Chapter 30
Cyber Threats to Critical Infrastructure Protection:
Public Private Aspects of Resilience

Denis Čaleta
Institute for Corporate Security Studies, ICS-Ljubljana, Slovenia

ABSTRACT

The globalisation of the world, and thus indirectly of security, poses serious dilemmas for the modern society about how to continue basing its development on the fundamental requirements related to the free movement of goods, services and people, and, on the other hand, about how to keep threats at an acceptable risk level. The emergence of asymmetric forms of threat to national and international security is based on completely different assumptions and perceptions of the basic concepts of providing security. The changing social conditions and tensions caused by the rapid technological development found particular social environments totally unprepared for confronting the new global security situation and, above all, the newly-emerging complex security threats. The integration of critical infrastructure protection processes into a comprehensive system of national security provision at the national and consequently the international level will be a very demanding project in terms of coordination and awareness of the necessity or regulating that area. In addition, it will represent a very significant shift in the attitude and mentality of all the participants involved. This paper addresses in detail some important dilemmas and factors which have a strong impact on the level of awareness, cooperation and confidence of all partners in the public and private environment that share the need for the protection of critical infrastructure.

INTRODUCTION

The functioning of modern society is imbued with a whole set of threats and risks, among which cyber and related threats play an important role. The structure of modern society is based on openness, democratic values and the protection of human rights. Yet, from the economic point of view, its development towards ensuring normal operation aims at providing free movement of people, capital, goods and services. The technological development and solutions, on which the functioning of certain parts of

DOI: 10.4018/978-1-5225-7912-0.ch030

Copyright © 2019, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

modern society is crucially dependent, points to the conclusion that comprehensive security in such an environment has become a very demanding task, which can no longer be provided by national security bodies alone without the appropriate support of other structures for ensuring security. In certain contexts, it can be established that the dependence on the functioning of infrastructure in individual sectors (referred to as critical infrastructure), its exposure and the complexity of its management have become an important risk factor. However, the openness of the society and its processes in its essence reflect that the comprehensive control of security risks and threats is unmanageable. It is precisely because of the interdependence of the functioning of the international environment that these risks and threats, in most cases, lead to transnational and multi-dimensional consequences.

With the development of information and other technologies, the society has become increasingly complex and vulnerable. We live in a high-risk society. The positive aspects of development also bring several strongly negative consequences that can, in their extreme form, present an increasing threat to individual, national or international security. The remarkable development of technology has certainly facilitated progress in all segments of the functioning of the society. However, the dependence of the society on the functioning of technological systems is strong; a minor system malfunction might have important consequences for the functioning of the society. For this reason, the reliance on the functioning of this infrastructure has obvious direct and indirect impacts on its threat and represents a tempting target for cyber attacks and threats.

Critical infrastructure is essential for the smooth functioning of the wider community. When we are talking about factors for the smooth functioning of critical infrastructure we can see that in this respect it is particularly expressed its cross-sectorial complementarities and interdependence. Communications and information technology as one of the critical infrastructure sub-sectors is in this context extremely important because continuous operation of other subsections of critical infrastructure increasingly depends on its normal functioning. This fact gives cyber threats a special connotation when we try to approach their prevention through a systematic approach. Of course, our effectiveness is influenced by many factors among which the fact that a growing share of critical infrastructure passes in the framework of private owners has an important role. Knowing that the country as such is no longer able to fully ensure appropriate measures, due to the complexity of the security risks associated with cyber threats, we are forced to search for new answers and mechanisms that will ensure an appropriate approach to preventing the whole set of risks jeopardising the smooth functioning of critical infrastructure. In this segment, we encounter the dilemmas posed by public-private partnership in various forms. In this context, we must not neglect the factors related to the safety awareness of owners, strategic management, corporate security management, and ultimately all the employees in these organizations which manage critical infrastructure. When it comes to its prevention, the complexity of cyber threats is very closely linked with the appropriate awareness of strategic management of the seriousness of the problem and the measures that must be implemented in order to keep the risk at a manageable level and that the business processes of the organization run without major restrictions. One of the major hazards that are the most dangerous is lack of awareness and false belief that the problem of cyber-threats does not concern the national or corporate environment. In particular, the problem of the lack of awareness becomes especially evident when it comes to the smooth functioning of critical infrastructure.

Security problems have been discussed in the past primarily in terms of the threats from the real physical environment, which, however, is now joined by the danger of cyberspace, which represents an essential part of the problem. In recent decades, we have been living in a time of rapidly expanding cyberspace, which results in the formation of the new information society, which functions in the so-

16 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:
www.igi-global.com/chapter/cyber-threats-to-critical-infrastructure-protection/220904

Related Content

Turning Weakness into Strength: How to Learn From an IT Security Incident
Randy L. Burkhead (2019). *Censorship, Surveillance, and Privacy: Concepts, Methodologies, Tools, and Applications (pp. 177-198).*
www.irma-international.org/chapter/turning-weakness-into-strength/213801

A Comparative View of Censored and Uncensored Political Discussion: The Case of Chinese Social Media Users
Qihao Ji (2019). *Censorship, Surveillance, and Privacy: Concepts, Methodologies, Tools, and Applications (pp. 1439-1453).*
www.irma-international.org/chapter/a-comparative-view-of-censored-and-uncensored-political-discussion/213864

Notifiable Disease Databases for Client Management and Surveillance
Ann M. Jollyand James J. Logan (2019). *Censorship, Surveillance, and Privacy: Concepts, Methodologies, Tools, and Applications (pp. 740-770).*
www.irma-international.org/chapter/notifiable-disease-databases-for-client-management-and-surveillance/213831

Collective Event Detection by a Distributed Low-Cost Smart Camera Network
Jhih-Yuan Hwangand Wei-Po Lee (2019). *Censorship, Surveillance, and Privacy: Concepts, Methodologies, Tools, and Applications (pp. 918-937).*
www.irma-international.org/chapter/collective-event-detection-by-a-distributed-low-cost-smart-camera-network/213838

Evaluation of Keystroke Dynamics Authentication Systems: Analysis of Physical and Touch Screen Keyboards
Moustafa Daferand Mohamad El-Abed (2017). *Developing Next-Generation Countermeasures for Homeland Security Threat Prevention (pp. 306-329).*
www.irma-international.org/chapter/evaluation-of-keystroke-dynamics-authentication-systems/164727