Valéria Csépe

The Psychological Dimensions of Subjective Security

Valéria Csépe, correspondent member of the Hungarian Academy of Sciences, Professor of the Budapest University of Technology and Economics; Research Professor at the Brain Imaging Centre of the Research Centre of Natural Sciences of the Hungarian Academy of Sciences

Abstract

This chapter focuses on the psychological dimensions of the societal factors of security that cannot entirely be explained by the classical information processing theories. The primary reason for that is the significant change seen in the 21st century in the individuals' place in the local and global social space. Technology, developing more rapidly than the human cognitive evolution, has modified the territories and methods of the individual, the societal space and empowerment, as well as the ways freedom and power are exercised. The so-called knowledge-based society requires new skills in an era when the decades-long stability of knowledge is cracking and new skills evolved that can hardly put under conscious control.

The personal, or subjective, security dimension, therefore, plays an important role in understanding the detachment of environmental challenges and cognitive developmental scale including the separation of attention, memory, learning ability and emotional processing. In this approach, the newest data of neuroscience provide a new insight into the effects of the global web on individuals and on the processing variations associated with the advent of virtual spaces. This chapter describes those security issues which play a significant role in the individuals' perception of threats and risks. To illustrate this from the aspect of the biologically, psychologically and socially determined individual, I shall outline the conflict areas of objective and subjective safety typical for the 21st century to discuss those already well-identifiable changes which must gain increasing importance in defining security and safety.

Keywords: globalization, information processing, digital word, knowledge society, threat perception, risk evaluation, cyber-crime, cognitive and affective components, subjective evaluation, vulnerability, threat-insensitivity

Introduction

The notion of security has changed a lot over the centuries. At the beginning, the conception aimed at understanding mainly the actions within objective security. Though the classic security policy distinguished between the objective and the subjective security already in the sixties, it came to the fore in its true depth and diversity only in the past decade. Although this study is not aimed at providing a historical overview, it should be mentioned in respect to subjective security that its themes have been noted in the foundation of security policy for decades now. Most experts agree that the breakthrough of a significant conceptual renewal of the security issue happened at the end of the Cold War; and the further development of this notion is affected by strong compelling forces today. The security policy discussions of the 1990's brought forward for the first time the new approach, being also new in philosophic aspects, that took the dual models of prevention and compensation as a basis in the solution schemes of dangers originating from basically social and technological uncertainty.

The lack of social and technological security is becoming a serious risk factor in the 21st century, but one of the main problems related to the knowledgeable management of this risk is that it cannot be classified as a risk solvable by law enforcement or political means. Globalization and digital revolution bring different changes with regard to subjective security. Becoming aware of the negative events associated with globalization has led to the weakening of the sense of security in the past years. The perception of specific threats has been complemented by an anticipation of abstract dangers at a high degree which have various psychological aspects, and demand skills different from handling of traditional security issues. The expansion of the digital world does not have a satisfactory impact on the individual behaviour, so that the subjective sense of security is unreasonably good – in spite of the fact that the dimensions of the digital world's expansion are the same as of other fields of globalization, and are serious factors in security policy. The low level of threat perception of individuals does not or does only hardly change the perception of the risk associated with digital globalization, does not influence the subjective security; even if it may be considered as a serious objective security risk. These are two opposite processes, and their factors and causes should be urgently and deeply explored. It may be surprising that the general phenomena of globalization reduce the subjective sense of security, while the effects of digital risks, which also have globalization-related phenomena, are not significant. The unreal sense of security and the underestimation of hazards endanger many population groups, but mainly the teenagers, who ever more widely and often use the smart devices of our age. Another, separate question is whether the today's generation of teenagers uses these devices at a high level, and whether the proper skills required by these devices are supplemented by conscious application; and whether this development, overestimated by some scientists, have measurable indicators.

