INTERNATIONAL JOURNAL OF CRITICAL INFRASTRUCTURE PROTECTION 7 (2014) 100–111

Available online at www.sciencedirect.com

ScienceDirect

www.elsevier.com/locate/ijcip

A framework for studying mortality arising from critical infrastructure loss

Athol Yates

Institute of Civil and International Security, Khalifa University, P.O. Box 127788, Abu Dhabi, United Arab Emirates

ARTICLE INFO

Article history:
Received 5 October 2012
Received in revised form
28 November 2013
Accepted 1 April 2014
Available online 5 April 2014

Keywords:
Critical infrastructure loss
Deaths
Mortality chain model

ABSTRACT

A key rationale for critical infrastructure protection policy around the world is that the critical infrastructure must be protected because its loss can lead to fatalities, and it is claimed, a large loss of life in some cases. However, little academic attention has been given to understanding the link between critical infrastructure loss and mortality, meaning that the validity of this rationale is uncertain. The limited study of the mortality impacts of critical infrastructure losses stands in contrast to the significant volume of research on the economic impacts of a critical infrastructure loss.

This paper conducts an analysis of this neglected area. It identifies critical infrastructure protection policy rationales related to protecting human health in the United States, Canada and United Kingdom. It proposes a conceptual mortality chain model that links the loss of a critical infrastructure to a death. The model has four stages: (i) initiating circumstance; (ii) actual/anticipated critical infrastructure loss event; (iii) hazards; and (iv) cause of death.

The paper also proposes conceptual and operational definitions of critical infrastructure death, which are essential to undertaking comparative critical infrastructure mortality analyses. The conceptual definition of a critical infrastructure death is one in which an actual or anticipated critical infrastructure loss event results in a premature death. A critical infrastructure loss event is an event resulting in: (i) a critical infrastructure being destroyed, damaged or affected so that it generates physical forces; or (ii) a loss of critical infrastructure service continuity. Examining anticipated critical infrastructure loss events, as well as actual ones, are important because deaths sometimes occur as people prepare for an anticipated critical infrastructure loss.

The operational definition, which is used to identify instances of critical infrastructure deaths fitting the conceptual definition, has four criteria. The first is that a complete mortality chain needs to exist linking a critical infrastructure loss event to an underlying cause of death, where each stage of the mortality chain is related to the previous one. The second is that each stage of the mortality chain must precede the following stage in time. The third is that the critical infrastructure loss event needs to be a necessary element and that, without it, the death would not have occurred when it did. The fourth criterion is that the death needs to occur within a specific period – from two days prior to the actual/anticipated critical infrastructure loss event to one year from the end of the acute phase of the critical infrastructure loss event. However, the period from two days before to fourteen days after the critical infrastructure loss event is the period of greatest interest for critical infrastructure deaths, because this is the time period when the majority of deaths occur.

E-mail address: athol.yates@kustar.ac.ae

http://dx.doi.org/10.1016/j.ijcip.2014.04.002

The definitions given above along with the conceptual mortality chain model form the critical infrastructure mortality framework that can be used to study the mortality arising from a loss of a critical infrastructure. The application and utility of the framework are demonstrated by applying it to the 40 victims of the 2012 Hurricane Sandy in New Jersey. The framework provides the foundation upon which comparative mortality studies can be undertaken to determine how, when and why people die from critical infrastructure loss events. This information is essential to being able to undertake evidence-based risk analysis and improve decision making focused on preventing deaths from actual and anticipated critical infrastructure loss events.

1. Introduction

The critical infrastructure is the backbone and arteries of all modern economies. Sometimes described as lifelines to reflect the essential services it supplies, the critical infrastructure provides the vital services that allow advanced societies and economies to operate effectively and efficiently. Without it, many attributes of modern societies could not exist, such as globalized supply chains, just-in-time production and consumption, worldwide communications and high-quality health care. Given the lack of a standard definition of critical infrastructure across countries [4], rather than attempting to define the term, this paper assumes that the critical infrastructure includes the energy, water, telecommunications, transportation, health, emergency services and chemical sectors.

Given the dependence of society on the critical infrastructure, its loss can have significant harmful impacts. In some situations, the harm can be characterized as inconvenience and nuisance, such as where there is a momentary power loss that disrupts activities. However, if the critical infrastructure loss continues for an extended period of time over a large area, the harm can be substantial. For example, the North American blackout of August 2003, which resulted in electricity outages for up to two days for some customers, affected an estimated 50 million people in eight U.S. states and the Canadian province of Ontario. It cost between $4 and $10 billion to the U.S. and Canadian economies [42]. The blackout resulted in traffic light failures, subway train stoppages, business, bank and school closures, and hospital capacity degradation because these facilities had to operate on limited emergency power [23]. Reported casualties linked to the blackout include three deaths from house fires caused by candles used to provide light, one death due to carbon monoxide poisoning when a portable electricity generator was used indoors, eight patients being admitted to a New York trauma hospital due to falls in the dark [10] and 23 people who presented themselves at a Manhattan Hospital with failures of their electrically-powered medical devices [12].

This paper considers the term critical infrastructure loss event to mean an event resulting in (i) a critical infrastructure being destroyed, damaged or affected so that it generates physical forces; or (ii) a loss of critical infrastructure service continuity.

2. The mortality justification

The United States, Canadian and United Kingdom critical infrastructure protection policies all explicitly identify the large-scale loss of life as a possible outcome of critical infrastructure loss events. Of these three countries, the United States provides the most numerous references to mass mortality.

The U.S. Homeland Security Presidential Directive 7 (HSPD-7) [39] states that "it is the policy of the United States to enhance the protection of our Nation's critical infrastructure and key resources against terrorist acts that could cause catastrophic health effects or mass casualties…". Other U.S. critical infrastructure protection policy documents also identify the link between critical infrastructure loss and fatalities. For example, the National Infrastructure Protection Plan [9] notes that "direct and indirect impacts [of critical infrastructure damage from terrorist attacks and natural, man-made, or technological hazards] could result in large-scale human casualties…" The Critical Infrastructure Task Force Report [15] states that "critical infrastructures are targets that can provide attackers with high-consequence effects—potentially inflicting long-term human suffering."

The link is also identified in proposed U.S. Federal legislation. For example, the proposed Cybersecurity Act of 2012 [41] defines critical infrastructure as an infrastructure that, if damaged or accessed in an unauthorized manner, could "reasonably result in the interruption of life-sustaining services, including energy, water, transportation, emergency services, or food, sufficient to cause a mass casualty event that includes an extraordinary number of fatalities…". Likewise, the proposed Promoting and Enhancing Cybersecurity and Information Sharing Effectiveness Act (PRECISE Act) of 2012 [40] defines critical infrastructure as "any facility or function that, by way of cyber vulnerability, the destruction or disruption of or unauthorized access to could result in a significant loss of life…".

The link between critical infrastructure impacts and fatalities is also recognized in Canadian and United Kingdom critical infrastructure protection policy documents. The Canadian National Strategy for Critical Infrastructure [32] states that "disruptions of this critical infrastructure could result in catastrophic loss of life." The U.K.'s Counter-Terrorism Strategy [17] states that the critical infrastructure is important because "damage to that infrastructure can…