We see what we want to see: Pitfalls of Perception and Decision-making in Security Management

Helvi Salminen
Thales DIS Finland Oy, Vantaa, Finland

helviksalminen@gmail.com

Abstract: We human beings are often convinced of having a clear picture of reality and believe ourselves to be thoroughly rational in our thinking and decision-making. However, our perception of reality is limited and prone to errors, and our decision-making is often guided by emotions and instincts instead of facts and rational thinking. If we don't stop to think we often jump to conclusions based on partial or erroneous information, and eloquently justify our decisions with apparently rational arguments. In many areas of human activities, including security management, limits of perception and errors in decision-making can have harmful, even disastrous consequences. Very often in security management the decision-making process is not sufficiently challenged by critical thinking as decisions are often made hidden behind the veil of secrets. Cognitive biases - systematic errors in thinking affecting decisions and judgments - have been identified and analysed in various contexts, and the results have been applied to improve decision-making processes. However, in the heavily regulated and compliance-dominated world of security management sufficient attention hasn't been paid to cognitive biases and their impacts. As result of insufficient attention an important risk factor is regularly underestimated. This paper includes an introduction to the concept of cognitive biases and the research on the phenomenon. The biases which in the author's experience have a particularly harmful impact on security management are described in detail. This introduction is followed by description of scenarios and real-life examples where erroneous perception and decision-making of security actors leads to disasters. De-biasing is the strategy which aims at eliminating or at least limiting of the impact of cognitive biases. This strategy has been successfully implemented in various types of environments. This paper presents ideas how de-biasing strategies could be implemented in security management in order to improve the quality of decision-making.

Keywords: Cognitive Bias, Security Management, Decision Making

1. Introduction

Cognitive biases are mental patterns which are deviations from rational reasoning. Biases and their impacts are widely discussed in scientific literature and at several popular books and websites. Definitions of nearly 200 biases can be found in various sources.

The Alleydog website (2023) summarizes various definitions of cognitive bias as follows:

- A Cognitive Bias is an involuntary pattern of thinking that produces distorted perceptions of people, surroundings, and situations around us. You can also consider it an altered way of thinking that affects our perceptions and decisions, and can cause mistakes in reasoning, logic, and evaluation.
- Some research suggests that cognitive biases are mental processing "shortcuts" that allow us to make decisions faster when time is a more important issue than accuracy of judgment. These types of cognitive biases are used more frequently when we have limited mental processing capabilities due to lack of time or lack of knowledge about a subject or situation. This is purported to be evolutionary in nature so that we can identify possible dangerous situations quickly.

Cognitive biases are mainly based on *system 1* processes – fast, intuitive judgements and actions without stopping to think.

Biases can be classified into different categories based on their impact and where they apply. They can, for instance impact an individual's decision-making, a group's behaviour, risk taking and motivation. Biases can also cause an individual to misunderstand the importance of alternatives or neglect essential facts in decision-making.

Cognitive biases have also been suggested to be attempts to resolve problems. Why these attempts often fail depends on the complexity of modern society where simple solutions often are not relevant. Valdez et al (2017) present a framework for studying cognitive biases. The article includes cognitive bias codex in which the biases are divided in the following four main categories:

- Too much information –to cope with a flood of information around us the brain filters out most of it, and picks out the pieces which are likely to be useful (for instance a*nchoring* and *confirmation bias*).

- Not enough meaning – the world is not seen as a set of isolated events, instead the brain tries to make sense of it by filling the gaps with already existing knowledge (for instance *illusion of validity* and *impact bias*).
- Need to act fast in a situation of uncertainty it is sometimes necessary to act fast and there is no time to make a profound judgement of all possibilities (for instance *overconfidence*).
- What should we remember – as it is not possible to remember everything one sees and experiences, lots of details are discarded and the remaining information is associated to existing memory structures which further enforces the criteria of selecting what to remember (for instance *misattribution of memory* and *primacy effect*).

Biases are common, and so is the bias blind spot: often people are not aware of their own biases and tend to see other people as more biased than themselves.

Perception error and cognitive biases impact all areas of human activity. This article describes the basic facts of cognitive biases and explains their potential impact on security management.

2. System 1 and system 2

People often prefer to see themselves as thoroughly rational and are convinced to make decisions based on facts. The human mind has the capability of rational thinking and decision-making, but the human cognition has also other characteristics.

