decontamination systems and methods have increased their importance compared to few decades ago.

The protection of critical infrastructures, such as logistics and transportation systems, harbours, airports, industrial and commercial facilities, etc., is based, among the possible measures to prevent, mitigate and respond effectively to a potential CBRN incidents, on the development of adequate capabilities and their timely and flexible deployment and performance.

In order to meet the demand of a new generation of decontamination systems for the possible future scenarios and challenges for CBRN preparedness, for about a couple of decades we have been working on projects to explore innovative solutions for a CBRN innovative decontamination system, which could reduce both the physical and physiological load at individual level, and the overall logistic burden at unit level.

It would have been a multipurpose decontaminant for a timely and efficient decontamination process that could satisfy the following fundamental requirements:

- Broad-Spectrum Decontaminant;
- Multi-scale decontamination system;
- Prompt-for-displacement;
- Good performance in different operational condition;
- Low environmental impact, and also
- Continuous research for developing new user requirements.

The result of our R&D is a multi-purpose decontaminant for CB(RN) that has become an international reference.

Chemical, biological, radiological substances and nuclear materials

CBRN and hazmat incidents involve the accidental or deliberate release of chemical, biological or radiological weapons. Also, nuclear accidents related to the detonation of a nuclear device that would produce fallout and contamination over a wide area.
CBRN substances can be divided into broad categories:

TIC – such as chlorine, ammonia, hydrogen cyanide, phosgene, pesticides and other agricultural chemicals

C – such as the nerve agents, sarin, soman, tabun, cyclosarin and VX, and the blister agents mustard and lewisite

B - Biological substances. A number of biological agents do not pose a contact hazard unless the skin is cut or abraded; however they are hazardous if inhaled or ingested.

Biological agents of interest include:

- Bacteria, such as Bacillus anthracis (anthrax) and Yersinia pestis (plague);
- Viruses, such as Variola (smallpox), and filoviruses (Ebola and Marburg);
- Fungi, such as Coccidioidomycosis (Valley fever);
- Toxins, such as ricin and botulinum toxin.

R – Radiological substances emit three main types of radiation: alpha, beta and gamma. Each has a differing ability to penetrate matter. Exposure to radiation can produce both short and long term damage to health.

N - Radioactive fallout may affect large numbers of buildings over a wide area to the extent that they would require extensive decontamination.

Chemical, biological and radiological substances vary widely in their physical and chemical properties, which challenge decontamination of people, materials and the environment.

CBRN Decontamination

A CBRN incident creates unique residual risks that may require decontamination. According to NATO Standard, decontamination is the process of making any person, object or area safe by absorbing, destroying, neutralizing, making harmless or removing chemical or biological agents or, Toxic Industrial Materials (TIM) or by removing radioactive material clinging to or around it[1].

CBRN decontamination is a progressive operation that should be initiated as quickly as possible to be effective. Decontamination of personnel normally takes priority[2].

The following summarizes the levels of active decontamination operations:

a) Immediate decontamination. Decontamination carried out by individuals immediately upon becoming contaminated. It is performed in an effort to minimize casualties, save lives, and limit the spread of contamination. Also called emergency decontamination.

b) Operational decontamination. Decontamination carried out by an individual and/or a unit, restricted to specific parts of operationally essential equipment, materiel and/or working areas, in order to minimize contact and transfer hazards and to sustain operations. This may include decontamination of the individual beyond the scope of immediate decontamination, as well as decontamination of mission-essential spares and limited terrain decontamination.

c) Thorough decontamination. Decontamination carried out by a unit to reduce contamination on personnel, equipment, material, and/or working areas equal to natural background or to the lowest possible levels, to allow the partial or total removal of personal protective equipment and to maintain operations with minimum degradation.

Table 1. Decontamination Levels/Techniques

Levels	Techniques[1]	Best Start Time	Performed by	Advantages
Immediate	Skin decon Personal wipe down Operator's spray down	Before 1 minute Within 15 minutes	Individual Individual or crew	Stops agent from penetrating.
Operational	MOPP-gear exchange[2] Vehicle washdown[3]	Within 6 hours	Unit Crew or decon team	Provides possible temporary relief from MOPP[4, 5].
Thorough	DED and DAD DTD[4]	When mission allows reconstitution	Decon Unit	Provides probable long-term MOPP reduction with minimum risk.

[1] The techniques become less effective the longer they are delayed.

[2] Performance degradation and risk assessment must be considered when exceeding 6 hours.

[3] Vehicle wash-down is most effective if started within 1 hour.

[4] (DED) Detailed Equipment Decon, (DAD) Detailed Aircraft Decon and (DTD) Detailed Personnel Decon.

[5] MOPP (Mission Oriented Protective Postures, protective gear used by U.S. military personnel in a toxic environment).

