Don't confuse cybernetics with security

by **Ivan Makatura**, Senior Security Consultant, IBM CEE Security Services

Today, people are dependent on information. Not just people who are addicted to their smart phones. There is more information than ever before and information is processed ever faster, in huge volumes, and in electronic form.

Hence, the risks are shifting into the cloud called cyberspace. At the same time, we see the term "cyber-security" more and more, but what does it actually mean?

Perhaps you are surprised that cybernetics has nothing to do with security. These two terms are only indirectly related. The meaning of the word comes from the ancient Greek word kybernétes = steersman. In Plato's Dialogues, cybernetics is the proper governance of the provinces.

Modern cybernetics is the science of communication and control theory that is concerned with the study of dynamic systems (including how people, animals, and machines communicate information). In short, "cybernetic" can be considered to mean "related to cyberspace".

The term "cyberspace" is used to describe the virtual world of computers where objects are neither physical nor representations of the physical world, but are made up entirely of data and information. The term is credited to writer William Gibson, who used it in his book, *Neuromancer*, written in 1984. Gibson defines cyberspace as "a consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts..."

The meaning of security

The term "security" comes from the Latin "securitas" (sine cura + tutus). These terms mean carefreeness, peace, protection. In every meaning of the word, it is a state in which the safety, order or protection of life, health, or property is preserved, i.e. when assets and objects owned by an entity are protected.

As regards public security, it can be perceived as the sum of the social relations which protect the rights and legitimate interests of the society and the constitution. It is in protection of these relations where security is interpreted as an acceptable level of danger.

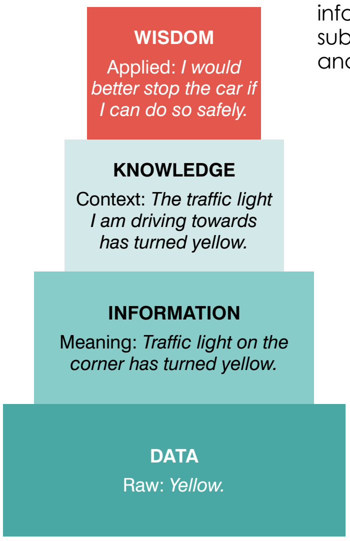
The resulting state of security can be seen in two ways:

- objective security – due to the absence of threats.
- subjective security – due to the absence of threat perception.

As regards threats to information assets, this expression has its own specifics and a different, more radical meaning than commonly attributed to it (e.g. in connection with police functions or other state security).

Data vs. information

Data represents single facts or numbers; data items on their own have little meaning. Data only becomes information if it is meaningful and valuable. The so-called "DIKW model" expresses a logical consequence of steps and stages and information is a contextualized 'progression' of data when it obtains meaning.



WISDOM
Applied: *I would better stop the car if I can do so safely.*

KNOWLEDGE
Context: *The traffic light I am driving towards has turned yellow.*

INFORMATION
Meaning: *Traffic light on the corner has turned yellow.*

DATA
Raw: *Yellow.*

Information security is a part of information management regardless of the physical state of the data, its format, or the storage and transmission medium. A valid definition for information security is the management of threats and risks that affect the data.

Cybersecurity, cybercrime, cyber-defence

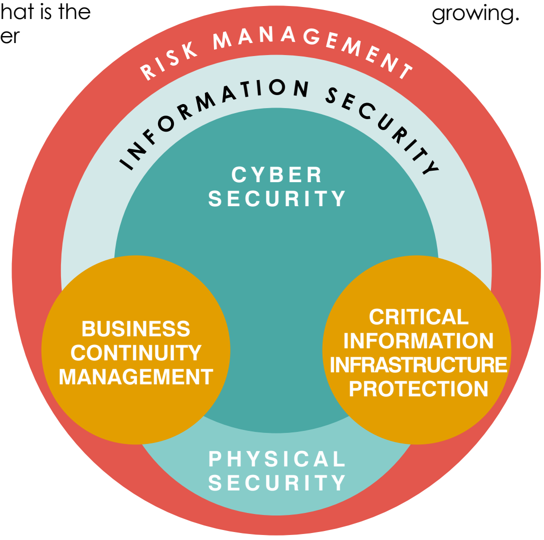
Since information security involves protecting information regardless of whether the information is stored electronically or physically, cybersecurity is a subset of a larger area of information security.

If we want to find a boundary between what is, and what is not cyber-security, we have to consider whether we are looking at the definition of cyber security from a subjective viewpoint (i.e. the owner, observer, recipient, etc.) of the information which is electronically processed, or from an objective viewpoint (i.e. information that is the subject matter and its connection with and impact on the world).

From a military-political point of view, security equals survival, and protection of fundamental human values. But what is the objective of cyber war, cyber-defence, and cybercrime? We are still talking about data, even if it is extremely important, it is still just about data. In this relationship, it is data which represents the objective. People perceive the impact of threats and are therefore the subject of observation. In legal theory, an objective is a goal to be achieved by a legal relationship. An objective represents assets. In this case, information assets.

These are all important human activities to protect data related to these activities or which are affected by these activities. The use of the term "cybersecurity" by politicians and top management is primarily about marketing. "Cybernetics" and the prefix "cyber" are often used with the hope to create the impression of proficiency.

The ultimate goal of protection is to guarantee the security of information, rather than the feeling of safety of information owners. One thing is certain, the importance of cybersecurity is constantly growing.


RISK MANAGEMENT
INFORMATION SECURITY
CYBER SECURITY
BUSINESS CONTINUITY MANAGEMENT
CRITICAL INFORMATION INFRASTRUCTURE PROTECTION
PHYSICAL SECURITY