ROCZNIKI NAUK SPOŁECZNYCH
Tom 13(49), numer 2 – 2021
DOI: https://doi.org/10.18290/rns21492.2

DARIA KRZEWNIAK

SELECTED ELEMENTS OF THE INTERNET USERS' INFORMATION SECURITY CULTURE

INTRODUCTION

The constantly developing information and communication technologies play a significant role in the modern people's lives. They have also become inherent attributes of the modern reality. They contribute to the progress of the science-based society and help to level up social inequalities and introduce social integration and inclusion.

The Internet, which has settled in the contemporary people's every-day functioning for good, appears an important element of the information and communication technologies. Almost every mobile device is developed with the online services in mind. The easy and relatively cheap Internet access influences the range and frequency of the web resources. It also changes the individual and social behaviour patterns. The mobile connection to the Internet means that not one but multiple ways of being online can be established. They are mixed with other cyberspace activities. The borders between being on- and offline got blurred. The transfer of the virtual behaviours into the real world is observed ever more frequently. Most importantly, it applies to the problematic behaviours of the youngest Internet users; hence, the reality broadening occurs.

The so-far experiences lead to the conclusion a substantial number of the cyberspace activities contradicts the socially desired norms and values and affects the Internauts' security level, the web messages' senders and recipients alike. Furthermore, the long-term culture of security research (Cieślarczyk, 2006; Filipek, 2016; Sadłowska-Wrzesińska, 2018) has concluded that—among

DARIA KRZEWNIAK, PhD—Siedlce University of Natural Sciences and Humanities, Faculty of Social Sciences, Institute of the Sciences of Security; address for correspondence: ul. Żytnia 39, 08-110 Siedlce; e-mail: daria.krzewniak@uph.edu.pl; ORCID: https://orcid.org/0000-0003-1085-8361.

others—the level and character of the culture of security influences undertaking or giving up the activities endangering an individual, other people and their surroundings. That psycho-social phenomenon indicates—to a large extent—how people perform their web activities, what values and norms are presented through the Internauts' cyberspace attitudes, behaviours and activities (co-activities) (Batorowska, 2015). There emerges an assumption the activities demonstrated by the Internet users are related to the level and nature of the information security culture.

The analysis of the respective elements of the Internauts' information security culture proves that—aside the positive trends appearing in the web —harmful, pathological and destructive contents appear ever more commonly and intensely. Their impact and possibility to shape the further, unwelcome attitudes and behaviours is far more powerful than in the case of the positive contents. Still, in the debates on the Internet security, the role (significance) of the information security culture seems underestimated. Consequently, the society remains unprepared for the challenges, occurrences and handling the cyberspace hazards.

Yet, the information security culture is a variable possible to upgrade through education. The education developing particular cultural elements appears a vital need of the modern, democratic societies aspiring to shape the skills of safe web navigation, critical and selective reception of the Internet contents and engaging themselves in the social trust, openness and wisdom spreading. The aim of the article is to analyse the Internet users' information security culture elements and pointing at the possibilities to popularise them among the society. In relation to that objective, the following research problems were formulated:

1. What level and nature of information security culture are manifest by Internet users?

2. What is the relationship between the information security culture of Internet users' and their online activity?

3. What are the possibilities of improving the information security culture of Internet users?

In response to research problems, hypotheses were formulated, assuming that:

1. Internet users represent verying levels and nature of the information security culture;

2. There is a close relationship between the information security culture of Internet users and their online activity. Individual with a high level of information security culture profess socially recognized values and norms, and

their online behaviour and actions are an expression of concern for their own and others' safety;

3. The information security culture of Internet users can be improved in the process of education at all levels, involving various environments in which people function—starting from the family, through school, peer group, professional environment, up to the impact on the national and international level. These activities must be multi-level and multi-dimensional.

To solve the research problems and verify the hypotheses the method of literature analysis and available statistical data as well as the method of synthesis were used.