According to dual-system theory, human cognition has two distinct types of thinking: one that is fast, automatic and effortless (system 1), and one that is slow, analytic and effortful (system 2). Often an activity is initiated by system 1 but completing it requires the involvement of system 2. System 1 includes the innate skills, system 2 is result of learning.

Kahneman (2012) explains the characteristics of these two systems, and mentions as automatic activities of system 1 for instance the following:

- Detect that one object is more distant than the other
- Orient to the source of a sudden sound
- Detect hostility in a voice
- Understand simple sentences

The following is a list of activities which require system 2 to be activated:

- Focus on the voice of a particular person in a crowded and noisy room.
- Monitor the appropriateness of your behaviour in a social situation.
- Fill out a tax form.
- Check the validity of a complex logical argument.

The influence of system 1 on human reasoning is often underestimated. Kahneman shows that it has an important role in our thinking process. When conscious rational thinking is not guiding the decisions, the result can be error of judgement. These errors are called cognitive biases which are described in the next section.

The advantages and disadvantages of the two systems have been described by Kahneman and several other researchers. The following table shows how Rzepczynski (2023) summarizes the characteristics, advantages and disadvantages of the two systems.

Table 1: System 1 and system 2 characteristics – based on Rzepczynski (2023)

	System 1	System 2
Characteristics	Fast Effortless Unconscious Triggers emotions Associative Looks for patterns Looks for causation Creates stories to explain events	Slow Effortful Conscious Logical Deliberative Can handle abstract concepts
Advantages	Speed of response in a crisis Easy completion of routine and repetitive tasks Creativity through associations, so good for expansive thinking	Allows reflection and consideration of the “bigger picture”, options, pros and cons, consequences Can handle logic, maths, statistics Good for reductive thinking

	System 1	System 2
Disadvantages	Jumps to conclusions Unhelpful emotional responses Can make errors that are not detected and corrected, such as wrong assumptions, poor judgements, false causal links	Slow, so requires time Requires effort and energy, which can lead to decision fatigue

3. Illusions

Many of the judgement errors that manifest themselves as cognitive biases have their roots in incomplete or erroneous perceptions of reality. Chabris and Simons (2009) describe in detail the mechanisms of everyday life perception errors, which they call illusions.

The six illusions having a major impact on people's lives are

- *Illusion of attention* – the belief of processing all information around and failure to understand that observations are limited only to the things on which attention is focused.
- *Illusion of memory* – the misunderstanding of how memory actually works and the overestimating of one's memory capacity and accuracy.
- *Illusion of confidence* – overestimating one's own abilities especially relative to other people, and seeing confidence as evidence of competence.
- *Illusion of knowledge* - a person thinks to know more than he/she really knows.
- *Illusion of cause* – seeing the causal relationship between things where there is none.
- *Illusion of potential* – believing that there are unused hidden potentials in the human brain and these potentials can be released with simple techniques.

The next sections look into more detail about each of the above-mentioned illusions.

3.1 Illusion of attention

According to Saariluoma et al. (2000) thinking starts from stimuli that our senses collect from our environment. Attention can be focused only on one thing at a time, so inevitably many surrounding events remain unnoticed and thus don't have impact on the thinking process. As the information on which decisions are made is incomplete, thinking errors – thinking which produces non-optimal results – are inevitable.

Chabris and Simons (2009) give several examples of in-attentional blindness – a situation in which an individual fails to perceive an unexpected stimulus in plain sight. This failure succeeds when there are numerous stimuli and attending to them all is practically impossible. Attention is given to stimuli which the individual expects to see or which are so salient that they attract the observer's attention.

People who believe their attention covers a bigger portion of reality than it actually does are under the *illusion of attention*. Chabris and Simons have conducted several experiments which verify this claim – people fail to see even a gorilla or a violent beating of a person when their attention is attracted to something else.

The limitations of attention can cause involuntary errors, but they can be used also on purpose to support the objectives of someone who is in control of a situation.

3.2 Illusion of memory

Many people would like to see memory as exact recordings of events. However, the human memory does not work as a video or sound recording device – instead of recording events exactly as they are, the memory makes selections of what to preserve and associates it with already existing memories. Believing to remember more things and more accurately is a symptom of the *illusion of memory.*

Chabris and Simons (2009) also explain how memories depend on the limitations of perceptions. We can only remember things which have been in the focus of our attention, and our attention depends also on what we expect to see. With several examples the authors also demonstrate that memories – even the most vivid ones – change when time passes. Also recalling events from the long-term memory change the memories.