The conception of security is different from the conception of even a decade ago; as – instead of defense against a concrete threat or danger – we expect security policy that can get prepared for risks appearing at a higher and more abstract level. This means that *we treat security as a social value, a generally applicable normative criterion.* So, today (at least in the western-type democracies), security is a political value without any independent meanings interpretable in itself, i.e. it is connected to the values of the individuals and the society. This connection also makes clear that modern security policy, taking many

aspects of security into consideration, shall be created, which can interpret and implement the (historical, cultural, religious, social, etc.) processes of the society and the factors that influence the individuals' subjective sense of security.

In the definition of dangers, mainly the threats and the challenging risks appear (frequently as synonyms) in the concept of vulnerability threatening security which is used widely and with various meanings. The first point of the concrete assessment will deal with psychological aspects of vulnerability. At the same time, we should note that the definition of vulnerability and the management of the resulting risks has a great importance both in security policy- and special policy aspects, due to the individual- and social-level determination. Two characteristic issues of these will be highlighted, which have been significantly changing in the past years, and have different intensities regarding the subjective sense of security and risks on the level of the individual. One is the negative effect of globalization on general subjective security, which is – in the absence of appropriate informedness – anxiety-increasing; and the other is the unreasonably high threshold of the perception of subjective security during the everyday use of Internet and smart devices. This is why greater emphasis is put on these new risk factors, in the perspective of security.

Globalization, information technology, knowledge society

Globalization is a multidimensional phenomenon, and there are certain areas in it where the understanding of processes necessitates deep know-how covering several areas of knowledge. The integration of the know-how attained in the different specific fields would be important for security policy considerations that are opposite to strong specialization, as well as for the topic of this study: the subjective security. It seems that the experts are hardly willing to undertake that, which may result from the fact that the methodology of this – quickly developing but still very young – scientific field, which has the task of revealing the human behaviour that indicates the changes and the psychological dimensions of subjective security, is incomplete.

In the past years, the every-day appearing of changes related to globalization, the perception of risks and threats, and the understanding that global and local phenomena go together have been linked with crises (economic, financial, and political), disasters (industrial, natural, hybrid – that is industrial disasters resulting from extreme natural phenomena), local wars, revolutions, cross-border terrorism. Today, several of the more complex phenomena of globalization (economy, climate, environment, etc.) are perceivable on the level of individuals; and – even if there is no deep knowledge – also the concrete (extreme weather) and the abstract (environment and sustainability) sense of danger is increasing. The largest negative shifting in individual security perception – i.e. in the subjective assessment of threats and risks – or, in other words, the diminishing of subjective security are mainly linked with the concrete facts of globalization: over-population, the shrinking of natural resources, the new migration that has started due to wars and unhuman living conditions, and dangers which are known but hidden from our perception (food- and water scarcity, etc.), international crime, and terrorism. Info-communication devices carry tragedies, terror, and environmental threats into our homes and through this into our everyday life;

and the negative occurrences, being almost the only ones that have newsworthiness, spoil subjective security through psychological factors like distress, fear, pessimism, and apathy.

While one of the communication means of the flood of threatening information is the digital world, the subjective perception of the dangers of its use has hardly changed at all. Private persons, and sometimes even political leaders handle their digital devices in a negligent way and fail to protect them from uninitiated peepers or those searching for information with hostile purposes. Thus, we may be surprised that our subjective sense of security related to globalization is significantly decreasing, but it does not change with regard to the use of the digital world. The crises and disasters of the world are not or not yet shocking enough to individuals, and our individual sensibility regarding data security has not yet developed enough. This has several various causes, which will be discussed later. Information technologies (IT) develop quickly and in a wide range, and the circle of the "smartly networked" (by which I refer to *"smart"* devices, and not necessarily the users and the method of use) – similarly to other global (economic, politic) networks – is growing quickly. In the global web, usage has theoretically no limits. The minimum education requirements for everyday use of user-friendly systems (mainly the Internet and the social media) are very low; real knowledge, or a low level of ethical and moral development are not impede presence, the mixing of opinions and facts, or the propagation of ideologies or even fallacies. The false, bad, intolerant, inciting world has appeared also on the Internet – which should serve the free flood of information and opinions, and the correspondence among communities – and, within the expanding web, in the social media. Terror, violence, fraud are communicated ever more frequently on the Internet, and a new branch of crime, the so-called cyber (or Internet) crime has also appeared.

