sciendo CzOTO 2021, volume 3, issue 1, pp. 289-295

CONTEMPORARY CONDITIONS OF INFORMATION SECURITY

doi: 10.2478/czoto-2021-0030
Date of submission of the article to the Editor: 15/11/2020
Date of acceptance of the article by the Editor: 18/03/2021

Andrzej Gałecki[1] – *orcid id: 0000-0002-1770-2522*
[1]University of Security in Poznań, **Poland**

Abstract: In the age of the information society, determined by the evolution of digital technology, information has become an essential element of the functioning of every human being. Its acquisition, processing and distribution serves to satisfy the key areas of society's life and constitutes a necessary component of every decision-making process. These days became dominated by the increasing demand for information. The problem of its protection against unwanted obtaining (disclosure) has become a challenge for many scientific communities. This state of affairs has forced us to take a number of steps to ensure the security of useful information, characterized by accuracy, unambiguity, completeness and authenticity. The problem of information security is inseparably linked to the threats present in the cyberspace environment. They are commonly identified with the so-called computer crime, resulting in factors like: infiltration, obtaining passwords and other data used for logging in, identity theft, damage (blocking) of systems and their software. Information manipulation is a completely different and underestimated threat to rational decision-making process. Wherefore, useful information that is characterized by the expected properties, is exposed not only to destruction or unauthorized acquisition, but also to distortion. Rising anxiety about the credibility of the information received in the virtual space and the sources of its transmission forced the need to distinguish the real form from the one that was modified. The presented conditions prompted the author to propose solutions with regard to information security, determined by the difficulty of obtaining it and manipulating it.

Keywords: cyberspace, cyberthreats, information society, heuristic methods, manipulation

INTRODUCTION

Having information is an unquestionable advantage of making all decisions rationally. In other words, information has crucial meaning for solving decision problems. Lack of information about the surrounding reality makes a person helpless, and thus ineffective in their actions. The functioning of all areas of the modern world, e.g. in the social, political, economic, and national security areas - depends on the availability of information resources and usefulness which is defined as credibility, timeliness and accuracy. A particular need for information understood in this way is observed while solving complex decision problems (difficult to predict or with a structure that has not been seen so far). Therefore, the question arises: what methods can be used of which the implementation would help to solve decision-making problems in the period of information deficit?

Due to the developing technology of cyber threats, the institutions responsible for information security have focused their main efforts on monitoring and analyzing them, notifying interested entities about recorded incidents, response in terms of combating their effects, as well as using measures to increase system defence.

In relation to the current objects of attack, in the recent period (NASK, 2019), the phenomenon of disseminating false information, referred to as disinformation, has been observed. Disinformation has become the basic tool of manipulation of which the spectrum of disinformation techniques is increasingly used in the media space. Therefore, another research problem was created in the form of the question: are there any ways to limit manipulation of the information?

SELECTED DETERMINANTS OF INFORMATION SECURITY

Since the production, gathering, distribution and, above all, use of information are a significant feature of the present day, it can be assumed that it is an indispensable component that serves man in every area of his functioning. Its lack or significant limitation is a problem in many processes, e.g. hazard identification. It is essential in the decision making process.

The effects of decisions will depend on the quality, quantity, timeliness and credibility of information. As part of the quality of information, its accuracy can be taken into account which is often defined by the recipient's requirements (with regard to its purpose, management level or command).Having information about the expected parameters is particularly important while solving complex situations that require making the right decisions in a short time. Such conditions accompany, for example, crisis situations initiated by various security threats. The crisis management process is determined by a number of factors, including: the specificity of a crisis situation, system effectiveness, as well as response time conditioned by the availability of information on threats.

The most important factor determining the correct identification of the causes, scale and effects of crisis situations are the limitations causing the information indeterminacy. Its determinants are gaps information and information distortions caused by intentional or accidental actions. The problem of making decisions in conditions of incomplete information or its complete loss required research.

