ENISA overview of cybersecurity and related terminology

VERSION 1

SEPTEMBER 2017

www.enisa.europa.eu

European Union Agency For Network and Information Security

Foreword by the Executive Director

In the last few years, there have been many new developments in the cyber world. We continue to witness the digitalization of our daily lives, the development of new technologies, new threats and new stakeholders.

The words cybersecurity, cyber warfare, cyber espionage, cyber terrorism and cyber defence are increasingly referred to in daily conversation by our citizens, media and politicians.

The purpose of this paper is to give an overview of the way ENISA categorises cyber protection.

In this categorisation, many cyber terms are used. ENISA's interpretation of the terms used can be found in Chapter 2.

Please take this paper as our contribution to the discussion for a cyber space taxonomy.

Udo Helmbrecht

Executive Director
ENISA

Table of Contents

1. Cyber space and layers of protection

In cyber space one operates on many different levels and one of the functions of the strategy should be to address coherently all the different levels of cyber space needs.

The following image draws on the Maslow's Pyramid of needs approach to categorising cyber space needs in a hierarchical way. Any EU strategy must cover all aspects of cyber space to ensure a comprehensive approach to addressing the cyber challenges of tomorrow.

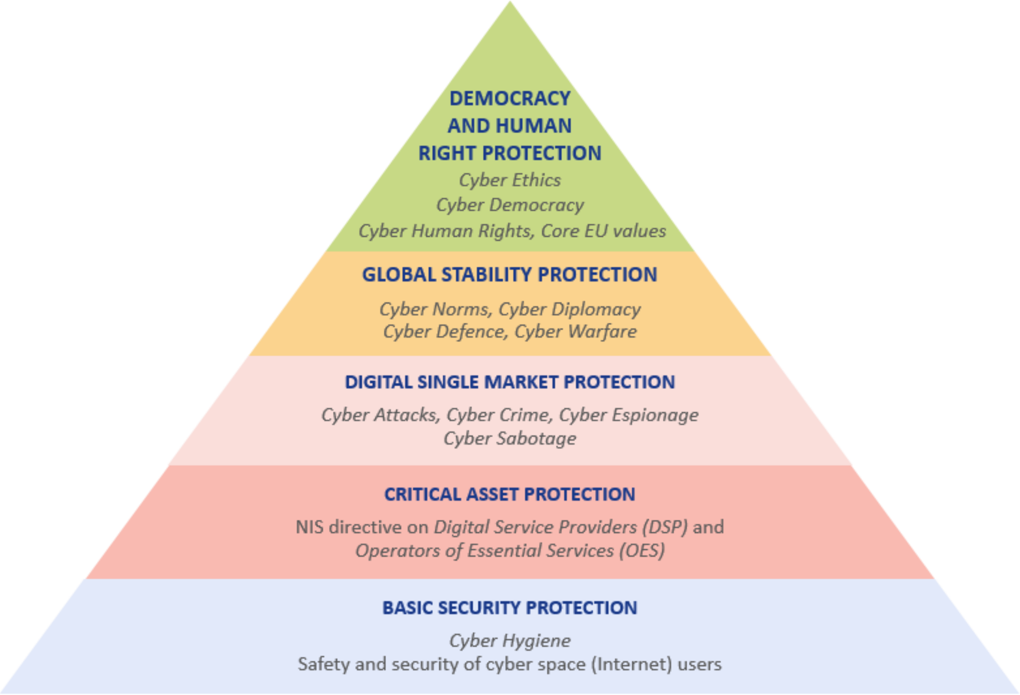
DEMOCRACY AND HUMAN RIGHT PROTECTION
Cyber Ethics
Cyber Democracy
Cyber Human Rights, Core EU values
GLOBAL STABILITY PROTECTION
Cyber Norms, Cyber Diplomacy
Cyber Defence, Cyber Warfare
DIGITAL SINGLE MARKET PROTECTION
Cyber Attacks, Cyber Crime, Cyber Espionage
Cyber Sabotage
CRITICAL ASSET PROTECTION
NIS directive on Digital Service Providers (DSP) and
Operators of Essential Services (OES)
BASIC SECURITY PROTECTION
Cyber Hygiene
Safety and security of cyber space (Internet) users

Figure 1. Layers of cybersecurity protection.