1. SECURITY CULTURE: THEORETICAL ASPECTS

As a psycho-social phenomenon, the security culture has recently been attracting more and more attention. Its numerous connections with a range of everyday life aspects is generally acknowledged (Cieślarczyk, 2006; Filipek, 2016). Both the theoretical analyses and empirical research prove people of the higher level of the security culture comprehend the matters of their own, the others' and their surroundings' security better. Additionally, they adapt to the occurring changes faster, have well-developed recognition skills, necessary for effective anticipation, and undertake challenges swifter. Such individuals make better use of the opportunities and deal with various difficulties and threats more efficaciously than others.

An individual's security culture's essence rests on the level of their knowledge and the attitude toward security, their reception of security and on their reactions to the lack of it. It can be assumed the people who perceive security in a narrow-minded, negative way and treat it exclusively because of the absence of threat feature a low level of the security culture. Their behaviours and—less commonly—actions (co-actions) focus on the protection against dangers and on limiting or, ideally, avoiding risks.

Conversely, those attracted to the broad, positive thinking about security feature a higher level of the security culture. Their actions and co-actions—less commonly behaviours—are directed towards securing themselves against various dangers; still, primarily, they focus on noticing and proper interpretation of the challenges. As a result, they treat threats from the perspectives of an individual and social progress.

In a broader sense, the security culture is

> […] a pattern of the basic assumptions, norms, rules symbols and convictions which influence the subject's perception of challenges, opportunities and/or hazards in the closer and more distant surroundings. It also influences how one perceives danger and how one thinks about it. It also impacts the thinking-related behaviours and actions (co-actions), variously mastered and articulated by the subject in broadly understood education, natural processes of internal integration and external adaptation. It also refers to strengthening the defence (not exclusively in the military context)—maintaining a relatively harmonious development of the subject and their achieving the, most broadly understood, security for the benefit of the subject and their surroundings (Cieślarczyk et al., 2014, pp. 22-23).

Thus, the level and nature of the security culture largely depend on the subjects' spirituality. Still, the factors from the subject's surroundings are not to be underestimated. In other words, a subject's security culture is the resultant of the subject's quality (the result of personal development) and the number and quality of their relations with the closer and further surroundings.

Consequently, when analysing the security culture, one needs to contemplate the structural elements. They nest within four areas:

– axio-normative: determining the norms and values which found, order and provide meaning to human life;

– psychological: comprising evaluations, attitudes, motives and meanings which people ascribe to the material creations and behaviours;

– behavioural: regarding the inner and outer motor conducts;

– material: indicating the material dimension or means (Jarmoszko, 2016).

The security culture constitutes the broadly-understood dimension of the human culture referring to the intentional and active participation in shaping security. The deliberate activities are subject-oriented on individuals and communities in their life situations and the surroundings in which they function. The activities' purpose is—in a sense—the drive towards the optimization and universalisation of the security procedures in the personal and structural dimensions alike (Jarmoszko, 2016).

2. INFORMATION CULTURE AND INFORMATION SECURITY CULTURE

The progress of the global information society has turned information into a most passionately desired resource. Frequently, it is of higher value than material goods. Gathering, processing and passing information has become the fundament of the modern societies' functioning. In this context, the emergence of novel means of communication broadens the range of possibilities and opportunities.

Still, the information penetration/infiltration of all the aspects of life brings about a string of negative consequences. For instance, it causes the information noise, disinformation, information gap or lack of critical evaluation of the available data and inability to select the useful pieces. Therefore, there appears a real need to protect people against the destructive impact of those phenomena. Such is the aim behind the transition from the information literacy to the information culture (Batorowska, 2015). The latter is "the manifestation of knowledge concerning the essence of the information and its function; the awareness of the information's role and meaning; correct use of the information terminology; proper interpretation and use of information; respecting, appropriate gathering, storing and sharing information" (Babik, 2016, p. 48).

Accordingly, the subject's information awareness, their values and attitudes toward information, conduct and ethics of the information use as well as the creations stemming from the participation in the information process become the focus of the information culture. Then, it encompasses the material-technical, social, psychical and ideological elements and the connections among them (Batorowska, 2013). The information culture is the binder combining a myriad of human functioning areas. Therefore, it determines the subject's level of advancement and innovativeness. Consequently, it establishes the level of information security.