Relying on human memory can have negative consequences if the memories are incomplete or altered – for instance in the case when eyewitness of a crime gives honest but faulty testimony resulting in conviction of an innocent person.

3.3 Illusion of confidence

According to Chabris and Simons (2009) the illusion of confidence has two distinct aspects which are, however, related to each other:

- People tend to overestimate their own capabilities especially relative to other people.
- Confidence is valued as a demonstration of competence.

The first aspect is clearly seen when people driving cars are asked how they consider themselves as drivers. A clear majority claims to be better drivers than the average – which of course cannot be true. Overconfidence – excessive belief in one's superior qualities – can turn against the confident person or company if it leads to lack of self-criticism and failure to see the need for development.

Chabris and Simons state that when starting to learn new skills the original skill level is low and confidence often higher than the reals skills – which means overconfidence. Along with improving skills the gap shrinks. The difference between skill level and confidence is called the confidence gap. Naturally the confidence gap can also be the other way around and the skill level can be higher than confidence in the skills. The following picture illustrates the two different confidence gaps.

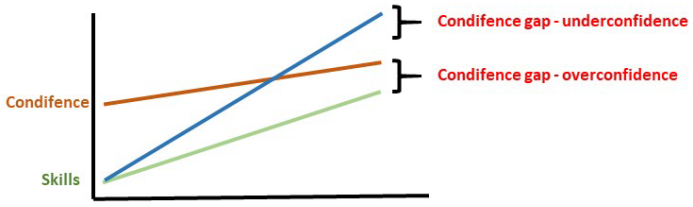

Figure 1: Confidence gap

In groups of humans confident persons tend to dominate communication, and usually are opinion leaders. People can act with confidence for good reasons, but it is not rare that a very confident person manifests overconfidence – not superior competence.

According to Chabris and Simons the most dangerous kind of overconfidence in one's abilities is when we one is unskilled, but the level of confidence is much higher. On the other hand, under-confidence can cause lack of initiative and poor performance.

Harris (2022) describes *confidence cycle* as a model for developing useful skills and achieving the balance of skills and confidence. The cycle is quite similar to the PDCA (Plan, Do, Check,Act) of ISO management system standards.

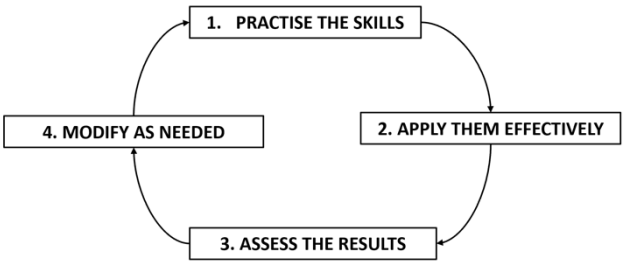

Figure 2: The confidence cycle – based on Harris (2022)

3.4 Illusion of knowledge

When people think to know more than they really do they are under the influence of *illusion of knowledge.* This illusion, like other everyday illusions, is very common.

Even when people know that they don't know everything, they often believe to have the knowledge which in a given context is essential for making rational decisions. The illusion of knowledge combined with the illusion of

confidence in a person is decision-making position is a toxic combination which at worst can cause disasters in organizations and private lives of individuals.

Chabris and Simons (2009) claim that the illusion of knowledge persists partly because people tend to rely on experts who are confident and think to know more than they really two. Some organizational cultures can also favour people who have the combination of illusions of confidence and knowledge.

3.5 Illusion of cause

When people make wrong assumptions about the cause of events, they have fallen into the trap of the *illusion of cause*. This illusion appears in many ways, all of which could be summarized "jumping into conclusions".

One of the factors contributing to the illusion cause is the timing of events. It is quite common for people to believe that earlier events cause later ones even when there is no dependence between the two. Mistaking to think that the correlation of events always indicates causal relationship is quite common.

One form of the illusion of cause are conspiracy theories. A person under this illusion is convinced to have identified in events patterns which are proofs of causal relationships. The observations of conspiracy theorists are guided by "research" in which the result is fixed in advance.

Anyone working in risk management and incident investigation should be very careful not to jump into conclusions. Interpretation of causal relationships should be based on facts, not on opinions.