Responders to Psychological and Physical Factors Affecting Decontamination

The consequences of CBRN emergencies can stretch local and national capabilities to their maximum extent. First responders remain responsible to mitigate the consequences of emergencies involving life, property and the environment. Due to the nature of CBRN incidents, the response of normal people to traumatic events is psychological and brings a physical distress. First responders, although well trained, a fortiori may suffer psychological and physical distress, when exposed to extremely hazardous environment.

In addition, stress is caused by personal protective equipment (PPE), designed to provide protection from serious injuries or illnesses resulting from contact with chemical, biological, radiological, physical, or other hazards.

While the use of PPE is necessary during CBRN emergencies, a number of physical, psychological, environmental and biological safety concerns may occur. One of the first challenges posed by PPE is the restriction to movement, add weight and bulk, and constrain movement, and also increase energy expenditure and lead to fatigue. Gloves can reduce a responder's dexterity and the ability to grip objects. Sensory perception is also reduced while wearing personal protective equipment. Hoods limit the ability to hear. Vision may be reduced while wearing mask. While wearing respiratory protection, such as masks or respirators, communication with other responders can be difficult. All of these factors can impact a responder's ability to work, and their risk for injury. Heat-related illnesses can result when wearing PPE clothing where body evaporation of sweat is limited, particularly when working in high temperatures environment[3].

It is well known that physical and psychological stress affect memory and other cognitive functions. For this reason all personnel under "complex and dangerous circumstances" requires simple operational methodologies and reliable equipment that do not require complex choices. Decontamination also must meet these important requirements.

Technical Factors Affecting Decontamination

Detection aims to establish the release or the presence of a CBRN agent in a given area/location. Detection mechanisms are necessary in the three stages of a CBRN incident, before, during and after. Before an incident, CBRN detectors allow continuous monitoring as early warning. During the incident, the detectors are kept on site in order to allow first responders to identify the nature and extent of the release and to organize the response accordingly. Once the incident has occurred, the detectors are indispensable in order to confirm the results of early identification, collect evidence and make sure the area was decontaminated.
However, the detection does not provide a complete and ideal solution in all of these cases, a concept of use of the detectors also needs to be developed, i.e. the detectors' properties and the ways in which generated data will be interpreted and used in decision-making. Most of the existing technology is flawed and no country can claim a full coverage of territory or infrastructure. The risk is that the partial implementation of imperfect technology would create a false sense of security. Detectors currently available on the market differ depending on the agent they are intended to identify. The goal of having a detector for all uses is still unrealistic. The detectors also differ in the way they operate; the main distinctions are between standoff and point detection and between fixed and hand-held detectors. Fixed detectors are used when nodal points or critical infrastructures are identified as highly sensitive. Hand-held instruments are particularly used in widely dispersed areas such as airports or seaports, or in targeted search situations.
A deliberate or accidental CBRN incident includes all or some of the following technical issues:

- Extremely hazardous environment;
- Initial ambiguity and/or delay in determining the type of material involved;
- Potential combination of CBRN materials, each presenting different response requirements;
- Narrow time frame in which to administer interventions/treatments;
- Need for specialised detection equipment;
- Need for timely, efficient and effective decontamination systems.

That means that the relationship between detection and decontamination can be problematic for the people tasked to deal with the CBRN incident.
According to NATO documents, decontamination is the process of making any person, object or area safe by absorbing, destroying, neutralizing, making harmless or removing chemical or biological agents or by removing radioactive material clinging to or around it. Along with avoidance and protection, decontamination is an essential part of CBRN defence.

The decontamination systems implemented by military and civilian agencies can be summarized in three main categories:

a) Multicomponent decontaminant is when the components are mixed just before use; often the required composition varies in dependence of the specific CBRN agent involved;
b) Different decontamination products for the specific CBRN agent;
c) Multi purpose and multi contaminating agent (all in one)

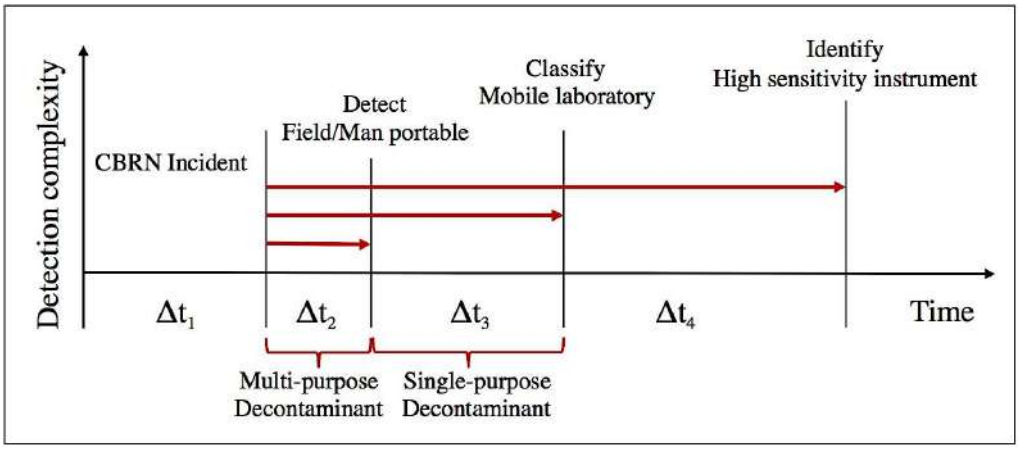
In a contaminated environment the diagram in Figure 1 represents the relationship between detection and decontamination. Decontamination, in this contest, is considered the process of removing or neutralizing contaminants accumulated on different surfaces and materials.