The information security is a complex issue; accordingly, in the subject literature, there function various definitions which—more or less successfully—express the essence of the matter. Some explanations narrow the term to the protection of the confidential data or ensuring security of the tele-information systems (i.a. Potejko, 2009; Marczyk, 2014). Other descriptions—approaching the problem more broadly—point at the possibility to acquire high quality information and ability to protect against its loss (i.a. Liderman, 2012; Fehler, 2016; Korzeniowski, 2017).

A given subject's level and quality of the information security is conditioned by the information security culture. It is the skill to identify—basing on important values—the true information and use it effectively (Filipek, 2017) for the sake of own, as well as the others', security. It means having the knowledge regarding shaping the information security policy, sensitivity to the abuse in that respect and determining the abilities to protect information against the threats of various backgrounds and natures (Batorowska, 2018). A high level of the culture and its positive features are connected with the Internet's constructive influence on the surroundings and favouring the balanced development of all the interaction participants. It is combined with the inclusion of other, objective security dimensions in the context of incoming information.

It needs to be pointed out the level of the information security culture is connected with technical issues. Hence, it is proved by the skills to select the incoming information by its credibility, timeliness and critical evaluation of the information source. The nature of the culture demonstrates itself in the subject's specific activities based on the incoming information and moderated through the subject's system of norms and values.

The information culture fosters the information security culture development of individuals and the whole society alike. The society's information culture creates the conditions for information security building. They are the three, interleaving and complementing each other, areas. Bearing in mind the increase of the information significance, their role in the current social reality will grow systematically.

3. THE INTERNET USERS' INFORMATION SECURITY CULTURE: PRACTICAL ASPECTS

The security culture is the subject's relatively constant feature. Compared to other—more objective—elements of the broadly understood system of security, this culture changes slower (Cieślarczyk et al., 2014). Its level and nature allow for predicting social behaviours when confronting danger. The culture predestines to undertaking certain activities; alternatively, in particular circumstances, it stops people from getting involved in other actions.

The choice, or abandonment, of specific behaviours and activities (co-activities) can primarily be inferred from the values and norms the subject respects. The values constitute an axis around which the other elements of the security culture are shaped (Figure 1). For behaviours, activities (co-activities) and attitudes create the direct manifestation of the subject's values and norms, the considerations regarding the Internauts' information security culture are presented from the outer ingredients towards the inner ones.

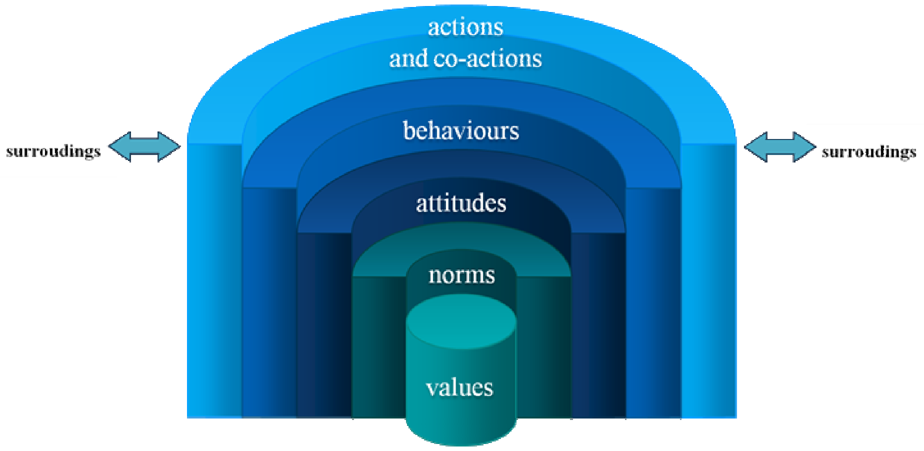

Figure 1. The cross-section of the security culture structure.
Source: the author's compilation based on: Cieślarczyk, 2006, p. 209.