3.6 Illusion of potential

Many people think that we humans use only 10 per cent of our brain capacity. This idea persists even though there is no evidence to support it. Instead, several sources, including OECD (2023) present several arguments against it, for instance, the following:

- The human brain weighs approximately 2% of the total body weight, it uses 20% of the whole energy. Evolution does not favour waste of resources, so it is unlikely that the sophisticated and complex human brain has evolved to be utilized only with 10 per cent efficiency.
- If we use only 10 per cent of the brain capacity, losing 90 per cent of it should not be a major problem. However, experiences in clinical neurology show that this level of loss has serious consequences.
- The knowledge of functions of different sections of the brain and modern imaging techniques clearly demonstrate that 90 per cent of the brain is not inactive.

So the 10 per cent myth has been busted by several researchers.

Chabris and Simons (2009) describe also another myth – the Mozart effect. This myth states that just by listening Mozart's music the dormant capacities of the human brain are released and can be used. Like the 10 per cent myth, the Mozart effect is not supported by any scientific evidence.

4. Cognitive biases in security management

We have now had a look at basics of cognitive biases. Security management is human activity and thus subject to cognitive biases.

4.1 Security management

The purpose of security management in an organization is to protect organization's valuable assets from threats which could damage or destroy the assets. The assets include people, buildings, machines, systems, business processes, information, reputation – and anything else that the organization needs to continue its activities. The assets must be identified, and the policies and procedures to protect them must be developed and applied.

Several frameworks have been defined for security management either in the form of publicly available standards like ISO/IEC 27001 for information security management or as control frameworks for a specific purpose like Intergraf Certification Requirements for security printing companies. The frameworks define requirements for management procedures or a set of mandatory controls which must be applied in the organization – or a combination of both.

Smith and Brooks (2013) describe in their book about security science three different types of strategic security management frameworks: risk-based, quality assurance, governance and strategic approach. Based on several models components of a consolidated framework of security science is introduced. Topics addressed by the framework include security risk management, business continuity management, technology; physical, personnel and industrial security, investigations, law, criminology, facility management, fire & life safety, and intelligence.

The Confederation of Finnish Industries (EK 2023) has developed a security management model. It is described as nested circles. In the inmost circle there is the target state – business continuity and compliance with security requirements. The target state is achieved with security management which consists of information security, facility management, crisis management, management of fraud and incidents, life safety, personnel security, environmental security, workplace security and security of production and operations.

The scientific approach of Smith and Brooks and the practical approach of the Confederation of Finnish Industries include a lot in common. They both address the same main asset categories and require organization's top management involvement. Many other existing frameworks are also built on same type of layered approach. Strong integration to business objectives is also emphasized I most models.

It is obvious that there is no simple definition of security management. However, keeping in mind the definition that the purpose of security is to protect an organization's valuable assets from different types of threats, it is possible to understand the impact of cognitive biases in managing security. The situation is complicated due to the nature of security – some issues are not open to everyone in the organization, for instance, monitoring methods would lose their efficiency if details are exposed to a large audience. This makes it more difficult to notice if security decisions go wrong due to cognitive biases.

4.2 Impact of cognitive biases on security management

Currently a comprehensive analysis of cognitive biases in security management is not available. This section includes descriptions of some cognitive biases which according to the author's professional experience and discussions with other security professionals could be particularly harmful when appearing in security management. For each bias its potential impact on security management is described briefly in an example case. When the example is from an event reported in public this is indicated. The definitions of biases included in this section are mainly based on Kahneman (2012) and Chabris and Simons (2009).

Anchoring is the tendency to make judgements based on a piece of information (anchor) which can be the first piece of information obtained on a subject, or information recently hear but irrelevant in the given context.

When a person searches and interprets only information which is compatible with existing ideas and discards other information, her/his reasoning is limited by *confirmation bias*.

- The security manager is investigating a major security incident. A previous minor incident was caused by one employee (X) who made a minor deviation from security rules, and was given a formal warning. In the current investigation the security manager concentrates major efforts on the actions of X who is suspended from work. X's actions could not be traced back to be the root cause, but were rather a enabled by some underlying problem. The collected audit trails indicate errors made by another employee (Y), but because this person had a clean record and is a popular person in the work community, the security manager systematically ignores the evidences. Only when a second incident occurs, proper actions are taken.
- In this case the anchor was the previous misconduct of X, and the confirmation bias caused important evidences to be ignored in the investigation.

Framing is a powerful tool in directing people's judgements. By presenting the same information differently causes the receiver to make different interpretations based on the frame more than the actual contents.

