Chapter 23
Cyberattacks on Critical Infrastructure and Potential Sustainable Development Impacts

Toufic Mezher
Masdar Institute of Science and Technology, UAE

Sameh El Khatib
Masdar Institute of Science and Technology, UAE

Thilanka Maduwanthi Sooriyaarachchi
Ceylon Electricity Board, Sri Lanka

ABSTRACT

Because of advancement in information and communication technologies, modern infrastructure systems are currently operated, monitored and controlled by automated systems such as distributed process control networks and supervisory control and data acquisition. Such systems will make the critical infrastructures in any country vulnerable to failures caused by either operational failures or to potential cyberattacks similar to Stuxnet and Night Dragon. The objective of this paper is to shed the light on the synergy between cybersecurity and sustainable development in relation to the potential social, economic, and environment consequences of potential cybersecurity attacks on critical infrastructures. Examples of both operational and cybersecurity incidents are shown including their sustainable development implications.

INTRODUCTION

With the advancement of Information and Communication Technologies (ICT), all complex systems such as critical infrastructure are connected through multi-layered network systems through the internet which is widely known as cyberspace (Choucri and Clark, 2013). Figures 1 and 2 show the growth of both ICT development, and the mostly used language on the internet (Internetworldstats, 2013). Public and private sectors, and individuals from developing and less

DOI: 10.4018/978-1-4666-9619-8.ch023

Figure 1. Global ICT development

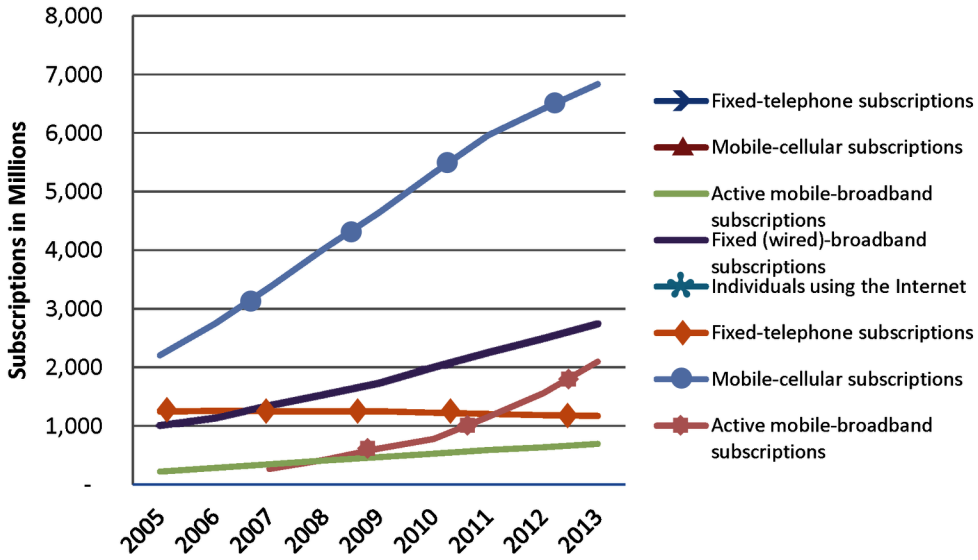
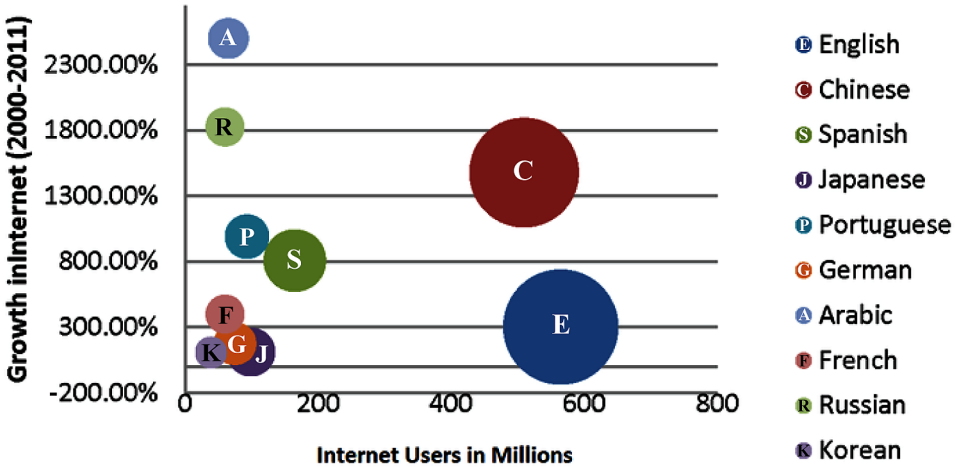


Figure 2. Distribution of internet languages and their growth



developed countries are becoming more connected to the internet using their own native languages. This makes them more susceptible to potential cybercrimes due of lack of security awareness.

We have seen many industrial disasters in the past that are attributed to operational accidents due to human or system errors and in many instances the consequences were disastrous in nature such as Chernobyl nuclear power plant in Ukraine and Bhopal chemical complex in India. Today, potential similar disastrous effects can be attributed to cyberattacks from either criminals or terrorists who want to inflict harm on societies. Cyberwars and cyberterrorism is on the increase and at a faster rate. The objective of this article is to shed the light at the sustainable development consequences of cyberattacks on the critical infrastructure and to highlight their economic, social, and environment impacts which may not be limited to the boundary of one country.