Figure 1 presents ENISA's perspective on cyber space needs, starting with EU core values, such as democracy and human rights at the top, and, working the way down, to the basic citizens' needs.

There are interdependencies between the layers described above.

Protection of the critical assets, i.e. critical information infrastructures provides a key basis for the success of the Digital Single Market[1] including businesses and citizens alike. Cybersecurity for citizens, infrastructures and business, in the current context, cannot be achieved without addressing it in a globalised context. Cyber diplomacy needs to be in place, as a means to prevent, defend and protect the EU, its citizens, infrastructures and businesses. Furthermore, it should be noted that core EU values and norms, including ethics, need to be applied to all levels in cyber space i.e. to all products and services available for EU customers, independent of their place of production/development in the world.

The following paragraphs provide a short description of the pyramid and the layers as cybersecurity requirements.

[1] COM(2015) 192 final

1.1 Layer 1. Basic security protection.

Safety and security of citizens in cyber space is not a matter for debate. Under no circumstances, should the safety of users be at risk due to actions in cyber space. Furthermore, preventive measures should be applied; education, awareness and cyber hygiene are very important. As you wash your hands to protect your health, or lock the door of you home to protect your properties, in the cyber space, you also have to be aware of the risks and take the appropriate measures. Thus, every user should be aware and should be using minimum-security protection actions: firewalls, malware detection, apply updates and patches to safeguard devices and IT systems.

1.2 Layer 2. Critical asset protection.

The Network and Information Security (NIS) Directive brings new security requirements for protecting essential services and digital services in the EU. These requirements are the most recent ones; over the past decade, several communications addressed the need for Critical Information Infrastructure Protection (CIIP)[2]. The implementation of the NIS Directive is an important step in protecting EU CIIP, the cooperation of EU CSIRTs via the CSIRTs network, the improvement of EU collaboration via the Cooperation Group, etc. Secure critical infrastructures in sectors like energy, transport, banking etc. provide bases for the society to function and for the economy to grow.

1.3 Layer 3. Digital single market protection.

The cyber space and technology evolution provide many opportunities for business development. Besides critical infrastructures, all businesses need to be protected as their reliance on cyber space is increasing. The exposure to cyber space related threats like cyber attacks, cyber crime, cyber sabotage and/or cyber espionage becomes more visible every day and can be observed in the media almost daily. Security measures should be deployed and an EU approach is needed to address and support business in general and SMEs in particular in their cybersecurity needs.

1.4 Layer 4. Global stability protection.

Espionage and war have millenniums of history. Cyber space associated terms are already in place; several actions during the past decade were assessed as cyber war, cyber espionage etc. There are several discussions on the need for cyber norms and cyber diplomacy[3]. Cyber defence activities are funded and developed across the globe. Given the nature of cyber space, adequate measures and international agreements need to be in place to guarantee global stability in front of risks. The EEAS activities, the Tallinn manual[4], etc. are good examples of activities at this level that need to be supported and extended.

1.5 Layer 5. Democracy and human rights protection.

Emerging technologies (autonomous vehicles, etc.) – require new discussions on the ethical aspects of the operation of new technology. Human rights protection online is an increasing challenge. Protection of the core EU values online needs to be guaranteed in cyber space. The impact of new technologies, products and services needs to be assessed and adequate measures should be in place – i.e. any new technology should not undermine human rights, liberties and democracy.

