Chapter 20
Defending Information Networks in Cyberspace:
Some Notes on Security Needs

Alberto Carneiro
Universidade Europeia, Portugal & Universidade Autónoma de Lisboa, Portugal

ABSTRACT

This chapter addresses some concerns and highlights some of the major problems affecting cyberspace. This chapter focuses on defensive attitudes and concerns pertaining to the cybersecurity issues. Section 1, "Facing Cyberspace Security," opens the area of threats and the need of defensive attitudes. Section 2, "Remembering Internet Issues," deals with known Internet problems in what concerns cybersecurity as a generic term. In –Section 3, "Defensive Cybersecurity," the focus is on the need to add more defensive features to security policies. Section 4, "In Search of Better Solutions," emphasizes the need to invest continuously in scientific research and the creation of more sophisticated processes in order to prevent new forms of attack and mitigate negative results.

FACING CYBERSPACE SECURITY

Our presence in cyberspace is directly related to the security of the information that circulates here. For this reason, our thoughts have to concentrate on threats, potential risks arising from the absence of security, and on the need to maintain data, privacy and other assets, developing defensive attitudes and proactive behaviors.

Cybersecurity: An Insecure World

Cybersecurity is a concept that arrived on the post-cold war agenda as a responsive reaction to a mixture of technological innovations and changing geopolitical conditions (Hansen & Nissenbaum, 2009; Carneiro, 2008). It can be faced as a distinct sector with a particular constellation of threats and entities. It is held that "network security" and "individual security" are significant technical and social areas, and their political importance arises from connections to other collective entities as "society," "nations", and "economy."

Shortly saying, it is essential to increase the levels of attention to cybersecurity. It is known that both organizations and individuals are poorly informed about cybersecurity and they are not sufficiently protected. In addition, attacks are becoming increasingly sophisticated (Kshetri, 2005; Saydjari, 2004) and may be made of denial of service, malevolence, and identity theft attacks in the lower layers of the network.

DOI: 10.4018/978-1-4666-6324-4.ch020

Everything happens as if cyberspace was a world even more insecure than the transactional world with which organizations are more accustomed to dealing with. In fact, the insecurity grows with the number of entities with which the organization connects. Additionally, when one opens a door to the outside world many presences can enter if we do not get proper care. This seems obvious, but many organizations are subject to undesirable presences within their networks because they did not take appropriate action according to a security policy.

The effectiveness of cybersecurity requires that national governments, private companies and non-governmental organizations can work together to understand the threats in cyberspace and to share information and resources that can mitigate them. Cyberspace is an environment where there are many connections that provide huge benefits for nations, organizations and individuals. However, this environment is also a space where there are criminals, terrorists and other actors whose intentions may affect the socio-economic values of the majority of its users. If most responsible entities fail to understand and mitigate these risks, national and economic security may be endangered.

A significant number of companies have been victims of cybercrime, including targeted attacks, industrial espionage and loss of confidentiality with regard to intellectual property. Companies can protect the confidentiality of their information by paying attention to three main areas: a) the protection of Information and Communication Technology (ICT) infrastructure; b) requiring identification, authentication and access control and c) ensure business continuity and risk management. Those situations lead to the conclusion that cyber threats are now much more important to business. Information security is an area often neglected and it seems that companies think that it can survive almost without investment. Perhaps many managers feel that the attacks of so-called "hackers" are things that only happen to other people and in science-fiction movies. Several criminal groups seem to have abandoned other activities with greater physical risk to engage in the cybercrime which is much more profitable. It is necessary to advocate for the urgent need to raise the level of cybersecurity in order to maintain competitiveness and sovereignty of each nation.

Global security in cyberspace must be based on the common will of the nations in order to use adequate skills that should be organized in order to defend themselves against common threats. Even though nation-states are the main actors of a global policy of the defense, private companies, political and military alliances and international organizations also play important roles in ensuring cybersecurity internationally.

Almost every day the dependence of many global organizations is increasing in what concerns their relationships with partners and markets they want to achieve. At a higher level, many countries and governments rely on computing infrastructure of cyberspace so that financial markets can function as well as the industries of transportation and power distribution networks. Regardless of their size, most companies want to safely use computer networks in real time, exploring technological innovations and their economic consequences. And yet it is essential to consider the national defense organisms and intelligence agencies that require different virtual networks to be able to act at distance, analyze data of varied nature in the name of internal security, military logistics and to create emergency response against contingencies. However, the efforts of the information security industry are almost always reactive, and in most cases the defensive position is not sufficiently favorable (Utin *et al*., 2008). The growth of this dependence increases the likelihood of risks and increasingly differentiates the dangers to which organizations are subjected. Thus, the cyber infrastructure must be addressed and studied in conjunction with networks of organizations, of flows of materials, and information among nations.

The ability to provide a trusted environment for individuals and businesses to interact online is critical to innovation and growth (Carneiro, 2007). Digital transformation makes the protection and