The Internet and our smart devices are not the causes but the possibilities of crime and cyber terror. This tool uses the newest psychological methodology, relies on visualizing personal characteristics, ideological opinion, identity, thinking, and attitude; and the behavioural manifestations of these may pose a threat. Personal qualities become visible just like the qualities of a driver in special or in everyday situations. But the number of people endangered by drivers speeding in the exit lanes of highways is only a fraction of the number of those being influenced, oppressed, or destroyed by the activities of those who rampage on the Internet, offenders, criminals, terrorists or the hackers working for the above, who are often anonym, hardly (or not) identifiable.

The actions we do on the web influence us: they change our information processing, habits, method of correspondence, behaviour; and what is more, if we use the online space in an extreme way (addiction), that will affect even the structure and function of our brain. The specializing branches of psychology – the profession that examines human behaviour and has a dual (helping and scientifically revealing) purpose – have dealt ever more with the effects of new technologies; and the new disciplines, the cyber psychology and even the cyber psychology of criminal behaviour are trying to reveal the human-related features and causes of the phenomena regularly observed in our days. According to a common view in cyber psychology, the Internet space (here as a global, multilayered web), or the cyber space is not only a transaction medium, not the intermediator of passive TV watching of telephoning. This medium, as formulated by Mary Aiken in the book: *The Cyber Effect* (2016), a work considered as standard reference about cyber psychology and psychology of Internet-based crime: "It is a highly interactive, highly engaging, and highly immersive

environment—uniquely compelling and attractive to humans" (Aiken, 2016: 11.). Indeed, the Internet space is full of place names, real and unreal people, and there are billions of people online.

But the world of Internet hides a number of serious evolutionary traps. Evolution has not prepared humans for faceless presence and communication. Our instincts work relatively well in face-to-face interactions, but when we are in the Internet space, these instincts let us down. Our obstruction is clear but our perception is not. According to the current psychological definition, perception is: the result of a calculation (brain process) based on the sensing of current actions, using also our knowledge and former experience for the assessment. We could illustrate this by a situation where you have a car key but you cannot drive. In the world of Internet, our evolutionary behaviour set does not work or works improperly. Moreover, this world is both a real and an unreal multi-dimensional space at the same time. Cognitive sciences identify Internet as a kind of space where we can find a lot more variations of human behaviour than what we have experienced before: from vulnerable people to criminals, from helpers to people with killing intentions. Thus, during our online encounters, we find the best and the darkest side of human behaviour, and we do not yet fully understand how the Internet world serving the normal population's needs affects the abnormal, deviant, criminal, or vulnerable groups. *This is why the Internet security policy shall presume that the false sense of subjective security* (and the factors besides evolutionary unpreparedness will be mentioned later) *is underestimated at the moment*. That is why the understanding of psychological components would have significant benefits in the estimation of threats and risks; and, together with the objective factors of security, it may result in a more complete preparation.

Information processing and emotions

The past two decades of brain research, basically transforming our knowledge regarding the relations of perception and affective and cognitive processes, had two significant outcomes that affect also the subjective security. Firstly: information processing is the result of not an intended cognitive process but an unintended neural process. Our brain is able to process about 10 millions of information units per second, whereas only 40 units are processed intentionally. The processing of the rest happens through unintended brain processes. Secondly: emotions play a primary and dominant role in perception and thinking. That is why the results of emotion research have an ever growing effect on the wide-range analysis of the above-mentioned global issues: nuclear proliferation (Hymans, 2006), combatting of terrorism (Saurette, 2006; Crawford, 2009), retaliation as an answer to threats, war motivation (Lebow, 2010).

