Chapter 13
Cyber Attacks and Preliminary Steps in Cyber Security in National Protection

Faruk Aydin
Turkish Air Force, Turkey

O. Tolga Pusatli
Cankaya University, Turkey

ABSTRACT

Cyber attacks launched by individuals and/or supported by nation states have increased due to the prevalence of information technologies at critical infrastructure of the states. In this chapter, such attacks and consecutive impacts are visited. In connection with this issue, evolution of cyber threats from annoying malware to serious weapons is studied by examples; hence, precautions against such threats are visited and usage of anti-malware applications as prevalent precautions is assessed within the scope. Selected information security standards and strategies of selected states and precautions for cyber security of Turkey are studied. Our findings underline that educated citizens and companies along with public institutions should cooperate to provide a nationwide cyber security. Consequently, it is defended that governments should play an affective role to protect, educate, and guide governmental and private companies and citizens on the cyber security by promoting the cyber security topic in the successive national development plans.

INTRODUCTION

While the extensive usage of information technologies (IT) in most industries, and hence business, cyber security has gained its importance in the modern world and promises to climb to higher priorities in government agendas in many countries. Nowadays, IT have been ubiquitous at many levels (personal, institutional, systemic) from individual to across the nation and hence global. Thus, cyber security is no longer considered as a subject constrained to personal computer security and/or securing e-mail accounts.

DOI: 10.4018/978-1-5225-5634-3.ch013

Copyright © 2018, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

With the widening and spreading nature of the topic, literature is fed with studies on cyber security at various levels in many countries. Thus, we acknowledge the increasing importance of cyber security and its position in the development plans of countries. In this chapter, we shall visit pioneer countries and their policies and take Turkey as an example to reveal what to do in order to protect both society and government against cyber attacks.

Quick examples include Tunisian Report (WSIS, 2005) accepted in the World Summit on The Information Society and the current and previous, development plans of Turkey (State Planning Organization, 2006), (Ministry of Development, 2013).

Basically, the Tunisian Report highlights following points;

- Information resources and technologies are being used for crime,
- Terrorism uses information technologies effectively,
- For that reason abuse of IT should be prevented; however, human rights should be considered during monitoring processes.

When we have a glance to Turkey, we easily capture that transformation of Turkey's society to the information society has been stressed in the vision of the 9th development plan covering 2007-2013 years of Turkey. Both the Tunisian report and the development plans, for example, show that the cyber security issue is considered as an important area both in Turkey as well as abroad.

In addition to this motivation, we observe that cyber attacks are not only targeting business for a brutal form of entertainment or for the purposes of theft; such attacks can be parts of extremist actions such as terrorism as well. For instance, Lucent Technologies, which is a multinational technology company, announced that Unity, a pro-Palestinian group, had attacked its web site in November 2000. The purpose of this attack was not to steal any valuable information but because the company did business in Israel as discussed in (Cross & Shinder, 2008).

Cyber crimes are serious threats not only for the world but also for Turkey. According to the 2012 Norton Cyber Crime Report (Norton, 2012) in Turkey more than 10 million people have been aggrieved because of cyber crime in one year. It is stated that the cost of this problem is around 556 million USD. Such a figure highlights the gravity of the topic.

With this quick introduction, we report on our study on cyber threats, common technological precautions and strategies against them as our aim. Within this scope, we try to find out how serious such threats can be for nations, and whether it is too early to speak of serious cyber threats that can put nationwide security in peril, or not. More specifically, we try to seek an answer for "should the state play an affective role in national cyber security? If it has to, what does the state have to do?"

This work takes a larger study conducted and reported in a thesis in Turkey in 2011 and 2012 (Aydin, 2012) and tries to catch subsequent important developments. The findings match with the earlier reported drafts of the current national development plan as in recognizing the cyber security in a higher rank at the time of writing this chapter; thus, the study has already started to prove itself that the topic should be kept as a high priority not only as a sole subject but to be considered by many in both public and private sectors. At the time of writing, the 10th National Development Plan of Turkey (Ministry of Development, 2013) has been published and it is underlined that the necessity of completing regulation on protecting privacy, private data, ensuring security of national information and securing e-commerce still exist. In parallel to this, a sub-department to combat cyber crime has been established under security

15 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-attacks-and-preliminary-steps-in-cyber-security-in-national-protection/203507

Related Content

Machine Learning-Based Approach for Predictive Analytics in Healthcare
Sandeep Kumar Hegdeand Monica R. Mundada (2022). *Deep Learning Applications for Cyber-Physical Systems (pp. 182-206).*
www.irma-international.org/chapter/machine-learning-based-approach-for-predictive-analytics-in-healthcare/293130

Test Suite Minimization in Regression Testing Using Hybrid Approach of ACO and GA
Abhishek Pandeyand Soumya Banerjee (2021). *Research Anthology on Recent Trends, Tools, and Implications of Computer Programming (pp. 133-150).*
www.irma-international.org/chapter/test-suite-minimization-in-regression-testing-using-hybrid-approach-of-aco-and-ga/261025

Towards MDA Software Evolution
Liliana María Favre (2010). *Model Driven Architecture for Reverse Engineering Technologies: Strategic Directions and System Evolution (pp. 236-240).*
www.irma-international.org/chapter/towards-mda-software-evolution/49186

An Optimal Hybrid Regression Testing Approach Based on Code Path Pruning
Varun Gupta (2018). *Multidisciplinary Approaches to Service-Oriented Engineering (pp. 265-286).*
www.irma-international.org/chapter/an-optimal-hybrid-regression-testing-approach-based-on-code-path-pruning/205303

Analysis of Issues in SDN Security and Solutions
Ankur Dumka, Hardwari Lal Mandoriaand Anushree Sah (2018). *Innovations in Software-Defined Networking and Network Functions Virtualization (pp. 217-239).*
www.irma-international.org/chapter/analysis-of-issues-in-sdn-security-and-solutions/198200