Currently, the web is as important a sphere of functioning as the real world. The web creates an alternative to nearly every activity; simultaneously, it has an incredible influence. Via the Internet, ever more social organizations and private individuals carry out charitable fundraising. The range of such social ventures is specifically broad when human health and life are at stake and the costs of diagnosis, treatment and reablement are beyond the capabilities of the ill and their families.

Crowdfunding, i.e. social funding of various schemes in turn for certain provisions (Grodzka, 2016), is becoming more and more popular, too. Participation in such initiatives fuels the social, economic and/or technological progress. And—as the experience proves—there is no security without progress. People thinking in long-term categories do not focus exclusively on the "here and now." They take part in the creation of new technologies and services which improve the world. That way, such people create the security making in a multitude of dimensions. The security creation requires the constant search for the newer and more efficacious solutions improving the everyday existence and upgrading the quality of life.

The Internauts' support toward such activities is becoming a precious social resource. Concurrently, it indicates the empathy level, which is a serious determinant of a society's high cultural level. Here, the co-activity is a manifestation of the Internauts' cooperation for the sake of the common purpose, which the Internauts' self-identify with. The fundament of their relationship is trust and involvement based on the opinions and experience exchange as well as on emotion-sharing.

Likewise, the Internet proves an operative tool supporting the policing activities. For instance, the watchful Internauts spot and reveal the hideouts of people issued the wanted notices. The vigilance and ability to predict are vital skills in the security building for oneself, others and the surroundings alike. The Internauts commonly participate in the search for petty offenders, too. In the social media, victims upload the images of the culprits and crime scene recordings, hoping somebody may recognise the lawbreakers. Not only can publication of such contents lead to apprehension of a criminal, but also serves a preventive function. It is then focused on shaping the society's legal awareness, getting justice for the forbidden acts and being a deterrent. Much as revealing the image of the wanted seems ethically and legally debatable, it needs to be acknowledged that—when human health and life are in peril, or the values important for the country and nation are endangered—the public good is supreme to the personal one. Consequently, the Internauts' involvement in the restoration of the law and order is a manifestation of the citizens' responsibility for the level of social security.

Nevertheless, the dark side of the web cannot be ignored. Pathological and destructive behaviours and activities (co-activities) can endlessly be listed. The web has its grey zone used by those who want to hide from the observant eye of the police and other law enforcement agencies. The so-called *Dark web* has its own, unwritten and difficult to accept principles which contradict the widely accepted social standards. Due to the increased anonymity, that part of the web is commonly used for illegal activities. Numerous criminals treat the Dark web as a source of income. There, one can find offers of prohibited products (e.g. weapons or drugs) or services (e.g. forging passports or driving licences). For there is little chance of reporting the case to the police, a considerable number of such offers are scams; hence, crooks feel unpunishable.

The Dark web is also the sphere which attracts hackers and paedophiles; even the terrorists resort to the Dark web, e.g. the ISIS state used it extensively. Such users, however, do not take into consideration all the most prominent intelligence agencies in the world carefully monitor the functioning of the Dark web (Ormsby, 2019). Such screening resulted in, among others, capturing Ross Ulbricht, a.k.a. Dread Pirate Roberts, the creator of the *Silk Road*—an Internet auction platform operating in *the Tor* and closed by the US authorities in 2013. Another case which gained publicity was the arrest of several paedophiles, including Matthew Graham, a.k.a. Lux, the *PedoEmpire* creator—a paedophile service. There, criminals not only discussed and exchanged experiences and knowledge on how to subdue children to make them obedient and lenient to sexual activities, but also sent amateur pornographic films with the underage made by the portal users.

However, the deviant and infringing others' security behaviours and activities are not exclusive to the hidden spheres of the web. In the commonly available part of the Internet, it is easy to come across various examples of conducts which deeply hurt others. Certain principles ruling the cyberspace must have had a share in this phenomenon. Primarily, the conviction of being anonymous and unpunishable contributed to the emergence of brand-new and unheard of before forms of aggression and increased the number of attacks whose authors are becoming ever more difficult to trace.