The diagram shows qualitatively the time when to start the decontamination. This time will be different depending on the category of decontaminant adopted. For the case a), with the need for mixing just before use two or more components, sometimes in a different ratio, it entails a considerable logistic effort, similar to the case b), where all the chemicals must be available on the field at the same time.

Inventory management is complex and the possibility of errors is high[4].

From the operational point of view, on both cases a) and b), before being able to administer the decontamination, it will be necessary to have the proper results from high level detection, consequently the related intervention time will be relatively long. On the contrary, a type c) decontaminant reduces significantly the disadvantages related to both types a) and b).

Figure 1. Estimation time in which decontamination must be administered



Both mentioned systems require personnel performing decontamination to make choices in the field, such as the proper decontaminant's formulation and the related equipment. The possibility of making mistakes increases due to the memory and the other cognitive functions deficits. The chances of making mistakes and cause accidents due to fatigue are significantly high.

Time is a key factor influencing the adhesion of the CBRN agent on surfaces; either surfaces of protective clothing or surfaces that need to be decontaminated. Contaminants can be located on the surface of PPE or permeate into the material. Contaminants may be easy to detect and remove/destroy; however, contaminants that have permeated a material are difficult or impossible to detect and remove. If contaminants that have permeated a material are not removed/destroyed by decontamination, they may continue to permeate the surfaces of the material where they might cause an unexpected exposure.

A time related factor is the contact time. The longer a contaminant remains in contact with a surface, and thus the greater is the contact, the highest is the probability and extent of permeation. For this reason, minimizing the contact time is one of the most important purposes of the decontamination. The same is true for the agent concentration influence penetration by diffusion. Molecules flow into the materials from high concentration to low concentration. An increase in temperature generally increases the rate of diffusion of contaminants. The size of contaminants molecules and the pores increase and the contaminating molecule becomes smaller, the material permeation increases. As well as a low viscosity liquid tends to permeate more easily than high viscosity liquid or solid[5].

A Multi-purpose decontaminant can be defined as a chemical formulation that can be used to decontaminate a wide range of CB(RN) agents, and used for all levels of decontamination, but which may sometimes be restricted for the Thorough Detailed Troop Decontamination (DTD), Detailed Equipment Decon (DED), Detailed Troop Decon (DTD) operations[6]. The DTD is the process of decontaminating individual fighting equipment to negligible risk and removing contaminated MOPP gear from the troops.

Our R&D has been focusing on a multipurpose decontaminant that could satisfy the following fundamental aspects:

- Broad-Spectrum Decontaminant (multi agent);
- Multi-scale decontamination system, with the same decontamination product;
- Prompt-for-displacement system;
- Good performance in different operational condition;
- Low environmental impact;
- Continuous research for developing user's new requirements.

All these features lead to reduce, at individual level, the physical and physiological load and, at unit level, the overall logistic burden.
The result of our R&D is a multi-purpose CB(RN) decontaminant that has become an international reference.

Multi-purpose Decontaminant

The decontamination formulation, developed in our laboratories and named BX24, has proved to be active against a broad spectrum of chemical warfare agents, TICs, biological agents, and effective in the removal and capture of radioactive dust from contaminated surfaces. The approach to the chemical and biological agents is “detoxification”; because detoxification of radiological material is not possible.

Our efforts on radiological removal would concentrate on reducing the volume of radiological waste during the decontamination (removal) process. With regard to mitigation of the effects of chemical and biological hazards in given situations, we sought to mitigate risk by the preventive application of our universal decontaminant BX24. For example on a generalist, or specialist CBRN vehicle, which was imminently at risk, or had to enter a contaminated area we could apply BX24. When dried, it would serve as a detoxifying layer for a couple of hours, to break down and neutralize contaminating hazards and ease the burden of post-mission detoxification. Whatever the situation, every effort must be made to reduce the time between contamination and decontamination. Then there are fixed sites, always important and often critically so. In such circumstances there will be a compelling case for detoxification as soon as possible; just as in the Homeland Security domain there will be the need to rapidly detoxify urban areas, critical sites and personnel, from mass decontamination to the emergency services themselves to the decontamination of VIPs, amongst other scenarios[7].

We have helped to develop modular and multifunctional solutions to cater for a spectrum of operations from small to medium to large scale, based on the multipurpose decontaminant BX24.

CBRN incidents may be small scale, in places that are difficult to access or where there are constraints on deployment or there may be a requirement to provide vehicle-borne protection, with a concept similar to a fire extinguisher. Under such circumstances there are man-portable solutions or for very small scale areas, and handheld devices, both containing the universal decontaminant BX24.

