Chapter 16
Hybrid Intelligence Framework for Improvement of Information Security of Critical Infrastructures

Alexander P. Ryjov
Lomonosov Moscow State University, Russia

Igor F. Mikhalevich
Russian University of Transport (Moscow Institute of Transport Engineers), Russia

ABSTRACT

Information infrastructures for corporations and governments (information and automated systems, telecommunication networks, and other elements) have dramatically changed in the last decades due to the broad usage of IoT, AI, mobile internet, and other advanced technologies. Protection against cyberattacks requires new solutions that correspond to an increased level of complexity for these infrastructures. Important tasks for these new tools are forecasting cyberattacks, developing and applying preventive protective measures to reduce the risk of information security incidents. For the prediction of cyberattacks and the development of preventive protective measures, the authors propose to use one of the hybrid (or augmented) intelligence (HI) frameworks – evaluation and monitoring of complex processes. The mission of the chapter is to discuss the main issues, challenges, and opportunities related to HI applications for protection against cyberattacks to information infrastructures.

INTRODUCTION

Artificial intelligence technologies are developing rapidly. This worries people and causes debate about the dangers and acceptable limits of use. Artificial intelligence is not limited to autonomous systems and has penetrated deeply into cyberspace. At the same time, there is an active connection to the cyber environment of critical infrastructures that previously operated on the basis of national networks isolated

DOI: 10.4018/978-1-7998-5728-0.ch016

from the global Internet, or autonomously. A single cyber environment has destroyed the boundaries between critical national infrastructures and increased their vulnerability to cyberattacks. The intensity and focus of cyberattacks on critical infrastructures is growing. It is difficult to identify sectors of critical infrastructures that have not been exposed to cyberattacks. At the same time, there is no unity at the international level on the composition of critical infrastructures. This breaks the line of defense for critical infrastructures that interact at the international level. Cybercrime is sophisticated and actively uses artificial intelligence. For example, for the unauthorized capture and use of computing resources, a variety represented in each house. Cybercrime is not worried about the possibility of negative consequences of the use of artificial intelligence use for society. Society must offer a different intelligence, uniting man and machine, but protected from the undeclared capabilities of machines. Such an intelligence seems to the authors a hybrid intelligence, the use of which will protect the critical infrastructures of states and the spheres of human activity.

CRITICAL INFRASTRUCTURES AND CYBERSPACE

Unified terminology and standards for critical infrastructures have not been adopted. But approaches to ensuring the security of critical infrastructures need to be coordinated, because the critical infrastructures of countries can affect each other's security. For example, the country's lack of a nuclear energy sector does not protect it from the spread of the consequences of incidents at nuclear power plants in other countries.

Here are some examples of national approaches to formulating critical infrastructures.

In the United States, critical infrastructure covers systems and assets from 16 sectors, the failure or destruction of which can lead to disastrous consequences in the field of defense, economy, health, and national security. Critical Infrastructure Sectors: Chemical, Commercial Facilities, Communications, Critical Manufacturing, Dams, Defense Industrial Base, Emergency Services, Energy, Financial Services, Food and Agriculture, Government Facilities, Public Health, Information Technology, Nuclear Reactors, Materials, and Waste, Transportation Systems, Water and Wastewater Systems (Executive Order N°13636 (2013), Presidential Executive Order of USA (May 11, 2017), Critical Infrastructure. Threat (2016))

Critical infrastructure of an EU state means an asset or system that is necessary to maintain the vital functions of society, the health, protection, safety, economic or social well-being of people, the violation or destruction of which will have a significant impact in a Member State as a result of the failure to perform these functions.

European Critical Infrastructure means a critical infrastructure located in a Member State, the violation or destruction of which will have a significant impact on at least two Member States. The significance of the impact should be evaluated in terms of cross-cutting criteria. This includes effects resulting from cross-industry dependencies on other types of infrastructure. The initial composition of European Critical Infrastructure from 2 sectors (Energy, Transport) has changed significantly and expanded to 9 sectors: Energy, Information and Communication Technology, Traffic and transportation, Healthcare, Water supply, Finance and insurance, Government and administration, Nutrition and agriculture, Media and cultural assets (Council directive 2008/114/EC, Good Practices Guide (2013))

Critical National Infrastructure in the UK include 13 sectors: Chemicals, Civil Nuclear, Communications, Defence, Emergency Services, Energy, Finance, Food, Government, Health, Space, Transport and