SECURITY SYSTEM CREATING IN CONDITIONS OF UNCERTAINTY AND RISK-OUTLINE OF THE PROBLEM

dr M.Szyłkowska
Faculty of Logistics – Military University of Technology, Warsaw, Poland
monika.szylkowska@wat.edu.pl

Abstract: *The article presents selected considerations in the field of the security environment with respect to uncertainty and risk factors along with the approximation of the strategy F.U.D. [fear, uncertainty and doubt].*

KEYWORDS: *SECURITY SYSTEM, F.U.D. STRATEGY, RISK FACTORS.*

1. Introduction

The organization of the security system in its geospatial form until recently contained the areas: land, air and sea and space, but the dynamics of technology development meant that its fifth dimension became permanent broadly understood and defined cyberspace, thus creating a security environment. Digital space, penetrating the remaining areas caused a specific problematic network, which sets the need for a new way of organizing and shaping the security environment. All areas of the environment in the process of shaping the security system have common elements: identification of risks and threats, potential analyses and probability of their occurrence, and the preparation of appropriate forces and measures and restitution plans. Time is an additional common factors for all areas.

The security environment is affected by certain conditions, which includes: chances, challenges, risks and threats of the implementation of interests and the achievement of goals in the field of security. Chances include all circumstances (phenomena and processes), which are conducive of the implementation of interests and the achievement of the intended goals. Challenges include the decision-making dilemmas and choices that a given subject faces, including the necessity of incurring specific costs. Risks are uncertainties connected with a particular action and its consequences – including the potential risk of adverse effects of the action taken. The principle is to increase the level of risk directly proportional to the level of activity (e.g. an increase in terrorist threats due to involvement in international operations). For this reason, the skilful estimation and reduction of particular risks is becoming ever more important. While threats are the direct or indirect destructive influences on the subject. Threats are a classic environmental factor. The strategic objective of each subject is (or should be) to ensure safe conditions for the implementation of interests by: reducing identified risks, eliminating threats (external and internal), proper estimation of challenges and skilful use of the occurring chances by making proper decisions [1].

2. Organization of the security system

The organization of each security system depends primarily on the strengths, means the abilities possessed, but the possibility of its shaping depends on the identified potential, which in turn determines the preparatory and executive activities in this area. The pursuit of tasks defined by each entity – in particular states – in the area of security is their organizing, maintaining and preparing in as comprehensive manner as possible The indicated activities take place at specific levels and are processed and implemented in them. These areas, in turn, defined a specific way of managing the system – creating appropriate organizational and functional links.

In shaping the security system – apart from identifying the indicated factors in specific areas – risk identification and assessment play a key role. Risk understood as uncertainty associated with a specific action and its consequences – including the potential danger of adverse effects of the action undertaken. The principle is to increase the level of risk directly proportional to the level of activity in specific areas. The risk as *a combination of the possibility of occurrence of any event and its consequences* is determined not only by the need of identification, but also the determination of thresholds of significance of impact on the functioning of the entity with the preparation and undertaking actions aimed at reducing the negative consequences of its materialization.

Examples of risk thresholds are given in Tab.1.

Type of risk	**Effect**
critical	significant damage to the functioning and possibilities of the entity’s further operation
serious	serious deterioration or disruption of the entity’s operation continuity
significant	significant impact on the functioning or partial disruption of operation continuity

Table 1. *Types and effects of risk*

Threats are another factor in the security environment. The strategic objective of each entity is (should be) to ensure safe conditions for the pursuit of interests by: reducing the identified threats, elimination of threats, proper assessment of challenges, and skilfully using emerging opportunities by making appropriate decisions. The possibility of eliminating threats also precedes the need to identify them and analyse the potential of materialization. In addition to typology of threats, it is important that the estimation of their occurrence is also made in combinations (e.g. external and internal). However, it is crucial to prepare the action in the event of the occurrence and materialization of the effects of the threat. This is involved with, among others, known standards for business continuity (e.g. ISO/IEC 27002 or NIST SP 800-34).

Regardless of the area/sector of operation – for each entity, ensuring the security of information assets of business continuity is of key importance. They have a basic meaning independent of the type of critical processes of a given entity. The business continuity management consist of:

- an analysis of business continuity requirements and risks in the scope of allowable break times in the implementation of critical processes and requirements regarding the availability of assets necessary to carry out these processes. In this area, the risk assessment allows to identify and estimate events that may cause a breach of the continuity of the organization,
- preparation and implementation of the organization’s strategy within the scope of ensuring business continuity (defining the type of actions that will be taken to ensure business continuity and minimizing losses),
- development and implementation of plans allowing to restore the continuity of processes and replacement plans for critical assets,

- development of activities related to ensuring the entity's readiness to respond to a crisis situation (reviews, tests, plans updates).