‘Rapid Intervention CBRN Trailer’ offers an excellent example of medium scale multi-functionality for a great number of scenarios; ideal as a Unit Decontamination System. The same solution could be used for incidents involving warfare agents in the field or on static sites, a chemical spill, or water, fire and bio-safety within a refugee camp.

At the higher end of the scale, there is a full spectrum decontamination system designed to cater for the exceptional demands of major emergencies or combat operations. It offers the very best technology for rapid decontamination of combat vehicles, aircraft, and personnel, including casualties, equipment, external infrastructure and terrain. It is a true ‘System of Systems’, delivering not only a multi-functional decontamination capability, but also the ability to neutralize chemical and biological agents with one decontaminant (eco-friendly and non-corrosive BX24) while polarizing radiological particulate. TDS 21, with its two Sanijet machines, can support four decontamination operators simultaneously and can be rapidly

re-configured and deployed to meet multiple operational priorities. While the CBRN shelter is shown integrated onto a High Mobility Vehicle, it is also within the payload for transportation by a support helicopter.

Unquestionably, the purpose is to keep things simple and lightening the burden on the individual soldier, and more widely, to reduce the overall logistic burden at unit and formation level. Even without a CBRN environment, given the requirement for ballistic protection, things can be mighty challenging, especially in hot climates. Add the burden of CBRN protection and you have a potentially lethal physiological cocktail. Stir in the toxic danger and psychological factors kick in as well, hence the critical importance of effective, simple training and equipment solutions.

Conclusion

Research and Development has always been a significant priority and strength against the CBRN emergency. Universities offer a fantastic source of knowledge and innovation, as does collaboration with international CBRN scientific centres of excellence. We are in the early stages of looking at further extending a 'proof of principle' that we already know to be highly effective, and in line with our philosophy of further easing the burden on the operator. We have already successfully expanded into other areas, such as solutions for sensitive equipment decontamination[8], mobile laboratories and CBRN, survey and scene assessment vehicle, integrated onto a battle proven and ballistically protected platform.

References

[1] Di Steven L. Hoenig, Handbook of Chemical Warfare and Terrorism, 130 Cremona Drive, Santa Barbara, CA 93117
[2] NATO Document - STANAG 4653 – AEP 58 Ed. 1 "Decontamination Triptych", 20.09.2005

[3] Armando S. Bevelacqua and Richard H. Stilp, Terrorism Handbook for Operational Responders, Emergency Film Group, Edgartown, MA, January 1998

[4] C.M. Boone, J.A. Cordia, L.F. Chau and R.M. van den Berg, Development and optimization of test methodology for the decontamination of chemical warfare agents, toxic industrial chemicals and radionuclides, TNO report DV 2006-A512

[5] https://www.osha.gov/SLTC/hazardouswaste/training/decon.html

[6] http://www.globalsecurity.org/wmd/library/policy/army/fm/3-5/fm3-5.pdf

[7] S. Miorotti, R. Bonora, and others, SX34 and the decontamination effects on chemical warfare agents (CWA), WSEAS Transactions on Environment and Development, E-ISSN: 2224-3496, Volume 11, 2015

[8] Renato Bonora, Chemical Warfare Decontamination of Eurofighter Materials, Combating WMD Journal, Issue 3, US Army Nuclear and Combating Weapons of Mass Destruction Agency Fort Belvoir VA, 2007, USA

Addressing Bio and Chemical Risk

Anna Giovanetti

ENEA, Territorial and Production Systems Sustainability Department

Each year about 108 million cargo containers are transported through seaport entailing the risks of illicit trafficking as well as CBRN threats. To be prepared for countering this risk it is necessary to know the different aspects of this risk and what is needed to do.

Biological threat

Bio-weapons

Biological weapons are deadly pathogens – bacteria, microorganisms or viruses – or toxins that can be deliberately released in order to inflict harm. These types of agents attract terrorists because of their virulence, toxicity, transmissibility and lethality, are relatively cheap to produce and relatively easy to store and transport. Unlike chemical agents, biological agents can be grown from a tiny initial supply. Besides naturally existing pathogens, also engineered organisms can be produced, up to 1,000 toxins could be made of natural or genetic sources, although not all of them would be suitable for use as biological weapons.

Although commonly termed "bioterrorism" the purposes of such attacks are not necessarily intended to intimidate government structures, but can also be motivated by religious, political, or ecological ideologies. In 1984 followers of Bhagwan Shree Rajneesh contaminated with Salmonella salad bars at local restaurants to incapacitate voters in The Dalles (OR), poisoning 751 individuals. In the autumn of 2001 letters containing anthrax spores were mailed to several news media offices and two Democratic U.S. Senators, killing five people and infecting 17 others.