- Company X is planning to buy a smaller company. It hires a consultant to make the research of potential targets. The research points out two alternatives. The consultant's report describes A as an innovative company with excellent future prospects, and explains that its poor economic result depends on a major investment in people and innovations. Instead, B which has a stable client base and good economic record, but very little growth in the last couple of years, is evaluated to have lost its innovative power – and for this reason the consultant's recommendation is A.

- The security manager of the company X reviews the risks of the two options. His recommendation is B, because B has a mature management system, which includes well-defined security procedures.
- These two frames – opportunities vs. risks - produce opposite results.

Security frameworks are specific frames. They define topics to which security management should pay attention. However, it is important to maintain an open mind and see if important security topics are not addressed by the frameworks.

Illusory correlation means seeing unrelated events as connected. If we add to the equation the causal relationship between the observed events, the result is the *illusion of cause.*

- Illusion of cause is particularly harmful in security incident investigation and risk analysis. If root causes of incidents are not identified, proper actions to prevent similar incidents in future cannot be taken. The same applies to risk treatment – even if the risk is correctly identified and analysed, failure to understand the causal relationship between the risk and possible consequences can result in inefficient risk treatment.

A person who has *authority bias* gives value to and is influenced by the opinion of an authority, even if there is a reason to doubt.

The following is a real life example (EDRI 2005)

- Sonera (Finnish telecom company which later merged with Telia) management ordered detailed examination of telephone behaviour of employees in order to find out who was leaking information to press. On another occasion the security staff voluntarily and without legal basis provided monitoring data to police to assist in investigation. Five persons got suspend sentences.
- The public sources don't give any clear clues about the impacting cognitive biases. However, considering the persons involved, *authority bias* could be one of them – the actions started from executive management orders which were not challenged by the security team. *Groupthink* (the pressure to agree with the group without criticism) and overconfidence may also have played an important role.

Availability bias makes us overestimate the probability of events and give too much value to ideas which are readily available in mind.

- Many of the issued addressed with security management procedures are known problems and deserve the attention given to them. However, if the security manager fails to "think out of the box" she/he is limited by the *availability bias*, and many important issues which are not inside the standard management frame, or are complex, remain unnoticed.
- The other side of the coin is the *salience bias* which causes us to overestimate the probability and significance of salient events which attract our attention. In the context of security management this could, for instance, occur in case of a minor security audit finding which is erroneously seen as an indication of an underlying major problem. The organization allocates a lot of resources to prevent the same type of minor issues from occurring, and thus fails to identify and correct issues which are more probable and potentially much more harmful.

We fire with a m*ental shotgun* when we answer to questions, and instead of answering the complex question answer a much easier question.

- The security manager is asked to verify if a proposed action is compliant with applicable requirements. The answer is provided quickly – compliance verified – and the actions taken.
- Later, a closer look at the regulations reveals the unpleasant fact that the action would have required approval of competent regulatory authorities.
- *Chauffeur knowledge* - fluently outspoken information without the speaker having real profound knowledge of the topic – is often the factor launching the mental shotgun.

According to Kahneman (2012) psychologists discovered in the 1980's that exposure to a word causes immediate changes in how easily many related words can be evoked. This *priming effect* is not restricted to concepts and words. A person's emotions, thoughts and actions can be influenced by stimuli of which the person is not even aware. The priming effects can also be concatenated and one priming can launch another. As the impacts of

priming don't happen in the conscious mind, they may be even harder to recognize than other types of biases. Effective priming requires knowledge of the culture of the target environment.

- Security frameworks require systematic and documented management of risks. The risk management procedure can be distracted by discussions which emphasize risks which receive lot of public attention but are irrelevant in the target environment. As result organization's resources can be spent on risk treatment plans which have no impact on the risk level, and more critical risks are not addressed.

5. Debiasing – limiting the impact of cognitive biases

5.1 Debiasing techniques

Various techniques, methods and interventions have been designed to limit the impact of cognitive biases. There are several types of de-biasing techniques targeting cognitive processes, motivation or the environment. To improve the decision-making the de-biasing technique can try to change the decision-maker's behaviour or the environment in which decisions are made.

The decision maker's behaviour can be impacted with suitable targeted training. Morewedge et al (2015) have shown that even a single training intervention can have significant de-biasing effects that persist across a variety of contexts affected by the same bias.

In a decision-making situation the organization can require the persons to consider more than one alternative and be trained in generating alternative solutions to problems. In many situations checklists are a good tool which can prevent skipping essential phases of the decision-making process.