Specific features of the virtual communities—non-spatial dimension, impalpability, anonymity, non-synchronicity and intentionality (Szymański, Jaworski, 2014)—as well as the multitude of communication channels among the users (e.g. the Internet communicators, social media, e-mail, blogs) have created a perfect environment for *cyber-bullying*. The term was coined in 2000 by Finkelhor, Mitchell and Wolak in their research on the American students. The scholars applied the term to the harassment with the use of the modern digital technologies (Monks, Coyne, 2012). Currently, humiliation, threatening, embarrassment, vilification, victimization, domineering and/or derision with the use of modern devices with the Internet access are common in the cyberbullying definitions (Kochan, Jędrzejko, 2018).

Cyber-bullying is somehow related to a relatively new—and equally pathological—phenomenon known as *patho-streaming*. It is transmitting live—most notably via *YouTube*—pathological behaviours, e.g. alcohol and drug abuse, fights, humiliation or setting people on fire (Siedlanowski, 2018). When it comes to combating such phenomena, the challenge is that—usually—once the streaming expires, the content is not stored or recorded on any channel.

What remains are the, so-called, screen shots of the “spiciest” fragments—made by the viewers. They add those screen shots to the contents of their channels and—from there—multiplicate them further. The more controversial and appalling the content, the more willingly watched it becomes. Obviously, it has a direct translation into the patho-streamers’ incomes for their “produce;” they receive money from the streaming platforms. Additionally, they are paid by the viewers, who—for “tips”—can demand ever more extreme tasks, naturally, crossing further barriers and boundaries. The most operative patho-streamers can earn from a few to a dozen or so thousand PLN for a several-minute streaming.

Sex-streaming emerges as a subgenre of patho-streaming. For a set amount of money—the ‘tip’—a person in front of the camera declares readiness to perform certain sexual activities. Since the research proves most of the recipients are under 15 years old, the problem is appearing urgent (Siedlanowski, 2018). To make the matters worse, the patterns and models of behaviour, actions and co-actions in the cyberspace influence the youth more profoundly than the traditional message from parents, educators and teachers. It is so because the former is “the so-called multi-factor influence occurring in numerous dimensions, multi-subject, carried out at one time and intensely repeated” (Jędrzejko, Traper, 2012, p. 107).

The above is forthrightly connected with *hating*—yet another negative cyberspace phenomenon which proves the low nature of the Internauts’ security culture. Hating means expressing radically negative opinions, usually lacking the subject matter justification (Naruszewicz-Duchlińska, 2015). The haters’ verbal assaults make the Internet appear an unfriendly medium. However, the qualitative analyses prove only a fraction of the internet utterances is aggressive and offending in their nature. Nevertheless, the impact of such statements is so serious that the number seems considerably bigger. It is connected with the so-called ‘positive inclination’ in social behaviours. Contrary to the negative ones, It makes positive or neutral claims not worthwhile. Hating is a premeditated activity focused on depreciating the recipient on the one hand, and calculated as an act of minimal risk as far as punishment is concerned, on the other. It uses the snowball effect; an aggressive comment provokes a hostile response which is retaliated with an even fiercer reply and so forth. Thus, the spiral of aggression winds up.

The above-presented instances of the Internauts’ activities highlight some of their attitudes. They are defined as “relatively constant tendencies of a human being to be positively or negatively disposed towards the subject”

(Wojciszke, 2003). Such understood attitudes have three components – emotional, cognitive and behavioural. They are a vital part of personality, which influences the manner and dynamics of human behaviour towards oneself, others and the surroundings in which they live.

When the Internauts engage in various activities, they generate a whole array of emotions. Showing care for others is a major indicator of the high level of security culture. Its special expression is empathy, i.e. the ability to understand others, share their emotions, react to their thoughts and feelings with appropriate sentiments. Empathy is a sign of above-average human sensitivity; its numerous manifestations can be noticed especially in the interactions among the participants of support groups for people with problems of all sorts. Sometimes, however, support becomes distorted. The forums and blogs for those with nutrition disorders may be an instance. The conversations participants, the so-called *Butterflies*, inspire each other and advise how to effectively lose weight. Although the health-hazardous forums and blogs are consequently removed, they are instantly replaced with new ones.