On the basis of the obtained research results (Gałecki, 2005), it was found that due to the availability and quality of information, deterministic and nondeterministic decisions can be distinguished. In the first case, when decisions are made on the basis of right time of receiving, complete and reliable information, it is accompanied by the so-called certainty conditions. From the point of view of the decision-making process, this is a comfortable situation, which, unfortunately, is not always the case. Usually, when information is incomplete or lost for various reasons, we are dealing with uncertain (undefined) states. In such conditions, decision-makers use the advantages of intuition, which is conducive to the ability to predict the development of a specific event.

When to use algorithmic rules and when to use heuristic rules? The main difference between the routine approach (using algorithms) and the creative approach (using heuristics) is that the first approach always produces a solution, while the creative approach is not always effective. Algorithmic rules, in comparison with heuristic rules, are reliable, i.e. they guarantee the solution of the task. They can have universal application, directed to a specific class of tasks. They are defined, i.e. they contain a defined chain of operations that must be performed in order to achieve the assumed goal. The basic condition for its fulfillment is to have useful information.

The undoubted advantage of heuristic rules is the possibility of applying them in situations of information indeterminacy. Although they are "slower" than algorithmic rules, they provide a chance for ultimate success in the process of solving decision problems. Although they are "slower" than algorithmic rules, they provide a chance for ultimate success in the process of solving decision problems. Decision-making practice provides many examples that the existing information gaps are a frequent cause of risky decisions which the effects are not fully predictable.

On the basis of the research conducted in the field of the application of heuristic methods, the ones whose properties favor solving information problems were distinguished. One of them is synectics (developed by W. J. Gordon), the essence which comes down to applying analogies to the subject of research (e.g. a specific event) and other circumstance seemingly having nothing in common. Due to its properties, the analyzed process can also use lateral thinking (created by Edward De Bono). Its characteristic feature is the resignation from template (ready-made) regulations in favor of unconventional actions, expressed in the lists of associations created for this purpose. The association function is also specific to the superposition method. Another proposal in this regard are the so-called availability (knowledge) heuristics, the idea of which is reduced to automatic inference based on the availability of memory traces. Gerd Gigerenzer, noticing its advantages, emphasized that it is a method that can be used in all conditions. In further considerations it was assumed that in the so-called Information uncertainty, the basic tools for creative solution of decision-making tasks should be: situational association, discovering facts, predicting events, the last of which would be based on extrapolation. Heuristic forecasting can be classified as a derivative of the above-mentioned methods, it makes it possible to predict circumstance that cannot always be presented by analyzing past facts. It is also identified with some features of intuition, therefore it can be concluded that on the basis of it, the experience of specialists and the ability to associate information, it is possible to make forecasts of the phenomenon we are interested in.

The occurring cases of information deficit are not something isolated and may result from the limited possibilities of obtaining or distorting its reception. In the Claude Shannon-Weaver model of information transfer, the process of communication between the sender and its recipient is included, in which the ideal state is the compliance of the received information with the content sent. In practice, we are dealing with a variety of intentional or accidental disturbances, perceived in terms of information security threats (the model takes into account the possibility of disturbances occurring during the signal flow through the channel, called it noise).

The concept of information security is defined as "a set of actions, methods and procedures undertaken by authorized entities, aimed at ensuring the integrity of collected, stored and processed information resources by securing them against undesirable, unauthorized disclosure, modification or destruction" (Potejjko 2009). The environment in which there is unlimited communication (information exchange) is cyberspace. It created perfect conditions for the comprehensive satisfaction of social needs, economic development and security, and at the same time multi-spectral threats to information and the systems processing it. Functioning in the information society, we do not usually wonder from what sources we receive information and whether it is fully reliable. Such doubts result from the widespread use of widely understood manipulation, which until recently was considered as harmless way of influencing humans. Today, its importance for the functioning of society, the operation of systems, organizations and the state is noticed and treated as a priority by many scientific circles. We come across the term manipulation very often.