To understand the effects of the emotional reactions influencing security and the rational answers to be given to risks, we should first make clear what is an emotion. This question is subject to a wide range of debates even today. These are not going to be discussed here, but here is a quotation of a definition well picturing the scope and complexity of emotions: "emotion is a combination of components, made up by biologically determined (physiological and psychological), and physical and socio-cultural systems, and defined through transformative interactions" (McDermott, 2004: 692.). At the same time, we

should note that emotion is a collective term, and within that, feeling, moods, and passion are related to very much different ontological and metaphysical principles. Emotion is made of physiological changes and these becoming awareness. For example, the physiological changes (quick heart rate, sweating) accompany fear even before we would know that we have fear and what made us feel like that. In general, we feel before we would think, and – surprisingly – we act before we would think. Most brain researchers agree that our brain uses automatic processes that are quicker than the conscious, deliberate processes, but the brain interprets these automatic, quick responses as conscious and deliberate.

Psychologists and neuroscientists often use the dual process- and two-factor theories based on the idea that our behaviour is controlled by two systems made up by processes having separate and different accesses and speeds (MacDonald, 2008). One is implicit, automatic, fast, early developed, parallel, effortless, non-reflexive, and high-capacity; while the other is explicit, slow, late developed, sequential, with limited attentional and memory resources, needing efforts. Both psychological and neuroscientific researches suggest that our brain has two separate operative systems: one emotional and one thinking-reasoning systems. Kahnemann (2011) calls the emotion-determined system intuitive and associative, and the other one reasoning, rule-driven. The first processing method, mainly relying on emotional processing strongly influences our responses, and the second – of the two rivaling methods –can hardly "teach" the first one. The emotional processing system can give quick responses to environmental effects, and this effective response – developed during the evolution – facilitates the immediate perceiving of being threatened.

The question is how the two changes being opposite to each other regarding subjective security (concrete versus digital globalization phenomena) influence our decisions in their complex environments. This is important both on the level of the individual and the decision-makers responsible for security. In emotionally stressful situations, danger detection often leads to wrong identification of endangering factors and objects. Under the influence of strong emotional reactions, the overestimation of the danger is significantly higher than its underestimation (Bauman–DeSteno, 2010). Of course, the main question of policy and social psychology goes beyond the evolution-related reasoning. What is the social context in which emotions have a real meaning? What is the common element that influences the decision of the individual, a group, a nation, or a government? What components do we consider threats, going beyond subjective security? We know that the components are varied, and embedded both socially and culturally. Nevertheless, the strongest driving force is fear. More deeply analyzing how the various science branches define fear would not be worth herein. But we should note that, according to neuroscientific research, fear can not only be conditioned, but can also be permanent or last longer than any other learned (conditioned) relations. This is why there might be a contradiction between objective risk and the factors causing fear, and this might be so great that it causes the overestimation of the risk and the significant decrease of the sense of subjective security. That is why fear may last a lot longer than the threat, and may be embedded in the behaviour of individuals and groups as a long-lasting learned response.

However, on the level of the individual, the factors to be considered in the assessment of threatening occurrences differently influence the subjective sense of security. This is illustrated by the model jointly dealing with threat and the possibility of becoming a victim, presented by Table 1. In the interpretation of the model, we must take into account that,

on the basis of the measured empiric data, the definition of subjective security is far not as clear as the table shows. In the light of the measured data, the subjective experiencing of being threatened, the evaluation of the possibility of becoming a victim may be better understood in two dimensions, on the basis of cognitive and affective components. The perception of subjective security is based on three important, potentially relevant pieces of information, accessible on the level of the individual (Jackson, 2005; 2006). These are (1) a possible event affecting security, the risk of involvement/becoming a victim ("What can happen to me?"), (2) physical, material, and mental consequences ("What effect will that have on me?"), (3) the concrete probability of involvement/becoming a victim ("What are the chances that it will affect me?"). In this regard, as I cannot emphasize enough in this study, both the cognitive and affective aspects influence the subjective perception of security.

Besides the subjective evaluation of all these aspects, we can also practically define an objective risk, which might be considered real, even though it cannot be presented in a breakdown to endangered populations.