Demonstrating empathy requires leaving one's comfort zone and brings numerous benefits. First, following the rule of reciprocity, helping the needy, the benefactors may assume they will, in turn, receive the same treatment, in case they need it. Second, it constitutes a significant feature fostering proper communication. The ones who lack empathy hate objection, impose their will and do not take the arguments of others into consideration. Typically, they are people of highly confrontational, quarrelsome and aggressive nature.

The disappearance of empathy is easily observable in relation to aggressive behaviours of the perpetrators and witnesses. In the cyberspace, a certain percentage of the young demonstrates no sensitivity whatsoever. Therefore, they take up ever bolder attempts at attacking others. Consequently, when they become observers of such behaviours, they show more acceptance/tolerance toward such conducts.

The lack of inhibitions, observable in the Internauts' conducts and activities (co-activities) commonly stem from their false conviction of anonymity, which encourages breaking the accepted social norms. It is also accompanied by the certainty of impunity for the undertaken activities. Those cognitive elements of their attitudes are actually a result of the occurrence of the possibility to create their identity during the Internet interactions and attempts at concealing their own, true "I". The physical remoteness from the interacted ones is another contributing factor. It is decidedly easier to attack somebody distant; the outcomes of the damage done are less or non-visible; thus, a counter-attack threat is reduced to nil (Wallace, 2016). The sense of security is additionally amplified by the restrictions imposed by the reduced possibility to send and receive non-verbal messages. Since the still-dominant form of the web messaging is the text and schematic form of the messages' non-verbal aspect (emojis), the Internet relations lack the possibility to analyse and interpret the direct messages informing about the interlocutors' mood (mimic, gestures, eye contact etc.). And those stop people from initiatives which could harm others in the face-to-face encounters.

The feeling of anonymity is strongly related to the *de-individualisation*. It happens when one perceives oneself through the perspective of the group they represent rather than seeing oneself as a unique individual of inimitable properties. Such a mindset is typical of the participants of the forums in which people fall for either of the two opposite and hostile factions since they have discrepant views. The cognitive categorisation "we—they" results in people identifying themselves with "their" factions on a high level of group conformity. In consequence, their irrational and destructive behaviours become fully predictable. Such understood de-individualisation becomes a result of crossing the barrier of group integrity. In such cases, the drive towards cyberbullying may be connected with the occurrence of the group-thinking syndrome, i.e. the group members' dysfunction of rational decision making (especially in high integrity groups). The group—illusioned with infallibility and superiority—makes decisions of a dramatically risky nature (Irving, 1972).

The Internauts strongly need to be liked, noticed and appreciated, which is straightforwardly connected with the need for belonging. Accordingly, the Internauts satisfy the need via the social media. The fact someone found and shared contents or accepted an invitation, read the available posts and commented them creates illusory conviction of the Internauts' acceptance and respect, thus, positively influencing one's self-assessment. Still, the creation of the web self-image requires a string of conceptual and implementation steps. Obviously, their aim is to present oneself in the most favourable light. In that context, the need for certain exhibitionism, revealing one's privacy is commonly demonstrated.

Simultaneously, numerous Internauts appear irresponsible as for the number and quality of the information bits they make publicly available. Myriads of posts, commonly containing sensitive data (by the standards of legal regulations) make the Internauts leave all their characteristics in the web—address, job, education, marital status etc. Making such data available, the Internauts—in an aware manner—give up their right to privacy.

The inconsiderate use of the Internet is frequently the cause of real threats. Publicising information on, e.g. a holiday leave is a most unreasonable act—it creates a perfect opportunity to have the Internaut's house plundered. The police records confirm the holiday time is a period of intensive break-ins and thefts. Another instance of a similarly reckless information spread is parents posting photographs of their—largely undressed—children's. It simply feeds the paedophiles' lust; in the Dark web, such criminals commonly exchange picture compilations of the underage, even those in which the intimate parts are covered.