Manipulation has different meanings and refers to various fields, but most often it is used in psychological terms (Grzywa, 2013). In this area, manipulation means a way of influencing another person, their way of thinking, opinions without their knowledge. There is also an opinion that manipulation to some extent violates the freedom of another person, affects their attitude, views and even behavior. According to the Dictionary of Foreign Words, manipulation is a sneaky use of some circumstances, bending, distorting facts in order to direct someone without his knowledge, influence other people's affairs, for their own benefit (Lost Spaces, 1995).

This term comes from the Latin "manus pellere", which means "to hold someone in someone's hand, to have someone in his hand" and means (broadly speaking) "influencing a person, using him against his will" (Hanas, 2000). The concept of manipulation or social manipulation (generally a negative term) appeared in social sciences in the 1980s (Harwas-Napierała, 2005). This term describes such a way of influencing other people, the mechanism of which is to be hidden from people subjected to its influence. This term describes such a way of influencing other people, the mechanism of which is to be hidden from people subjected to its influence. It is usually characterized by an indirect influence on consciousness, as well as a specific intention and purpose of this influence. Manipulation, therefore, is the intetional and deliberate control of the behavior of a person, a social group subjected to the influence. The condition for effective manipulation is its imperceptibility (Grzywa, 2013). Manipulation has become a technical term that describes a whole series of procedures that make it easier to influence someone's decisions (Babik, 2011).It also means maneuver, trick, guile. It is the ability to govern others, based on the knowledge of the principles of command, to conduct negotiations in order to get the partner to change his mind (Cialdini, 2009).

An example of the use of the first type of manipulation are the rules also referred to as stratagems, developed for the purpose of war by Sun Tzu. Currently, the strategic theses of one of the greatest thinkers of the Far East and the German philosopher Artur Schopenhauer are applied in business, politics, in organized and unorganized activities, as well as in the cyberspace environment.

We can also manipulate with actions, words, gestures, facial expressions (non-verbal communication), smell, as well as sound and image. The methods of word manipulation were presented, inter alia, by Artur Schopenhauer in the space of the art of dispute (Schopenhauer, 1997). In times of mass information transfer, we become its recipients and distributors. There is no doubt that an image (photos, graphics, caricature, etc.) is an excellent form of influencing human consciousness, view, and attitude. Skillful transformation (deformation) of the real image creates the conditions for the reception expected by its sender.

One of the manipulation tools is disinformation, the importance of which in the CERT Polska report was defined as one of the major challenges for information security. Falsifying information has become a practice used by cybercriminals as well as an information warfare tool. Due to the significance of this threat, NASK PIB has prepared a separate report "The phenomenon of disinformation in the era of the digital revolution" devoted to the social, economic and psychological aspects of disinformation (NASK, 2019).

Contemporary disinformation has taken many different forms, such as hostile propaganda, ideological subversion, trolling, and malicious moderation of discussions on forums and social media. It often uses measures that are tailored to the specifics of countries, societies and specific target groups to distort the truth, sow distrust or raise doubts (NASK, 2019). Disinformation can be perceived as an advanced formula of communication, interfering with the recipient's decision-making process, the purpose of which is to evoke a view, decision, action or lack thereof, in accordance with the assumption of the center that planned the process of misleading the recipient. The subject of distorted message may concern political aspects, conspiracy theories, existing and prognostic threats (e.g. pandemic development), etc.

PROPOSALS CONCERNING THE SELECTION OF INFORMATION

The popularization of the Internet, the use of various social networking sites and platforms has resulted in measures to counteraction disinformation and its harmful impact on the formation of views and democratic processes. Following the published Communication of the European Commission of April 26, 2019, another very important document was adopted - the Code of Conduct on Combating Disinformation was a form of self-regulation of the business sector and was developed by representatives of online platforms, the advertising industry and the media, with the support of academia and civil society (NASK, 2019). On this basis, a number of initiatives were undertaken aimed at reducing the negative potential of disseminating false information. Among others, representatives of Google, Facebook, Twitter and Mozilla have undertaken self-regulatory actions in this area, in order to reduce the phenomenon of disinformation in the Internet space.