Table 1

Possible variations of the concept of subjective security

	0% … Cognitive components of subjective evaluation … 100% objective evaluation				
	100% … Affective components of subjective evaluation … 0% subjective evaluation				
Possible event	N	Y	Y	Y	
Implications	N	N	Y	Y	
Likelihood					
Psychological condition	Distress	Uncertainty	Uncertainty and worrying	Subjective risk perception	Objective individual risk
	Anticipating	Anticipating	Anticipated	Anticipated	
Security-relevant denomination (criminology)	Loss of security	Fear	Subjective probability of becoming a victim		
Possible indicators	Physiological indicators	Questionnaires (psychological tests)	Specific questionnaires	These indicators are usually not included in the security statistics	

N: factor ignored by the individual; I: factor taken into consideration by the individual

Source: Jackson, 2005

The consequences of continuous loss of security are serious, may last for a long time, and lead to the condition of permanent feeling of threat. The cognitive and affective aspects considerable on the level of the individual are manifested in the anticipation of fear. This is further strengthened by the learned fear response, and may lead to events with extreme consequences (see the terror attack against the New York Twin Towers 11 September 2001). This extreme loss of security amplifies threat perception, and the threat-intensive condition may last for years, or even longer than a decade. The threat can of course be institutionalized, turned into program of governments, and the mass diminishing of subjective sense of security may generate conflicts. That is why emotional processes must not be ignored neither in the evaluation of subjective security, nor in the estimation of risks. Moreover, emotions play a role also in the assessment of reliability, since they influence the two main factor of that: the interpretation of evidences and the evaluation of risks (Mercer, 2010).

In summary we can conclude that emotion is an assimilation mechanism that influences the choice and the interpretation of threat perception. This is why we should not ignore emotional components when we determine the individual's subjective sense of security. The interaction of rationality, cognitive heuristics, emotional states, and the political- and institutional context shall be incorporated in these strategies.

Vulnerability and risk

The notion of vulnerability – in the context of security – is mostly mixed with the expressions: *threat* and *risk*. Vulnerability means roughly the same related to both humans and things (e.g. an information technology system), and its level determines the likelihood of being attacked. The notion of danger is also linked to this. Everything that deliberately or accidentally takes over, causes damage, or destroys – using vulnerability – is a danger. This is true regarding the individual's physical and subjective reality and also regarding objects. Objects are meant in a wide sense here, from software to concrete objects. So, whether related to a person, an object, or a system, vulnerability is the weak point of any efforts for security. Risk is the root of these two, so it can be assessed on the basis of the determination of vulnerability and the evaluation of danger. In general, low vulnerability also means low risk. But we should overview in short what risks the individual's vulnerability means.

Psychological vulnerability is inherent in human life, but its level can be quite various. According to the relevant research, an elevated level may lead to serious psychological problems, because a higher level of psychological vulnerability goes hand in hand with the dominance of negative emotions and depression symptoms. On the other hand, a low level of psychological vulnerability shows a close correlation with satisfaction, dispositional optimism, and self-efficiency (Sinclair–Wallston, 1999). Furthermore, several studies have shown that the level of spiritual vulnerability and that of conformation are correlated, and this influences subjective welfare, satisfaction, and subjective security, including societal security (Satici et al., 2016; Uysal, 2015). So, spiritual vulnerability is a part of the subjective security which – as a personal quality – influences the individual assessment of objective security.

However, vulnerability can be defined not only as an inherent personal quality but also as a consequential – i.e. changing due to environmental impact and through experi-

ence – individual quality. The digital revolution is accompanied by negative consequences> most of the web-users – including those who are highly psychologically vulnerable – do not care about the security of their private sphere, carrying risks that may go far beyond the individual's security leading to business-related or even to national security risks. Today it is self-evident that many human activities – e.g. correspondence, social interactions, entertainment, shopping, search for information – are carried out online, and their medium is the segments of the digital world which have varying security controls.

