Early Warning Systems as Critical Information Infrastructure: Analysis of Potential Threats and Related Concepts

Edward Mutafungwa

Department of Communications and Networks, Otakaari 5, FIN-02015, P. O. Box 3000, Teknillinen korkeakoulu (Helsinki University of Technology), Espoo, Finland, edward.mutafungwa@tkk.fi

The increased frequency of occurrence of natural and man-made hazards has underscored the need for early warning systems capable of rapidly and reliably disseminating suitably targeted warning messages in response to an imminent hazard event [GLANTZ (2003), WMO (2007)]. The message dissemination process is typically initiated and executed out by a combination of human operators, Information Technology (IT) systems and existing communication resources that constitute an end-to-end early warning system. The constituent components of an early warning system would be designed to interact in a predictable, harmonised and effective matter, to enable messages to be rapidly composed and disseminated in time to save lives and property at risk.

To that end, early warning systems could be considered to be critical information infrastructure (CII). A CII has been defined to be IT and communications systems that are critical infrastructures for themselves or for the operation of other critical infrastructure [EC (2005)]. The actual designation of what constitutes critical infrastructure varies from country to country [ABELE-WIGERT (2006)], but it generally includes both the people and public or private assets that would be saved if early warning systems function as specified.

As with other CII, early warning systems continuously operate under a specter threats (human/non-human, deliberate/non-deliberate, etc.) that could potentially disrupt their normal operation or cause them to function in a way that deviates from their original purpose. For instance, ill-intentioned individuals could compromise the system into sending hoax warnings causing unnecessary panic and long-term loss of confidence in the legitimate early warning service. Or then, significant outage or faults in parts of the early warning system or interconnected message dissemination infrastructure could result in failure to disseminate messages during crucial moments of imminent hazard events.

Therefore, the concept of critical information infrastructure protection (CIIP) that has recently gaining significant attention [DUNN (2003)] is also highly relevant for early warning systems. CIIP constitutes the programs and activities of various stakeholders (operators, users, authorities, etc.) which aim to keep the performance of CII (such as, an early warning system) above a defined minimum level of service in case of failures, attacks or accidents [EC (2005)]. Moreover, CIIP aims to minimize recovery time and any potential damage to a CII.

The implementation of an effective CIIP strategy requires a comprehensive analysis of potential threats and related concepts of security, vulnerability and attack for a CII. This paper analyzes the potential threats to an early warning system. This analysis includes the classification of threat consequences, the nature of the threats and the accentuation of threats due to system (intra)interdependency. The objective is to contribute to the discourse on early warning systems within the CIIP framework and hopefully bring attention to hitherto unanalyzed aspects of early warning systems.

Literature

Abele-Wigert, I., Dunn, M. (2006): International CIIP Handbook 2006: An Inventory of 20 National and 6 International Critical Information Infrastructure Protection Policies, Center for Security Studies, ETH Zurich, Vol. I, 493 p.

Dunn, M., Mauer, V. (2006): Analyzing Issues, Challenges, and Prospects; Center for Security Studies, ETH Zurich, Vol. II, 235 p.

EC (2005): Green Paper on a European Programme for Critical Information Infrastructure Protection, European Commission Communication COM 256, 17 November 2005.

Glantz, M. H. (2003): A Usable Science report on the workshop on “Early Warning Systems: Do’s and Don’ts,” 20-23 October 2003, Shanghai, China, report prepared February 2004.

WMO (2007): WMO Multi-Hazard Early Warning Demonstration Projects, Outline for Documentation of Good Practices in Early Warning Systems, developed by the Expert Meeting on National Meteorological and Hydrological Services’ Participation in Disaster Risk Reduction Coordination Mechanisms and Early Warning Systems, WMO HQ (Geneva, Switzerland), 26-28/11/2007.