Principles related to ensuring business continuity analogy concern the comprehensive development of the security system.

Returning to the aforementioned time factor, it should be emphasized that it is of key importance especially in the case of the materialization of negative events – reactions to an event and restoring the state of full functionality from before the event. In this sense, the division can be assumed:

Events	Time of unavailability
critical	exceeding the permissible time of unavailability
serious	within the maximum period of unavailability

Table 2*. Events affecting the time of unavailability of the entity. Developed based on NIST SP 800-34.*

The time parameter will be determined to a different extent – mainly depending on the type of entity and defined critical processes for its operation.

3. Uncertainty

The starting point for the analysis of the conditions of *uncertainty* is the theory of U. Beck: *Today and in the future we will have to live not so much in a world of previously unknown threats, as in a world that must decide about its future in the conditions of uncertainty created by itself.* According to this theory, among others, the society will not be able to control the threats it poses – not because of neglect and failure of modernity, but because of its victories (e.g. increase in industrialization affecting the growth of greenhouse gas emissions) [2]. However, it is worth adding that uncertainty – as a non-measurable phenomenon in principle will also apply to threats that are not yet possible to determine [naming] (e.g. types of digital threats). F.J. Milliken distinguishes three types of uncertainty regarding the environment:
- *uncertainty of state* (misunderstanding of events and directions of development of the environment),
- *uncertainty of the effect* (no possibility to predict external influence on the organization), and
- *uncertainty of reaction.*

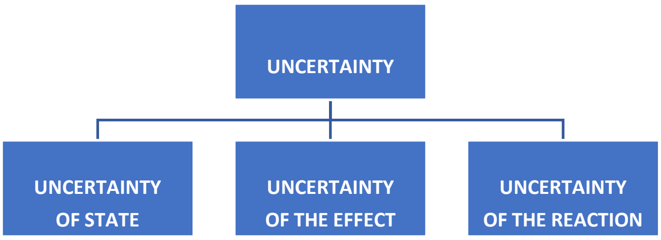

Fig. 1. *Types of uncertainty*

Uncertainty includes changes not only difficult to calculate and events that cannot be estimated, but above all – unpredictability. This fact causes significant complications in the possibility of shaping the security system at the stage of initial identification. In such a defined concept, it seems impossible to include an element of *uncertainty* in the analyses, however, one may attempt to adopt this category as a set preventing the adoption of preventive action plans, but enabling the undertaking of *ex post* actions (e.g. technical failures).

4. F.U.D. strategy

The F.U.D. [fear, uncertainty and doubts] is based on disinformation used, among others, in sales, marketing, politics, or broadly understood propaganda. The goal of the strategy is to influence perception by distributing negative ones and questionable or false information about the competition / opponent, etc.

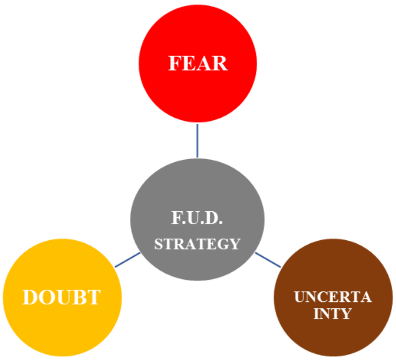

Fig.2. *Elements of FUD strategy*

FUD is an intended *tactic of rhetoric and error*, which was initially used in sales and marketing, especially in advanced technologies to discourage customers to consider competition products [beginning of the 1870s]. The idea was to convince buyers to use the *safe equipment* of a specific manufacturer, not competition equipment. The hidden coercion was based on reluctance to change, because change means risk, and risk can mean loss. An example can be a description of the system manufacturer: *Our software is 100% compatible with the existing* software. *[implication: some competitive systems are not.]* or: *Our equipment is 100% compatible with current systems*, or: *Our systems have already been used by over 1000 companies similar to yours. It has been proven. [implication: competition systems do not have such evidence]*.[3] After 1991, this term was generalized, referring to all kinds of disinformation used as a competitive weapon, which is currently used in a wide range. Analogically to the previously indicated uncertainty factor, the FUD strategy aims to induce a subjective sense of fear, doubt and uncertainty.