Danger insensitivity of individuals

Activities on the Internet have a trace, an undeletable trace. The indicators accessible on the surface can be easily captured, and analyzed through intelligent computer algorithms, using the knowledge of various disciplines having a deep knowledge abouthuman behaviour. The positive usage of these data sources is related to social science, the services aiming at providing a better service for customers, and also targeted online marketing. By use of well-developed computer programs made for tailored search engines and recommendation systems traceable on the Internet, one can have an insight into the users' plans, wishes, attitude, and even religion and political preferences, or extreme behavioural deviances. The good cause, i.e. to serve the customer, the citizen, is based on the data capturing the individuals' behavioural patterns. This poses a serious challenge regarding privacy and the integrity of private life – even by itself, without a negative will of the data collector. The (Internet-) psychological examinations of the past years have shown that personal qualities, even characteristics we consider as only ours and private can be easily learned through so-called digital behaviour data that seem to be harmless. Getting to know the person's individual- and the groups' common characteristics, intentions, values, attitude itself means "only" the damage of privacy; but in a fierce social-political situation, it may cause serious risks and should be taken into consideration even in security policy aspects. An American study published a few years ago (Kosinski et al., 2013) reported about the results of a survey on the reliability of findings related to several qualities, on the basis of information about almost 60 thousand volunteers. The profile information available in the myPersonality Facebook applications (www.mypersonality.org/wiki), likes (an average of 170/person) were compared with the results of a psychometric test and a questionnaire. The results are not reassuring either regarding the protection of privacy nor security. Merely using the Facebook "like" data, you can find out by 80-90% accuracy personal characteristics such as sexual orientation, intelligence, religious tolerance, xenophobia, emotional lability, aggression.

In terms of security, we can conclude that the identification of vulnerability based on personal characteristics may pose serious risks with regard to the choice of target persons in case of a planned (business, political, etc.) attack. The risk of any kinds of danger may be increased by the identification of the patterns of vulnerability, which is applicable to persons and groups who may become emotionally instable, behave neurotically, be influenceable, or easy to win over to foreign and dangerous ideologies. The digital footprint of Facebook posts can be profiled (similarly to *profiler* activities used in the crime investigations) in psychological aspects, and it is not only a telltale but also a security risk. A huge amount of private data is available, there are no limits to classification and profiling, there

are hardly any digital limitations, and you do not even need the person's agreement for using the information available on the Internet – unlike other kinds of data mining. The user often does not wish to share these data with others, but the conclusions that can be drawn from them may have security risks (for welfare, freedom, life). The analysis of the digital footprint left by individuals and groups – having psychological knowledge and the right mathematical algorithms – facilitates the identification of the main factors of vulnerability. The societies including people who are at a high level of digital development but not yet mature in relation to human behaviour and not prepared for defense should stand up to the real security challenge.

Aspects of threat perception

Danger can be interpreted by itself, primarily because it is mediated by the object, person, or event which carries the danger. Perception is the processing of the dangers felt, resulting in the identification and interpretation of what we have processed. According to classical psychology, perception is a uniform and conscious process that arises from processing by sensors, and is linked to the presence of stimuli. Perception is the basis of understanding, learning, knowledge, and the motivations leading to actions. However, individual perception is not exclusively determined by sensor information, but also by emotional state, information processing, reasoning, and the pattern of meaning-attribution. But on the group level, the identification of perception – including the perception of dangers – is usually difficult. The interpretation and communication of perception is similar to that of emotions, that is why we find its results in the collective moods. In this regard, danger is the social construction which is created through personal talks, the public information given by experts and political leaders, and the communication by communities (Meyer, 2009).