Obviously, there are Internauts who do guard their privacy as they realise the dangers of publicising the sensitive data concerning themselves and their dearest. The broad, perspective, security-oriented thinking is characteristic for such persons. They either know or intuitively sense their activities in the web do translate into their real lives and impact their health, economic, social and other dimensions of security. Such Internauts are aware the web offers a multitude of wonderful opportunities supporting development, self- and environment improvement. All that under the condition one uses the web wisely. They realise the security in the web needs to be constantly maintained and one needs to keep a watchful eye on the others' virtual security and—together—undertake actions aiming at sustaining and developing security.

The Internauts' attitudes seem diverse; the same applies to the norms and values—the focal security culture elements. A lot suggests the Internauts do appreciate life and health—own and others' alike. The others' wellbeing, their dignity and trust are also among the values they aspire for. Family and friends rank high among the Internauts' priorities, too. They respect the freedom of speech, opportunity to present independent opinions, spreading the less popular ideas and following the rules of proper behaviour.

Still, the unlimited freedom of speech brings about the temptation to manipulate the truth and lie. A lie brings moral decay to the liars' life and misleads the lied ones. Dishonesties are destructive, falsify information, distort the perception of reality and infringe mutual trust (Jędrzejko, Morańska, 2013). The occurrence of a lie in the web can be spotted only if one has an effective method of the incoming information assessment. Such a method is based on the gained knowledge and axiological-moral system. "The *web trap* lies in the attempts to turn information into 'knowledge' and then into 'wisdom'" (Jędrzejko, Morańska, 2013, p. 215).

People are bombarded with a myriad of information pieces. Hence, the essence of the message becomes difficult to grasp and separation of the significant bits from the irrelevant ones turns out a challenge. The structure of values can change under the influence of the incoming contents: "The media are capable of developing the non-existent desires, reinforcing consumerism and amplifying selfish attitudes. Therefore, instead of uniting people, the media contribute to their isolation, loneliness—even among the closest ones—and confusion among the material things. Promoting the comfortable life, the media may promote self-centredness, admiration for the tough, ruthless and—sometimes—violent society members. In other words, they can lower human culture" (Melosik, 2007, p. 89.) One is ready to negate the dignity of others when—under the cover of anonymity—they direct offensive remarks and comments at their victims.

Furthermore, the availability of various, not necessarily true, statements and judgements concerning an issue disturbs decision making and hampers establishing one's own views. Chaos and lack of criticism while receiving information lead to the disappearance of authorities—scientific and moral alike (Jędrzejko, Morańska, 2013). Accordingly, abiding the language norm or a certain group's cultural ideas seem unjustifiable. Disregard toward the netiquette is connected with the rejection of the egalitarian principles of the Internet existence and the balance between the needs of an individual and those of their community. "Netiquette takes care of an individual as the Internet consists of such. The Internet itself is, however, a common good; it requires common care and involvement" (Pręgłowski, 2012, p. 201).

Haters question the order of the matters, simultaneously, contributing nothing. Concurrently, by their confrontational conduct and lack of responsibility for their words, they break the ethical norms. The haters also go beyond the aesthetic norms for they brutalise the discourse. Additionally, they infringe the netiquette conventions by humiliating their web interlocutors (Naruszewicz-Duchlińska, 2015). The rule-breaking is a premeditated activity focused on provoking the opponent's negative emotions. For haters, the freedom of speech is a handy justification for their breaking the communication conventions. Indirectly, they manifest their independence from the communication and mental standards. Therefore, they touch upon taboos and refer to the sphere of desecration (described as thematic aggression—Taras, 2013).

4. INFORMATION SECURITY CULTURE: DEVELOPMENT POSSIBILITIES

The Internauts' behaviours place them variously on the scale from low to high levels of the information security culture. Some skilfully move about the sea of web information caring for the quality of their relations with other users and own psychical and physical comfort. Others follow the negative behaviours; either in a premeditated or careless manner, they involve themselves in the activities which put them and others in peril.

The positive displays of the information security culture in the web fade against the negative ones. There is a social conviction that acting accordingly to social rules and expectations is something normal and natural; henceforward, it does not require attention. Conversely, harmful, pathological and destructive contents and activities spark intense interest. Once the interest rises, so does their impact. In this context, the development of the knowledge, media, information and digital competences appear vital. They serve openness, wisdom and efficacious handling the modern cyberspace challenges. However, the so-far experience suggests the educational activities are insufficient in this respect.