Dispersion, tramsmission and incubation

The most effective and alarming mode of transmission for biological agent is via aerosol dissemination, in particular if the particle size is in the range of 1–5 μm able to penetrate deep in the lung. Aerosol dissemination of the plague (Yersinia pestis) or anthrax (Bacillus anthracis) over Washington DC, could lead to the death of 1–3 million people. In some countries, biological agents have been engineered for optimal dispersal and dissemination as small-particle aerosols. Other routes of dissemination, such as through the water or food supply, are less likely, due to constant monitoring and significantly higher amounts of the biological agent required to cause harm or death.

The incubation periods, ranges from 48 h for respiratory anthrax, to 21 d for Q-fever. Incubation may be an asset because it provides a window for quarantine and treatment of the victims and vaccination of others but also a challenge because identification of the disease is often difficult, while timely detection of an attack is crucial to allow for the deployment of response mechanisms, including medical countermeasures. In fact in early stages many diseases present flu-like symptoms and patients are thus likely to go on with their normal lives, which could cause widespread contamination in the case of transmissible diseases.

A distinction needs to be made between contagious agents (such as cholera, plague, smallpox, or typhus), which can be transmitted from person to person, and non-contagious agents (such as anthrax, botulism, tularemia, or ricin). The response to a contagious agent exposure would require a potential quarantine of affected population, raising in this way also legal issues.

Bio-agents' categories

Based on the ease of transmission, severity of morbidity, mortality and likelihood of use, biological agents can be classified into three categories (Table 1).

The highest-priority agents, Category A agents, include organisms that pose a risk to national security because they can be easily disseminated or transmitted person-to-person; cause high mortality and subsequently have a major public health impact; might cause public panic and social disruption; require special action for public health preparedness.

Category B agents includes foodborne or waterborne pathogens and those that are moderately easy to disseminate; cause moderate morbidity and low mortality; require enhancements of diagnostic capacity and disease surveillance. These categories include new or emerging pathogens.

Category C agents includes emerging pathogens that could be engineered for mass dissemination in the future because of their availability, easiness of production and dissemination, potential for high morbidity and mortality and major health impact. Preparedness for Category C agents requires to improve disease detection, diagnosis, treatment, and prevention.

Table 1. Categories of biological agents

CATEGORY A	CATEGORY B	CATEGORY C
Variola major (smallpox) Bacillus anthracis (anthrax) Yersinia pestis (plague) Clostridium botulinum toxin (botulism) Francisella tularensis (tularemia) Hemorrhagic fever (e.g., Ebola, Marburg, Lassa viruses)	Foodborne or Waterborne agents Coxiella burnetti (Q fever) Brucella species (brucellosis) Burkholderia mallei (glanders) Alphaviruses Venezuelan encephalomyelitis eastern and western equine encephalomyelitis Ricin toxin from Ricinus communis (castor beans) Epsilon toxin of Clostridium perfringens Staphylococcus enterotoxin B Salmonella species Shigella dysenteriae Escherichia coli O157:H7 Vibrio cholerae Cryptosporidium parvum	Nipah virus Hantaviruses Tickborne hemorrhagic fever viruses Tickborne encephalitis viruses Yellow fever virus Multidrug-resistant Mycobacterium tuberculosis

Preparedness and Response

The anthrax attacks of 2001, the SARS outbreak in 2004, and the recent H1N1 swine flu outbreak have pointed out that an essential component of preparedness for bioterrorism includes surveillance methods capable to detect and monitor the course of an outbreak and thus minimize associated morbidity and mortality. Preparedness for and response to an attack involving biological agents are complicated by the large number of potential agents (most of which are rarely encountered naturally), their sometimes long incubation periods and consequent delayed onset of disease, and their potential for secondary transmission.

In addition to naturally occurring pathogens, agents used by bioterrorists may be genetically engineered to resist current therapies and evade vaccine-induced immunity.

In the event of a bioterrorism attack, an effective response will require focusing necessary public health resources on managing the outbreak of an infectious disease, such as i) bio-detection; ii) surveillance and epidemiologic expertise; iii) use of specialized drugs, vaccines, and other medical supplies; iv) laboratory diagnosis skills; v) medical recommendations, such as prophylaxis guidelines and vi) various quarantine-related issues.

Bio-detection: agents are colourless and odourless thus difficult to detect. Available instruments are usually large, slow and expensive. The more reliable the detection instrument, the longer it takes to identify the defined threat. Bio-detection comprises: standoff detectors; point detectors; epidemiological data. Biological agents have different properties and each test must be tailored to recognise a specific pathogen. In some cases, even a very small quantity of pathogen will cause disease. In those cases (as for example, in the case of the tularaemia pathogen, which requires as few as 10 organisms to infect), sensors need to be sensitive enough to detect even a minimal presence of pathogens. As example, recently it was set up a device for detecting Hazardous Materials/Weapons of Mass (http://biofiredefense.com/razorex/) able to simultaneously test in 30 min up to 12 real time PCR samples of agents such as Anthrax, Brucella melitensis, Botulism A, Coxiella, E. coli 0157, Tularemia, Ricin, Smallpox, Plague, Campylobacter, L. monocytogenes, Salmonella, Cryptosporidium Target 1, and E. coli 0157.