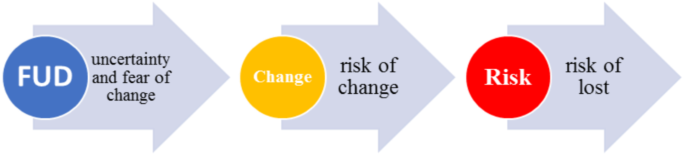

Fig. 3. *FUD strategy process*

With regard to security, this factor can be of key importance in two ways: an example can be a reinforcement of a sense of threat in society, which results in restricting rights and freedoms [to the privacy contained in the *Patriot Act*, which formally ceased to apply in 2015 – work is under way over regulations defined in the so-called *Freedom Act*]. The tightening of safety regulations is not new and finds its justification, however, the risk factors and risks that would underlie the changes are often overinterpreted. In another respect, the implementation of the FUD strategy may cause social unrest inspired by the services of foreign countries using, for example, social media.

In such context, the decisive aspect is also worth emphasizing. The decision-making process is based, above all, on information resources. The more reliable the information source – the more accurately the decision is made and the operation is more proper. The decision-making situation is influenced by both external conditions (general and task environment) and internal conditions (goals, structure, etc.) under which uncertain factors can cause the risk of making the wrong decision.

6. Results and discussion

Considering the unpredictability of uncertain factors – understood as unknown threats and risks, it can be assumed that the creation of a security system is objectively restricted in this respect. However, as mentioned, this category of uncertain events should be taken into account in management plans and – in particular, in ensuring the continuity of operation – using the *analogy of effects* as a tool. Then, taking appropriate actions would depend on the assessment of the impact of the given event. Regardless of objective reasons and barriers, identification of risks and threats should be subject to continuous updating as part of a dynamic and flexible adaptation of information resources and knowledge, as well as activities – to dynamically changing conditions of the environment and the security environment. Also in this case, the time factor is crucial – the faster identification, update and modification – the higher the level of the security system. The FUD strategy is today mainly associated with the sales and marketing sector, but its tools can be seen in all areas – especially in the area of information flows in cyberspace. Phenomena such as *fake news*, or *hate news* have permanently become part of online social media, becoming a tool of disinformation and propaganda.

These are phenomena that require not only analysis, but also the adoption of remedies, because – as results from the research – the impact on shaping public opinion by means of electronic media is definitely stronger than their classic counterparts. In addition, each user can become the creator of any information, anywhere in the digital space. In turn, the recipients of information check credibility and the truthfulness of only those that seem most unreliable or controversial for them. According to the results of the research carried out in 2018 [*Digital competences and the proliferation of threats*], in the area of checking the accuracy of information found on the Internet – almost ¼ of respondents confirmed that they check only what is controversial for them, and over 1/5 very rarely analyse the accuracy of information obtained from the network. 4.0% of respondents admitted that they never check whether the information obtained online is true. Taking into account the indicated tools of the FUD strategy and the results of research, it can be concluded that in the process of shaping the security system, not only factors and *uncertainty* criteria should be taken into account, but also factors related to the potential effects of the FUD strategy together with the possibility of neutralization of its effect in the information sphere.

7. References

[1] Szyłkowska M., *Human factor in the proliferation of threats* [in:] The Intentional Scientific Journal: "Security & Future" Issue 2/2018, s. 55- 58, ISSN (Print) 2535-0668, ISSN (Online) 2535-082X. 2018.

[2] Beck U., *Society of risk. On the way to another reality,* Pub. Scholar 2012.

[3] Chase–Jenkins L., Farr I. (2008), Risk Appetite: Boundary for Decisions, „Emphasis", Vol. 1, pp. 22–25.

[4] Miliken F.J., *Three Types of Perceived Uncertainty about the Environment: State, Effect, and Response Uncertainty* [in:] *Academy of Management Review", 1987, vol. 12, no. 1.*

[5] Source: https://strategypeak.com/fud-fear-uncertainty-doubt/

[6] SP 800-34 Rev. 1: Contingency Planning Guide for Federal Information Systems, source: https://csrc.nist.gov/publications/detail/sp/800-34/rev-1/final

[7] BSI (2008), Risk Management Code of Practice, British Standard BS 31100:2008, The British Standards Institution, London.

[8] Research carried out with the CAWI method – *Digital competences and the proliferation of threats,* November 2018.