Threat perception has many aspects. In security regard, we usually take the non-psychologic factors into account. If psychological factors are not known, it is difficult to understand the false perception of danger on all levels, whether individual, common, or political. This paper aims at giving psychological explanations for threat perception. In the analysis of the components of false perception, we collate the perception preceding actions *(ex ante)*, with the real behaviour after the actions *(ex post)*. In the standard information processing models, the estimation of false perception as a process is based on the degree of deviation from a rational decision. The question is what shall be considered standard; and how flexible the boundaries are. That is, whether the response to threat perception pursues rational or optimal information search. The starting point of the notion of false perception and false calculation lies in the assumption that there is accurate perception and calculation, and there are standards and boundaries in order to reliably separate them. Unfortunately, these boundaries are difficult to determine, even after the response to threat perception has been given. It would be especially difficult to give an accurate explanation for political-level conflicts. Regarding decisions following obviously false threat perceptions, historians try to find the intention only years later, in possession of all documents. There are many co-existing explanations for why many people – usually those who are in leader positions (business, political, etc.) – communicate false information about their own skills

and intentions. This question would be difficult to answer, that is why psychology dealing with threat perception studies the possible patterns, rather than the accuracy of perception.

Intention and ability

The intention and the ability are the two central elements of danger, threat. Their definition includes many contradictions, in spite of the fact that both are decisive factors in models estimating the degree of threat, as well as in strategies focusing on rational deterrence and the danger perception. One of the causes of this is that although the intention is manifested in purposive behaviour, the psychological researches show that people do not realize the preferences; and one of the basic characteristics of these preference is instability (Kahneman–Tversky, 1979; 2000). The most difficult thing is to estimate complex human behaviour, as we have no concrete, tangible information about that. Such are: morale, motivation, loyalty, and leadership abilities. A separate branch of cognitive psychology deals with the cognitive distortion influencing the patterns of danger perception, first and foremost in order to reveal and analyze the factors appearing in the patterns of danger perception. And a separate research branch deals with the danger perception distortions which cannot be or can only hardly be explained on the basis of rational information processing models.

The "cognitive revolution" – which can be considered a rebellion of psychologists – four decades ago broke away from the simplified explanations of human behaviour. The mind – together with the research about human intents, conclusions, and judgments – was brought back into psychology. The real problem regarding the new, rational models of the popular information processing was that behaviour in real situations could not or could only falsely be determined on the basis of these. Why is that important regarding security? Among others because the perception of danger and threat is influenced by a number of psychological processes, including cognitive processes. Regarding the nature of decisions made in danger situations, we should take into consideration the fact that human cognition is not very good at the estimation of likelihood. We should not forget either, that the response of a bigger social group or a country to a danger is the joint decision of political decision-makers and the security policy, but every participant's information processing capacity is limited, and rationality can prevail only conditionally. As rationality is limited, the reduction of the complexity and uncertainty of the situation may distort danger perception and evaluation, as a result of the quick cognitive estimation of the information. This shortened cognitive process can explain relatively well the false danger perception. A number of psychological studies confirm that human behaviour rarely meet the expectations based on the abstract rational models (Kahneman et al., 1982; Kahneman, 2011; Hastie–Dawes, 2001; Gilovich et al., 2002). The results of cognitive psychological examinations show that decisions made by people are mostly based on estimates and on the ascribing of intentions, instead of using rational models. That is why the demand for easily deductible conclusions significantly increases when processing uncertain, complex environmental information. The source of the cognitive distortion – in complex situations – should be searched for in human thinking; and these are the following: preference for simplicity, aversion from uncertainty and dissonance, and elementary misunderstanding of the essence of likelihood (Tetlock, 2005). Most people have very bad likelihood estimation abilities, which – together with the other

factors – strongly limit the chance of rational decisions. This is particularly noteworthy if we take into consideration also the fact that tall the aspects listed above are only cognitive factors of danger and threat perception – and these factors are influenced by emotional processes, as well as the individual's and the community's long-lasting, learned fears. That is why subjective security can be hardly judged without the knowledge of modern psychology – which in turn often calls neuroscience for help in understanding issues, due to the complexity of behaviour. This statement points far away. It is namely about the fact that there will not be well-implementable security without taking into account the perception of subjective security and the effects of emotional and cognitive factors, nor without the understanding of the opposite processes derivable from globalization phenomena. As a result, some of the results of psychological researches that reveal decisive factors of subjective security have become non-public information, and are becoming a security policy issue.