Surveillance and epidemiologic investigation. After an event, a proper emergency response to an epidemic will require enhanced surveillance activity to manage the outbreak and to monitor progress. A bioterrorism event most likely would cause unusual cases of illness or death. An observant physician, veterinarian, laboratory technician, or surveillance data-entry clerk may be critical to early detection and communication the appropriate authorities.

Laboratory diagnosis. Laboratory confirmation of a specimen will be extremely important during a bioterrorism response. Plans should be in place to facilitate sample collection, transport, testing, and training for laboratory readiness for bioterrorism. The laboratories in the network must be identified by increasing levels of sophistication: Level A labs are public health and hospital laboratories with a certified biological safety cabinet as a minimum; Level B labs possess Biosafety Level (BSL) 2; Level C labs are BSL-3 facilities with the capability to perform nucleic acid amplification molecular typing, and toxicity testing; Level D labs can validate new assays, detect genetic recombinants, provide specialized reagents, securely bank isolates, and possess BSL-3 and BSL-4 bio-containment facilities. For bioterrorism events affecting civilian populations is necessary to utilize the Level D laboratories.

Medical management. The key issues associated with medical management of bioterrorism victims will be the provision of preventive services and the medical treatment of patients. Preventive services involve the provision of antibiotics, vaccines, or other medications to prevent disease and death in exposed victims. Plans will need to predict supplementary staffing needs and identify auxiliary staff, determine equipment and resource requirements, and identify technical assistance that may be required. In addition, provisions for properly documenting the treatment of victims should be specified. The proper application of mass prophylaxis or immunization will involve complex coordination with other emergency response authorities and a vigorous campaign to inform the public; a specific list of the emergency personnel should be developed in advance and policy should be developed to address priority emergency prophylaxis for emergency personnel. If medication shortages develop during the early phases of the incident, the medication issuance may need to be limited to a 1- or 2-day, pending identification of the agent. For the at-risk population, mass immunization may be needed. Recommendations for immunization balance scientific evidence of benefits, costs, and risks against the risk posed by the biological agent. Planning for mass immunization should involve linkage with public health departments at the state and local levels.

Emergency public health measures. Responding to a bioterrorism incident or large-scale infectious disease outbreak may require the use of a variety of emergency public health measures. These may include quarantine, isolation, closing public places, seizing property, mandatory vaccination, travel restrictions, and disposal of the dead. The most critical public health responses will be those taken immediately. Thus health officials and their lawyers should review the statutes, regulations, and ordinances that authorize these emergency public health measures and develop legally sound procedures for executing them.

Environmental issues

In general, environmental issues are not critical in a biological event, in fact many biological agents live for only a short time outside the human body being sensitive to environmental conditions, including heat and light, which makes bio-decontamination unnecessary as a rule. Spore forming agents (e.g., anthrax) are more persistent; however, these biological agents occur naturally throughout much of the United States without causing outbreaks. Where these agents occur naturally, background levels are rarely known; thus, sampling is of little value.

Future perspectives

It is critical to remain vigilant about potential bioterrorism attacks and rather consider proactive than reactive measures. After the anthrax letters in 2001 significant investment has been made to increased surveillance, awareness, and preparedness. We currently do not have the optimal tools to provide us with the impact of multiple concurrent large-scale bioterrorism attacks and which steps would be crucial in response to them. The legitimate desire to improve response and develop new treatments for biological agents (for some, we do not have any treatment options aside from supportive care, e.g., ricin) needs to be weighed against a potential diversion of agents. Widespread surveillance through biosensoring technology is becoming a more realistic goal. There are mobile rapid-screening units available that allow for the preliminary detection of biological agents that may soon become more frequently used. Finally, an as-yet unresolved issue is emerging pathogens and biological toxins. While the CDC's category A biological agents remain the most likely to be disseminated at this time, little is known about new bacterial strains or viruses that may be utilized by larger organizations against a nation or population. The intelligence community has to be aware and should monitor such potential developments, since we currently have no effective response or even ability to detect some of these agents.

Chemical threat

The Organisation for the Prohibition of Chemical Weapons (OPCW) defines chemical weapons as any toxic chemical or its precursor that can cause death, injury, temporary incapacitation or sensory irritation through its chemical action. Chemical agents are categorised according to their effects as: Nerve agents, such as sarin and VX; Blood agents, such as hydrogen cyanide; Blister agents, such as sulphur mustard and other mustard agents; Choking agents, such as phosgene; Irritants, such as tear gas. Chlorine, mustard gas and sarin are among the most well-know and regularly used weaponised chemicals.