Obviously, falsifying information is one thing, and influencing the perception of occurring phenomena, masking what is important in the context of decisions made, is another. The use of manipulation techniques may also have the dimension of a specific "investment" in the strategic intentions of its initiator. There are examples of the use of algorithms to determine the psychodemographic profile of global network users (Doliwa, et al., 2018), used to identify the vulnerability of global network users to various types of events (e.g. in the political dimension).

Is it possible then to select reliable information from its distorted form? In airspace recognition systems for selecting useful information against the background of imitating disturbances, created in order to make it difficult to detect and track actual information about the air situation, specialized anti-jamming systems are used. On the other hand, the IFF (Identification Friend or Foe) system is used to assess the reliability (type and nationality of an aircraft or other unit). Its operation is reduced to sending a query from the interrogator to a transponder on board the aircraft, as a result of which the transponder responds to its content in a strictly defined manner.

Based on the existing solutions in the technology of radar reconnaissance systems, in relation to information posted in the Internet space, the key in determining its authenticity is the identification of the source of the sender (Fig. 1). A solution proposal in this respect would be the use of signatures (identifiers) containing the characteristics of the sender and the type of information. On the basis of the association function, which is a common feature of the heuristic methods presented in this paper, and the comparison of the sent message with information from other sources (in relation to the "best representative"), it is possible to solve the problem formulated in this way. Moreover, in order to check the reliability of the information source, it would be reasonable to assign a trustworthy status, and the selection of the actual information can be made based on the authentication algorithm. The model of the layered structure of communication protocols (Transmission Control Protocol / Internet Protocol - TCP / IP) uses a simple, but above all effective user verification mechanism.

