Contents lists available at ScienceDirect

Technological Forecasting & Social Change

journal homepage:

SafeCity — A GIS-based tool profiled for supporting decision making in urban development and infrastructure protection

Marcin Kulawiak*, Zbigniew Lubniewski

Gdansk University of Technology, Dept. of Geoinformatics, Gabriela Narutowicza 11/12, 80-233 Gdansk, Poland

ARTICLE INFO

Article history:
Received 2 August 2012
Received in revised form 26 July 2013
Accepted 28 August 2013
Available online xxxx

Keywords:
GIS
Critical Infrastructure
CARVER
GeoServer
Geovisual Analytics

ABSTRACT

This paper presents a system for analysis of municipal Critical Infrastructures, which offers integrated tools for target analysis, hazard scenario simulations and spatial analysis within a remotely accessible Web-based Geographic Information System. The system has been applied to research conducted in the city of Gdansk with the aid of blast attack, chemical leakage and flood hazard scenarios, as well as a spatial density algorithm, which highlights events in which the proximity of infrastructures influences their susceptibility to a single attack. The paper also discusses the way in which the tools provided by the system aim to assist in the processes of infrastructure vulnerability assessment, mitigating discovered risks as well as strategic planning of city development.

1. Introduction

The importance of infrastructures in the proper functioning of a city cannot be overestimated. Ever since the dawn of the industrial era, a well developed infrastructure decided the success or failure of a city's economic growth [1]. The natural consequence of infrastructure development was the creation of local clusters of interconnected services and companies [2]. This local concentration of different infrastructure sectors did not come into wider attention until the second half of the XX century, when the aftermath of World War II saw a decentralization of urban areas in the United Kingdom [3]. However, this was mainly a local trend. Globally the rapid evolution of telecommunication networks has led to the creation of a new type of infrastructure which controls access to all sorts of goods and services via software mechanisms such as passwords or biometric judgments [4]. The internet itself has been designed, in accordance with the post-war paradigms, as a dispersed network able to withstand a direct physical attack [5]. However, while the entire network may be resistant to most types of hazards, a local malfunction of several nodes (caused e.g. by a power shortage) may be enough to disconnect a small city, the consequences of which may be quite severe [6]. By the end of the last century the impact of technological development on modern municipalities has become so great that certain types of infrastructure have been recognized as essential to the proper functioning of a city.

The first formal definition of Critical Infrastructure was produced by the United States government in Executive Order 13010 issued in 1996. The document defines Critical Infrastructures as “independent, mostly privately-owned, man-made systems that function collaboratively and synergistically to produce and distribute a continuous flow of essential goods and services”. The provided services must be vital enough so that “incapacity or destruction” of one of the infrastructures would have a “debilitating impact” on citizen security [7]. This definition was later expanded in the USA National Strategy on Homeland Security (NSHS), published in 2002. This document not only contains a list of Critical Infrastructure sectors, but also makes a distinction between Critical Infrastructures and key assets, which are defined as individual targets whose “destruction would not endanger vital systems, but could create local disaster or profoundly damage” the “morale and confidence” of citizens. Such assets would include historical attractions (national, state, and local

* Corresponding author. Tel.: +48 58 3471728; fax: +48 58 3472090.
E-mail address: Marcin.Kulawiak@eti.pg.gda.pl (M. Kulawiak).

0040-1625/$ – see front matter © 2013 Published by Elsevier Inc.
http://dx.doi.org/10.1016/j.techfore.2013.08.031

monuments and icons) and other localized facilities with destructive potential or of high value to a community such as schools, courthouses and bridges [8]. Three years later, in Europe the Green Paper on the European Programme for Critical Infrastructure Protection (EPCIP) provided the definitions of Critical Infrastructures on different levels (e.g. National and European), the definition of their threats (a "threat" being any person, activity, or event with the potential to cause harm to a system or operational environment — the primary types of threats include natural disasters, accidental threats and threats of intentional or malicious nature [9]) as well as the role of their owners and operators. Both these documents also contain lists of Critical Infrastructure sectors. These, in general, are largely similar and consist of Energy, Water, Food, Public Health, Financial, Transport, and Chemical industry, Telecommunications and Research facilities [10].

The successful protection of Critical Infrastructure is a complex process, encompassing the events occurring before a threat is identified, the time during a crisis and its aftermath. Consequently, the main phases of Critical Infrastructure emergency management are referred to as Preparedness, Mitigation, Response and Recovery. As the naming indicates, the first phase involves threat identification, assessment of risk and planning of response actions, as well as training of emergency services [11]. The next phase concentrates on attempts to prevent hazards from developing into disasters, as well as reducing the effects of disasters when they occur. Mitigatory measures may involve structural means such as perimeter fencing or flood dykes, or non-structural measures such as legislation (e.g. regulating evacuation or methods of alarming the public), land-use planning (e.g. the designation of non-essential land to be used as flood zones) and insurance [12]. The Response phase takes place immediately after a disaster strikes, and includes the mobilization of necessary emergency services and first responders in the affected area. A well rehearsed emergency plan developed as part of the preparedness phase is paramount to the efficiency of the search and rescue efforts, as the fatality rates increase dramatically after the initial 72 h after impact [13]. The efforts of the final phase aim to restore the affected area to its original state, and involve rebuilding destroyed assets and repair of other essential infrastructures [14].

In the last decade the issue of Critical Infrastructure protection has received a lot of attention from researchers worldwide. Soon after the events of 9/11, it was proposed that the security of Critical Infrastructure could be improved by development of existing supervisory control and data acquisition systems (SCADA) [15]. However, it soon transpired that the rising protection costs stemming from the quick evolution of existing as well as new threats, e.g. related to cyber security, make it impossible to completely secure any given infrastructure [16].

Later research suggested that Critical Infrastructures should not be analyzed individually, but rather as a network of distributed interdependent systems [17]. The tight interconnections between these systems could, in a worst-case scenario, lead to a cascading failure [18]. Evidence supporting this theory could be found in the wake of crises such as Hurricane Katrina [19]. In consequence, new models and methods of Critical Infrastructure risk analysis have been proposed, including probabilistic models [20], graph models [21], economical models [22,23], agent-based models [24] and network models [25], as well as empirical approaches [26].

A common characteristic of all the aforementioned methodologies is that they have been developed for use by professional analysts. The task of constructing an analysis and presenting results in a meaningful way rests on the user. The available tools also relatively seldom [21,23,25] consider the geographical location of infrastructures as a factor affecting their security.

This study aims to prove that modern technology in the form of a well-proven vulnerability assessment methodology coupled with a user-friendly Geographic Information System (GIS) and tools for Geovisual Analytics may help in significantly enhancing the security of Critical Infrastructures in medium as well as small cities which need to cope with a very limited budget for infrastructure protection.

The responsibility for protecting Critical Infrastructures may be subject to local legislation, but most often it lies on the owner and/or operator. Most often at least one of these roles is attributed to a local municipality. However, municipalities often lack the expertise and resources necessary to ascertain appropriate level of protection to the right infrastructures, many of which are used in ways that were not foreseen during their development [27]. Thus, successful management of risk for a large number of different types of Critical Infrastructure with variable resistance to various types of threats requires support from dedicated tools employing specialistic knowledge from many branches in support of integrated analysis and comparison of different types of municipal infrastructure.

2. Critical Infrastructure analysis and risk assessment

The first step in protecting Critical Infrastructure involves identifying and evaluating the factors that may negatively influence its operations. This process is referred to as risk assessment [28] or Security Vulnerability Assessment (SVA) [29]. Although there are numerous methods of assessing risk, they all share a common set of variables. These characteristics are defined as follows [30]:

Vulnerability v_i is the likelihood that an inherent weakness in a system or its operating environment may be exploited to cause harm to the system. It is expressed as a probability p_i that component i will fail [31]: $v_i = p_i$. Vulnerability is often expressed in percentage and thus ranges from 0% to 100%.

Damage d_i is the cost of a fault, expressed in terms of casualties, loss of productivity, loss of capital equipment, loss of time and so forth. It is typically expressed in currency.

Risk r_i denotes the possibility of incurring a certain amount of damage. Therefore, the risk for component i equals: $r_i = p_i * d_i$. Like damage, risk may also be expressed in terms of monetary loss.

Availability a_i is the probability that a component is operational at any point in time. Therefore $a_i = (1 - p_i)$, which means that availability is the complement of the probability of a fault.

Criticality represents the combined value of a component, measured in the number of lives endangered by an attack directed against it as well as the damage