Often things can go wrong because there are organizational habits which may have been relevant when formed but can be harmful in the current situation. Breaking the cycle of habits is not easy, but can be done for instance by rewarding the desired behaviour. Additional information can help when erroneous judgement depends on insufficient knowledge.

Training is essential in debiasing. Soll et al (2015) show that even a single well-designed training event can have long-term impacts.

Useful de-biasing techniques are often context-dependent – what works in one situation may be quite useless in a totally different environment.

5.2 Encouraging example of successful de-biasing

There are encouraging examples of successful debiasing. One of them is the case of RWE (prior to 1990 Rheinisch-Westfälisches Elektrizitätswerk AG) de-biasing project described by Günther et al (2017). RWE is a German company operating in the energy sector. The company's economic result had dropped significantly. and the shareholders were demanding answers from management. The situation was analysed, and the result of the analysis was management underperformance and several cognitive biases. Status quo and confirmation biases had led management to think that things were well as they were and the need for changes was not recognized. Overconfidence and excessive optimism also blinded the management from seeing the need for change.

Once the situation had been analysed, the change project was started. Cultural change was key, and before all big change proposals, it was mandatory to list what de-biasing techniques had been applied when preparing the decision proposal. In the decision-making process a devil's advocate was involved, the role being to present doubt and arguments against the proposed course of action. Naturally, key persons were trained to use the de-biasing techniques.

The debiasing change was a success, and management example and participation was a key success factor.

6. Summary

Cognitive biases are errors of human judgement which impact human activities, including security management. The psychological mechanisms forming the basis of these thinking errors have been studied by several scientists. Debiasing techniques which limit the impact of biases have been developed and successfully applied.

However, there is not much information available on the appearing and impact of cognitive biases on security management. As consequence, also the debiasing techniques which would best suit to decrease the impact of biases is missing. Though *security by obscurity* is not considered to be a valid security management approach, to be efficient in preventing harmful events details of control implementations and investigation methods are not exposed to the entire organization. This makes it more difficult to detect the presence of cognitive biases in security management processes, and as consequence also debiasing techniques are not applied.

Security management is activity which impacts the entire organization by restricting risky actions or by acting as an enabler of business opportunities. Having more information about the impact of biases and suitable debiasing methods could significantly improve the quality of security management. This knowledge could also help to develop better and more efficient security frameworks and procedures.

References

Alleydog (2023) Cognitive Bias definition | Psychology Glossary | AlleyDog.com
Chabris, C., Simons, D. (2009) The Invisible Gorilla, Broadway Paperbacks, New York
EDRI (2005) https://edri.org/our-work/edrigramnumber3-11snooping/
EK – Confederation of Finnish Industries (2023) *https://ek.fi/hyotytietoa-yrityksille/yritysturvallisuus/* (February 28th, 2023) http://eprints.cs.univie.ac.at/5258/1/calero-valdez2017framework.pdf
Günther, B., Heiligtag, S:, Webb, A., A case study in combating bias, McKinsey Quarterly
Harris, R (2022) The Confidence Gap, Robinson, London
Iresearchnet psychology website (2023) https://psychology.iresearchnet.com/social-psychology/social-influence/debiasing/ (February 28th, 2023)
Kahneman, D. (2012) Thinking, Fast and Slow, Penguin Books, London
Kannengiesser, U., Gero, J.S. (2019) Design thinking, fast and slow: A framework for Kahneman's dual-system theory in design, Design science, Cambridge
Morewedge, C.K. et al (2015), Debiasing Decisions: Improved Decision Making With a Single Training Intervention, Questrom School of Business at Boston University
OECD (2023) Neuromyth 4 – we only use 10% of our brain, OECD
Rzepczynski, M (2023) https://www.blogger.com/profile/13692706752978475626
Saariluoma, P:, Maartola, I:, Niemi, P. (2000) Ajattelurskit ja kognitiiviset prosessit taloudellisessa toiminnassa - Thinking risks and cognitive processes in economic activity, Tekes, Helsinki
Smith, C.L., Brooks, D.J (2013) Security Science – The Theory and Practice of Security, Elsevier, Amsterdam
Soll, S., Milkman, C., Payne, J.W. (2015) A User's Guide to Debiasing, Wiley
Valdez, A.C. et al (2017) A Framework for Studying Biases in Visualization Research, http://eprints.cs.univie.ac.at/5258/1/calero-valdez2017framework.pdf (February 28th, 2023)