Chapter 4
Cybersecurity

In this chapter we define and explain the notion of cybersecurity. What characterizes cybersecurity, and what are the kinds of threats that cybersecurity must prevent or provide protection from? We also explain how cybersecurity relates to information security, critical infrastructure protection, and safety.

4.1 What is Cybersecurity?

While cybersecurity may involve the security of a cyberspace itself, most organizations are concerned with the protection of their own cyber-systems from cyber-threats. Both of these concerns are within the scope of our definition of cybersecurity.

Definition 4.1 *Cybersecurity* is the protection of cyber-systems against cyber-threats.

Cyber-threats are those that arise via a cyberspace, and are therefore a kind of threat that any cyber-system is exposed to.

Definition 4.2 A *cyber-threat* is a threat that exploits a cyberspace.

Cyber-threats may be malicious or they may be non-malicious. Examples of malicious threats are denial of service (DoS) attacks and injection attacks that are caused by intention. Non-malicious threats are, for example, systems that crash due to programming errors or loss of Internet connection due to wear and tear of communication cables or other hardware.

Notice, importantly, that what defines cybersecurity is not what we seek to protect, but rather what we seek to protect it from; it is not defined by the kinds of assets that are to be protected, but rather by the kinds of *threats* to assets.

A. Refsdal et al., *Cyber-Risk Management*, SpringerBriefs
in Computer Science, DOI 10.1007/978-3-319-23570-7_4

The assets of concern depend on the organization and the cyber-system in question, although cybersecurity is often about the protection of information assets or infrastructure assets. We discuss this more closely in the following sections by relating cybersecurity to information security, infrastructure protection, and safety.

4.2 How Does Cybersecurity Relate to Information Security?

Information security is the preservation of confidentiality, integrity, and availability of information [35]. Information can come in any form, be it electronic or material, or even as the knowledge of personnel. In order to ensure and maintain information security, information in all formats needs to be protected from threats and threat sources of any kind, including physical, human, and technology-related threats. Cybersecurity, on the other hand, concerns protection from threats that use a cyberspace. Such threats may target information assets, which is why information security is an important part of cybersecurity. However, cybersecurity addresses only those information assets that can be targeted via a cyberspace. Cybersecurity is not limited to the protection of information assets alone. As we discuss below, it often concerns the protection of infrastructure. We may also be concerned about the wider impact of threats to information or infrastructure security in order to protect assets such as life, health, reputation, revenue, and so forth.

Most standards and guidelines on cybersecurity relate cybersecurity to information security. This is to be expected as there is considerable overlap, but in order to properly understand what cybersecurity is and how to ensure it, we must be careful not to confuse these two kinds of security. Cybersecurity goes beyond information security in that it is not limited to the protection of information assets and the preservation of confidentiality, integrity, and availability of information. Information security, on the other hand, goes beyond cybersecurity in that it is not limited only to threats that arise via a cyberspace.

4.3 How Does Cybersecurity Relate to Critical Infrastructure Protection?

Infrastructure security, in particular *critical infrastructure protection* (CIP) and critical information infrastructure protection (CIIP), is concerned with the prevention of the disruption, disabling, destruction, or malicious control of infrastructure [12, 28]. Such infrastructures include, for example, telecommunication, transportation, finance, power supply, water supply, and emergency services. CIP is crucial for societal security, as well as for organizations and other stakeholders that provide or rely on critical infrastructures.

Many critical infrastructures make use of a cyberspace and are therefore cyber-systems. Hence, the security of such systems involves protection from cyber-threats.

CIP in general, however, goes beyond cybersecurity since CIP involves the protection and the security of any critical infrastructures, whether or not they make use of a cyberspace. Cybersecurity, on the other hand, concerns the protection of infrastructures that can be targeted via a cyberspace. Such infrastructures include, for example, telecommunication networks and cyber-physical systems like a smart grid.

How cybersecurity relates to information security and CIP is illustrated in the Venn diagram of Fig. 4.1. From the diagram we see that while cybersecurity may involve both information security and CIP, the former is not simply a combination of the latter two.

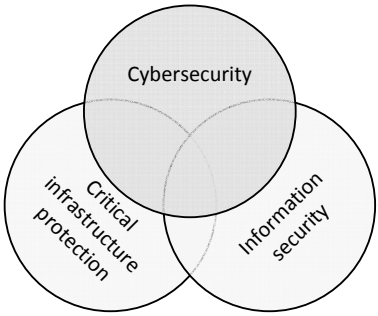

Fig. 4.1 Cybersecurity vs. information security and critical infrastructure protection

4.4 How Does Cybersecurity Relate to Safety?

Safety can be defined as the protection of life and health by the prevention of physical injury caused by damage to property or to the environment [1, 23]. One of the main differences between safety and cybersecurity is that while safety focuses on system incidents that can harm the surroundings, cybersecurity focuses on threats that cause harm via a cyberspace. A further difference is that the assets that are considered with respect to safety are usually limited to human life and health, as well as environmental assets, while the assets of concern with respect to cybersecurity can be anything that needs to be protected.

The distinction between safety and cybersecurity does not mean that safety issues are outside the scope of the latter. The reason for this is that safety incidents may have security impact, in the same way that security incidents may have safety impact. For example, a cyber-attack on a power distribution control system that leads to a blackout could have fatal safety consequences for hospital patients. And a safety incident, such as a gas explosion, could damage information systems and disable security controls, thereby leaving a system vulnerable to cyber-threats. When seeking to ensure cybersecurity we therefore need to take into account safety incidents that may yield vulnerabilities or that otherwise can be exploited by threat sources.

How cybersecurity relates to safety is illustrated by the Venn diagram of Fig. 4.2.

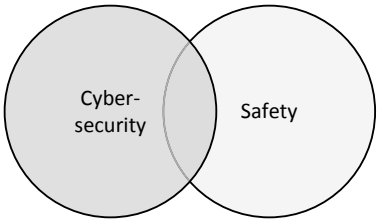

Fig. 4.2 Cybersecurity vs. safety

4.5 Further Reading

The term cybersecurity is in widespread use. As it is used in many different contexts, it is also used with somewhat different meanings. Some use it quite synonymously with network and information security, others focus more strictly on information security, while some are mostly concerned with CIP.

The ISO/IEC 27032 standard [28] defines cybersecurity as information security in a cyberspace, limiting its scope to the strictly virtual and non-physical aspects of the Internet. The EU has ongoing activities regarding cybersecurity that concern both security of and within a cyberspace [13], as well as CIIP [12].

The definition of cybersecurity provided by the ITU includes both information security and the protection of cyber-systems [37]. Others focus more strictly on CIP, such as the National Institute of Standards and Technology (NIST) cybersecurity framework [55].

The definition of cybersecurity provided by the Committee on National Security Systems (CNSS) [7] is similar to our definition, although the former is restricted to adversaries and attacks, rather than cyber-threats in general.

There are a lot of standards and literature on safety. As a detailed discussion of this term is outside the scope of this book, we refer the reader to the IEC/TR 61508-1 standard [23] for a common definition. Algirdas Avižienis et al. [1] discuss how safety relates to concepts such as security and dependability.