References

Aiken, Mary (2016): *The Cyber Effect*. John Murray, London.

Baumann, Jolie – DeSteno, David (2010): Emotion guided threat detection: Expecting guns where there are none. *Journal of personality and social psychology,* Vol. 99, No. 4. 595–610.

Crawford, Neta (2009): Human nature and world politics. *International relations,* Vol. 23, No. 2. 271–288.

Gilovich, Thomas – Griffin, Dale – Kahneman, Daniel (eds.) (2002): *Heuristics and biases: The psychology of intuitive judgment*. Cambridge, Cambridge University Press.

Hastie, Reid – Dawes, Robyn M. (2001): *Rational choice in an uncertain world: The psychology of judgment and decision making.* Sage, Thousand Oaks.

Hymans, Jacques E. C. (2006): *The psychology of nuclear proliferation: Identity, emotions, and foreign policy.* Cambridge University Press, Cambridge.

Jackson, Jonathan (2005): Validating New Measures of the Fear of Crime. *International Journal of Social Research Methodology,* Vol. 8, No. 4. 297–315.

Jackson, Jonathan (2006): Introducing Fear of Crime to Risk Research. *Risk Analysis,* Vol. 26, No. 1. 253–264.

Kahneman, Daniel (2011): *Thinking, Fast and Slow.* Farrar, Strauss and Giroux, New York.

Kahneman, Daniel – Slovic, Paul – Tversky, Amos (eds.) (1982): *Judgement under uncertainty: Heuristics and biases.* Cambridge University Press, Cambridge.

Kahneman, Daniel – Tversky, Amos (1979): Prospect theory: An analysis of decision under risk. *Econometrica,* Vol. 47, No. 2. 263–291.

Kahneman, David – Tversky, Amos (eds.) (2000): *Choices, values and frames*. Cambridge University Press – Russell Sage Foundation, Cambridge.

Kosinski, Michal – Stillwell, David – Graepel, Thore (2013): Private traits and attributes are predictable from digital records of human behaviour. *Proceedings of the National Academy of Sciences,* Vol. 110, No. 5. 5802–5805.

Lebow, Richard Ned (2010): *Why nations fight: Past and future motives for war.* Cambridge University Press, Cambridge.

MacDonald, Kevin (2008): Effortful control, explicit processing, and the regulation of human evolved predispositions. *Psychological Review,* Vol. 115, No. 4. 1012–1031.

Makropoulos, Michael (1995): Sicherheit. *Historisches Wörterbuch der Philosophie,* Ritter, Joachim – Gründer, Karlfried et al. (eds.), Wissenschaftliche Buchgesellschaft, Darmstadt, 745–750.

McDermott, Rose (2004): The feeling of rationality: The meaning of neuroscientific advances for political science. *Perspectives on politics,* Vol. 2, No. 4. 691–706.

Satici, Seydi Ahmet – Uysal, Recep – Yilmaz, M. Fatih – Deniz, M. Engin (2016): Social safeness and psychological vulnerability in Turkish youth: The mediating role of life satisfaction. *Current Psychology,* Vol. 35, No. 1. 22–28.

Saurette, Paul (2006): You dissin me? Humiliation and post 9/11 global politics. *Review of International Studies,* Vol. 32, No. 3. 495–522.

Sinclair, Vaughn G. – Wallston, Kenneth A. (1999): The development and validation of the Psychological Vulnerability Scale. *Cognitive Therapy and Research,* Vol. 23, No. 2. 119–129.

Tetlock, Philip E. (2005): *Expert political judgment: How good is it? How can we know?* Princeton University Press, Princeton.

Uysal, Recep (2015): Social competence and psychological vulnerability: The mediating role of flourishing. *Psychological Reports,* Vol. 117, No. 2. 554–565.

Zubin, Joseph, Spring, Bonnie (1977): Vulnerability: A new view of schizophrenia. *Journal of Abnormal Psychology,* Vol. 86, No. 2. 103–126.