Catastrophic chemical event

Several industrial accidents causing many casualties highlight the potential impact of a terrorist attack on chemical storage sites or transport vehicles. In 1984, a methyl isocyanate leak at a Union Carbide plant in Bhopal, India, killed as many as 5,000 people and injured more than 14,000. In US since 2002, three major chlorine gas leaks have occurred causing several deaths. The most serious incident of chemical terrorism until today was the attack in the Tokyo subway in 1995 which resulted in 13 fatalities and approximately 5,000 casualties. The Aum-Shinrikyo sect synthesized the organophosphate sarin and deployed it against civilian targets in Japan.

Triage

A catastrophic event may cause mass casualties in the order of several thousand, producing an imbalance between medical needs and available resources, thus robust triage strategies are needed. Triage is the process to classify and prioritize victims according to predetermined severity algorithms to ensure the greatest survivability within a context of limited resources. The primary goal is to identify patients who have the greatest chance for survival with healthcare intervention and to optimally use limited resources. Triage decisions rely on rapid assessments (> 1 min) for every patient, determining a priority category, and visibly identifying the categories (tags attached to each patient) for rescuers who will treat and/or transport the patients.

Data used for triage decisions include physiologic indicators, injury mechanisms, resources, trauma, mental status, ability to walk, respirations, and pulse. Patients who can walk, are dead or non-salvageable are immediately identified and do not receive immediate care. The remaining patients are assessed for immediate or delayed treatment and transport to a medical treatment facility.

There are different types of triage procedures depending on the type of emergency, the age of the exposed subjects and the resources available.

Preparedness

The worst time to determine the appropriate actions in response to an emergency situation is during the emergency, thus, it is critical that health department officials clarify the preparedness roles and responsibilities and identify likely response activities.

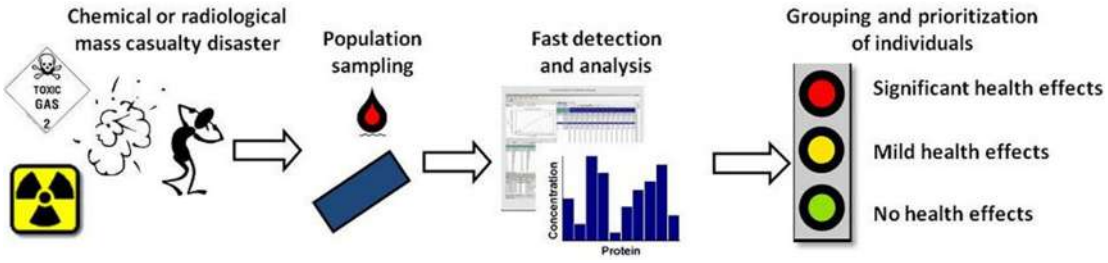
Preparedness encompasses the various activities that can be taken before an emergency. Such activities define and enhance the response system and range from expanding existing surveillance systems to developing and maintaining Emergency Operating Procedures.

Emergency involving chemical exposures may cause immediate respiratory symptoms or evidence of a toxidrome with no apparent traumatic injuries. Many chemical materials such as chlorine and phosgene have a latency period resulting in rapid deterioration of victims after initial triage. Current triage systems do not take this latency period into account, patients may initially triage into a delayed category for treatment and then quickly deteriorate with respiratory distress.

Biomarkers

To assess acute and chronic effects of exposures for chemical agents there is a need for organ specific biomarkers and clinical and epidemiological databases.

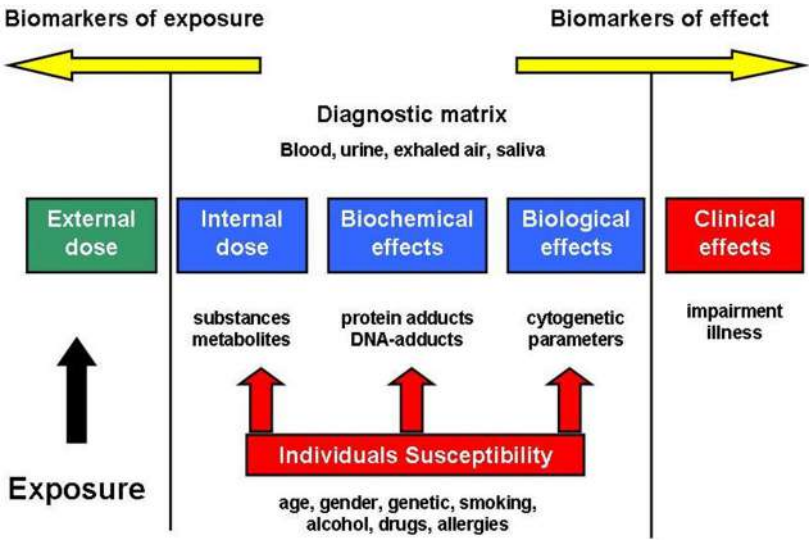
Conceptual flow chart for exposure assessment of mass casualties



From Göransson Nyberg, Stricklin, Sellström 2011

2.4.1 Biotechnology is a broad discipline in which biological processes, organisms, cells or cellular components are exploited to develop new technologies; its very rapid growth during the 1990s is due to the integration of the life sciences with other enabling technologies such as computers and analytical chemistry. After the sequencing in 1999 of the human genome, a new era of biotechnology known as "genomics" was ushered into research and development. Rapid diagnostic tests, reliable and easily to use in mass casualty situations are expected to be realized.