[2] COM(2009) 149 final, COM(2011) 163 final

[3] http://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/en/pdf

[4] Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations: https://ccdcoe.org/research.html

2. Cybersecurity related definitions

Cyber space is the time-dependent set of tangible and intangible assets, which store and/or transfer electronic information.

Cybersecurity comprises all activities necessary to protect cyberspace, its users, and impacted persons from cyber threats.

2.1 Terminology used in the pyramid

While in this document, we do not aim to provide new definitions to cybersecurity and to cyber space, we work with the following understanding of the terminology:

Information security. The classic model for information security defines three objectives: **Confidentiality**, **Integrity**, and **Availability**.

Network and information security, as defined in the ENISA regulation 526/2013, means the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the **Availability**, **Authenticity**, **Integrity** and **Confidentiality** of stored or transmitted data and the related services offered by or accessible via those networks and systems.

Information security, *network and information security* are subsets of *cybersecurity*.

Cybersecurity covers all aspects of prevention, forecasting; tolerance; detection; mitigation, removal, analysis and investigation of **cyber incidents.** Considering the different types of components of the cyber space, cybersecurity should cover the following attributes: **Availability, Reliability, Safety, Confidentiality, Integrity, Maintainability** (for tangible systems, information and networks) **Robustness, Survivability, Resilience** (to support the dynamicity of the cyber space), **Accountability, Authenticity** and **Non-repudiation** (to support information security).

Cyber ethics. Ethics are principles and or standards of human conduct. Cyber ethics is a code of behaviour on the Internet[5]. Cyber ethics is the philosophic study of ethics pertaining to computers, encompassing user behaviour and what computers are programmed to do, and how this affects individuals and society[6]**.**

Cyber hygiene covers several practices[7] that should be implemented and carried out regularly to protect users and businesses online.

Cyber incident. Any occurrence that has impact on any of the components of the cyber space or on the functioning of the cyber space, independent if it's natural or human made; malicious or non-malicious intent; deliberate, accidental or due to incompetence; due to development or due to operational interactions is called **cyber incident**. Also we call cyber incident any incident generated by any of cyber space components even if the damage/disruption, dysfunctionality is caused outside the cyber space.

Cyber accident. To support a 'grading' of cyber incidents, we define **cyber accidents** as any occurrence associated with cyber space causing *significant damage* to cyber space or any other asset (has performance impact, requires repairs, replacement) or causing *personal injury*.

[5] https://www.microsoft.com/en-us/safety/online-privacy/cyberethics-practice.aspx
[6] https://en.wikipedia.org/wiki/Cyberethics
[7] https://www.enisa.europa.eu/publications/cyber-hygiene

Cyber investigation. A process conducted for the purpose of cyber accident and incident prevention which includes the gathering and analysis of information, the drawing of conclusions, including the determination of causes and, when appropriate, the making of safety and security recommendations.

Cyber attacks cover all cyber incident triggered by malicious intent where damages, disruptions or dysfunctionalities are caused.

Cybercrime refers to any crime/criminal activity facilitated by or using cyber space.

Cyber sabotage refers to any sabotage activity facilitated by or using cyber space.

Cyber espionage: we understand 2 types of espionage vectors: (a) **state espionage** (intelligence, when state actors are involved) or (b) **industrial espionage** (when commercial actors are involved).

Cyber defense[8] refers to a variety of defensive mechanisms that could be used to mitigate or respond to cyber attacks.

Cyberwarfare refers to any action by a state, group or criminal organisation facilitated by or using cyber space targeting another state.

[8] Kolini, Farzan and Janczewski, Lech, "Cyber Defense Capability Model: A Foundation Taxonomy" (2015), International Conference on Information Resources Management (CONF-IRM) 2015, Proceedings, Paper 32, available at: http://aisel.aisnet.org/confirm2015/32

ENISA

European Union Agency for Network
and Information Security

Heraklion Office

Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office

1 Vasilissis Sofias
Marousi 151 24, Attiki, Greece

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu