Chapter 6
Modelling Economic Consequences of ICT Infrastructure Failure in Support of Critical Infrastructure Protection Policies

Olaf Jonkeren
European Commission, JRC, Institute for the Protection and Security of the Citizen, Italy

David Ward
European Commission, JRC, Institute for the Protection and Security of the Citizen, Italy

ABSTRACT

There is a large body of work and effort been made in the modelling of critical infrastructures (CI’s) by academia, enterprises, stakeholders, operators, etc.; however, their endeavours have received mixed success so far. This can be traced back to several difficult and historical hurdles in CI modeling such as the chronic unavailability of reliable and recognised data, the specificity of the resulting model, and therefore, its application, the underlying mathematics, narrow-mindedness and lack of awareness of the consequences of infrastructure failure, the recognition and dissemination of the modelling methodology-knowledge, etc. Consequently, bridging theory and application and providing tools for analysing CI’s is key to ensuring that such modelling delivers the benefits voiced and satisfies the needs raised. This chapter sets out to tackle several of these issues.

DOI: 10.4018/978-1-4666-2964-6.ch006
1 INTRODUCTION

The first issue refers to the above mentioned modelling difficulties namely the availability of: (1) reliable and up-to-date data and, (2) a suitable, versatile model, based on an internationally recognised method.

The second issue involves application and exploitability, for which we have decided to leverage the European Directive (2008/114/EC) on the identification and designation of Critical Infrastructures. This Directive is the first European attempt to get all European CI actors or operators involved in the assessment of their infrastructures. It aims to foster a better understanding of the impact of CI disruption on ‘neighbouring’ countries and also at national level. One of the criteria in the Directive that is used to evaluate potential critical infrastructures is the economic effects criterion. It is this criterion that is the subject of the modelling exercise discussed herein and allows us to combine application with exploitation.

The third issue concerns an effort to improve the link between research and policy making for Critical Infrastructure Protection (CIP) by providing a modelling framework for CI failure impact analysis (at a national level) and therefore raising awareness among key CI actors.

To deal with the second and third issues the authors exploit the case of the Estonian cyber attacks that took place in 2007 and are an internationally renowned case study. The authors set out to estimate the economic impact of this ICT infrastructure failure event and therefore connect policy to prediction to post-event assessment.

Since its first appearance as an expression by Dennis Stevenson in 1993 (Information and Communications Technology in UK Schools: An Independent Inquiry, 1997) Information Communication(s) Technology or simply ‘ICT’, has evolved from being IT (Information Technology) focused to an umbrella concept encompassing fields from education to industrial control systems. This ‘everywhereness’ implies that ICT as we have today is cross-sectoral in nature. The telecommunications and finance sectors are two evident interdependent representatives of this ‘everywhereness’.

In fact, modern society is so dependent on ICT nowadays that it is only when its functionality is violated, depletes or its services fail do we realize its cross-sectoral nature and the importance it has in our daily lives. Violations and attacks, such as through cyber incidents, are by far from rare and dramatically on the increase in frequency, variety and scale of the significance for the victims. As a measure of this escalation, from 2006 to 2010 cyber incidents\(^1\) in the USA rose by a factor of 7 (Cyber Security Market, 2012). The target is the data exchanged and ultimately the people that need and use this data.

The exchange of data in an ICT network can be viewed as an exchange of services between systems. These services could for example be money, documents, data, etc. Moreover, conceptually the complexity in any network is not just about the extension and content of the network itself but also how the network interfaces with other networks. Therefore, networks can also be viewed as a collection of infrastructures or sub-systems that form a complete system. For this reason integrated networks and infrastructures are often referred to as ‘systems of systems’ (SoS), especially when these networks exchange services. An ICT system that supports and provides bank transaction services and therefore allows banks and their customers to communicate maybe be seen as an ICT system spanning numerous sectors and subsectors. This forces us to recognise that ICT systems are part of a SoS where induced disruption of an infrastructure’s operations can occur even if it pertains to another system (See Figure 1) and/or the disruption initiates in another sector, infrastructure etc. This not only reveals interdependency (Moteff, John D.; Parformak, Paul, 2002) but also possible domino or cascading effects i.e. the disruption of a system, sector, or organization can lead to a cascading disrup-