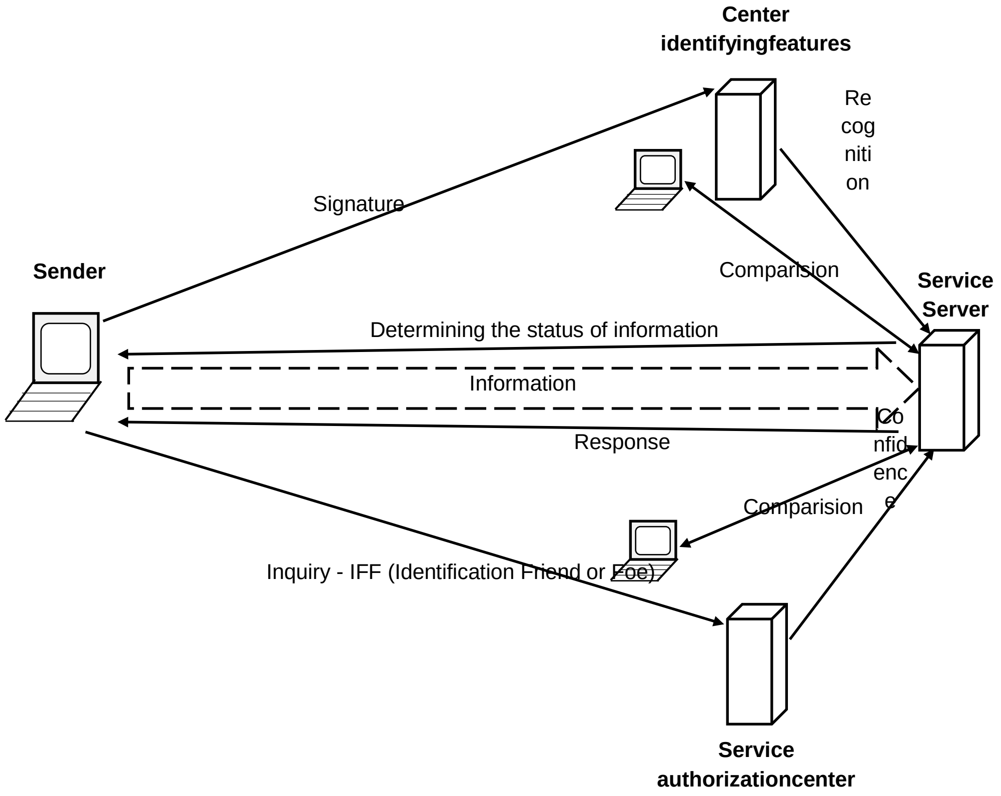

Fig. 1. General information verification scheme

Another solution for authentication is to attach a key (Message Authentication Code - MAC) to the message. It should be borne in mind that the use of the universal key does not ensure the security of the transmitted information. In the era of cyber threats, intercepting it with the attached code should not be a big problem (nowadays it is done by specialized programs). For this reason, to ensure integrity and authenticity, each piece of information should be randomly assigned unique keys (secret keys) that identify the credibility of the source and the content of the information.

CONCLUSION

An in-depth analysis of what the heuristics offers fix the author of this study in the belief that the implementation of some of the methods presented to solve decision problems in situations of information indeterminacy is possible. The conducted research proves that the most favorable conditions for this goal would be: morphological analysis, lateral thinking, superposition, but most of all symbolic and direct analogy and the synectic method.

Information indeterminacy may also be caused by information manipulation, which not only has become a common phenomenon, but also a "norm" in the functioning of many environments in our lives. Such a state of affairs threatens its rational assessment, because among many distorted (false) contents of information, those that are true information may be omitted. For this reason, one should strive to obtain useful information, the main determinant of which is its credibility. It can therefore be assumed that in this aspect, information security in the era of cyber threats becomes more and more important.

The development of science contributed to, inter alia, easy communication and exchange of all information by users of the global Internet network, creating conditions for its unauthorized interference and criminal use. In the environment of a dynamically changing world, in order to maintain an acceptable level of human functioning, it is necessary to take actions limiting the possibility of interfering with the possessed information resources. Due to the changing conditions of information security in the cyberspace environment, the results obtained in this area should be implemented and verified in accordance with the Deming cycle.

REFERENCES

Babik, W., 2011. *On manipulating information in private and public information space,* in: *Man, media education*, Pedagogical University, Krakow, 3.

Gałecki, A., 2005. *Sources and methods of pose for information on the air situation*, National Defense University, Warsaw, 121.

Cialdini, R., 2009. *Influencing people. Theory and Practice*, Gdańskie Wydawnictwo Psychologiczne, Gdańsk, 186-195.

Doliwa, U., et al., 2018. *Precise profiling of Facebook Users or reading tea leaves?* A critical analysis of the operation of the algorithm created by Michał Kosiński and used by the Cambridge Analytica software, Zeszyty Prasoznawcze, Kraków, 61, 3 (235), 532.

Grzywa, A., 2013. *Manipulation everything you need to know about it*, Wydawnictwo Słowa i Myśli, Lublin, 11.

Hanas, Z., 2005. *Various Forms of Manipulating a Man*, Communio, 2000, 1, 56.

Harwas-Napierała, B., 2005. *Ethical aspects of manipulation*, Poznań Theological Studies, Adam Mickiewicz University, Poznań, 248.

NASK CERT Polska, 2019. *The security landscape of the Polish Internet*, Annual report on the activities of CERT Polska, 9.

Potejko, P., 2009. *Information security* in: Wojtaszczyk, K., Materska-Sosnowska, A. (ed.), State security, ASPRA-JR publishing house, Warsaw, 194.

Schopenhauer, A., 1973. *Erystyka, or the art of disputes*, Wydawnictwo Literackie Kraków, 45.

Dictionary of Foreign Words, 1995. PWN Publishing House, Warsaw, 686.

The phenomenon of disinformation in the age of digital revolution, 2019. State. Society. Polityka, Biznes, NASK National Research Institute, Warsaw, 9.