2.4.2. Biomonitoring is a valuable tool for assessing human exposures to chemical contaminants. Biomarkers can measure exposure, effect, or susceptibility. The ideal biomarker should be sensitive, specific, biologically relevant, practical, inexpensive, and readily available. Seldom does a biomarker meet all of these criteria, and most biomarkers represent a compromise. Biomarkers include biochemical, molecular, genetic, immunologic, or physiological signals of events in biological systems. The events are depicted as a flow chart between an external exposure to a chemical and resulting clinical effects.



Source: from Göransson Nyberg, Stricklin, Sellström 2011

Exposure is generally assessed by measuring parent compound in blood, whilst urinary metabolites can be shared with other substances. Adducts to macromolecules or DNA are particularly useful when assessing exposure to genotoxic compounds, because they reflects the dose that has avoided detoxification and reached its target.

Biomarkers of effect should be non-invasive and reflect early responses preceding functional damage. Analytical methods must be reproducible, easy to perform and applicable to a large number of samples. Biomarkers should identify early and reversible biochemical events that may also be predictive of later response.

Individual's susceptibility may arise from genetic or from non-genetic factors such as age, concomitant disease state, diet, or dietary supplementation. Genetic polymorphisms are biomarkers of susceptibility. The rapid advances of the Human Genome and Environmental Genome projects are generating a long list of genes and their variants (polymorphisms). New technologies such as microchip arrays allow researchers to understand which genes are perturbed and to explore patterns of gene expression.

Organs' toxicity

Many toxic chemicals can damage the respiratory airways, with potentially life-threatening effects.

Ammonia, hydrochloric and sulfuric acid, vesicants and other corrosive agents affect the upper airways. Inhalation of these chemicals can cause acute inflammation, painful ulcerations, increased secretions, and difficulties in breathing and swallowing.

Secondary bacterial infections may further exacerbate the initial injury. Symptoms may be immediate or delayed. Vesicating agents such as sulfur mustard, nitrogen mustard, lewisite, and caustic industrial chemicals can cause severe blistering and burns to the eyes, mucous membranes, skin, as well as chronic eye inflammation and blindness. Sulfur mustard can cause tissue damage within minutes. Physical injury from other vesicating agents may not be evident for several hours and may result in delayed recognition of exposure. A variety of chemicals are known to affect the nervous system. Some directly target neural signaling pathways such as classic nerve agents (sarin, soman, tabun, and VX), organophosphate pesticides and some animal toxins, or indirectly such as metabolic poisons (cyanide) by disrupting cell respiration. Diagnosis following exposure to nerve agent is generally based on clinical observations depending on type of chemical, level of exposure and time elapsed. Exposure to nerve agents can trigger seizures and loss of consciousness, other acute effects include: muscle paralysis, cardio respiratory depression, and massive secretion from mucous membranes, eye irritation, behavioural effects, cognitive difficulties and also serious long-term neurological effects, including neuronal degeneration.

Environmental issues

The need to perform environmental decontamination for chemicals depends on the chemical involved. Persistent chemicals can remain in the environment for long periods and must be actively removed through decontamination. Other chemicals are more volatile and will evaporate without outside intervention, thus eliminating the need for decontamination.

Future perspectives

The development of new and improved medical technologies utilizing recent developments within medicine, biotechnology and intelligent communication technology is foreseen. Diagnostic tools should be robust, simple, efficient and cheap in order to be produced and implemented.

The development of new tools depends on commercial realities. If the market is lacking it has to be politically augmented and realized through public investments.

Interest in saliva as a diagnostic medium has increased dramatically as saliva and other oral fluids have been shown to reflect systemic fluid levels of hormonal, immunological and toxicological molecules and contain biomarkers associated with infectious and neoplastic diseases, allowing the detection of a broad range of chemical from occupational exposure, accidents or acts of war and terrorism.

Researchers are working to develop a simpler, portable microanalytical sensor system to quickly diagnose pesticide exposure in humans and a modelling method than can estimate the dose.

References

1. Biological and Chemical Terrorism: Strategic Plan for Preparedness and Response Recommendations of the CDC Strategic Planning Workgroup 2000 https://www.cdc.gov/mmwr/preview/mmwrhtml/rr4904a1.htm

2. CDC The public health respons to biological and chemical terrorism interim planning guidance for state public health officials 2001 https://emergency.cdc.gov/Documents/Planning/PlanningGuidance.PDF

3. Göransson Nyberg A, Stricklin D, Sellström Å Mass Casualties and Health Care Following the Release of Toxic Chemicals or Radioactive Material—Contribution of Modern Biotechnology Int. J. Environ. Res. Public Health 2011, 8, 4521-4549

ENEA

Promotion and Communication Service

www.enea.it

April 2017