Once the digital technologies have settled for good in almost every sphere of life, upgrading the level of the information security culture should become an inherent element of upbringing and education. The security culture is a psycho-social phenomenon and can be developed through education. To head off the potential effects of the negative influences of the modern technologies, the problematic areas of the Internauts' information security culture should be focused on.

The web environment constitutes a person's vital sphere of individual and social experiences; it becomes one's broad communication reality. Accordingly, shaping the competences crucial to the cyberspace independent and collective functioning seems the key issue. In such a context, the cyberspace's communal and participation nature (Pacewicz, Ptaszek, 2019), necessity to develop social and cultural skills as well as the respect for the social and cultural variety and discrepant systems of values, norms, views, opinions and attitudes need to be emphasised.

Consequently, there emerges the need to present such forms of one's own expression in the web which do not affront other Internauts. Another important aspect of the education for the information security culture should be the development of critical understanding the media environment and the rules operating the new media and the cultural, economic and technological conditioning of the Internet use. Education should also undertake the specifics of the Internet as a medium as well as the contents connected with shaping and popularisation of the socially desired patterns of the web behaviours. Simultaneously, it needs to be remembered the Internet communication is restricted in the same way as the other communication channels are.

The shaping of the utterance culture and proper Internet behaviours should be equally important elements of the educational activities to maintain the proper cultural level of the use of the language and following the rules of appropriate behaviour in the real world. So far, however, the netiquette has not been codified; subsequently, its breakers are not punished, either. Those may be the reasons for the improper and harming web activities.

In the light of the above, there arises an urgent need for the development of the ability to use the web in an aware, active and creative manner; maintaining the proper social norms and values, however. The appropriate use of the web should be supported with the knowledge and skills to recognise and react appropriately to the problematic aspects of that area of human activity.

To reach the broadest spectrum of recipients, the development of the information security culture through education should be diverse and use various channels and media. It is people of all ages who participate in the cyberspace interactions. Social relations require a strong motivation and consistency from both their organisers and participants. The actions should be long-term, cognitive, aesthetic, complex and designed to shape the morals. They also require time to develop.

CONCLUSIONS

The Internet has revolutionised human behaviours, changed the conditions of receiving, passing and collecting information. For centuries, they were determined by social and economic standing. Currently, more than a half of the world's population has access to the web anytime and anyplace. Hence, the influence of the medium is unprecedented.

The web carries both the positive but also harmful, pathological and destructive contents. It spreads knowledge as well as propaganda and manipulation. The Internet has an enormous potential to promote fake authorities and to question the true ones. However, it can become an effective means to combat lies, manipulation and scam. For some, it contributes to the realisation of important schemes. In other cases, it can lead to humiliation and disregard of human dignity and abandonment of the Plato's triad of the good, truth and beauty. The web can foster or disturb progress. Thus, its impact on the human reasoning is unquestionable, its power great and direction dependent on countless variables.

Simultaneously, the human functioning in the web is determined by a myriad of factors. An important-though-underrated one is the information security culture, which encompasses the system of human values, norms, attitudes, behaviours and actions (co-actions) toward a specific sector of reality, here—the cyberspace. For the purpose of the article was formulated three research problems and three hypotheses, which are preliminary answers to these problems. The first hypothesis, assuming that Internet users present a verying level and nature of information security culture, was positively verified. The analysis allowed to conclude that the level of the information security culture of Internet users is divided into a continuum—from low to high level. Some Internet users have a proper security culture nature in which socially approved values are the central axis. Around them evolve other components of this phenomenon psychosocial. Another part of Internet users shows an inappropriate nature of security culture. They undertake actions inconsistent with the applicable standards, the values are not guidelines for their behavior.

The second working hypothesis indicating that there is a close relationship between Internet users' information security culture and their online activity was also positively verified. The high level of the information security culture is related to the frequent undertaking the activities (co-activities) fostering own and other Internauts' security, showing positive emotions, constructive thoughts and convictions, norms and values crucial from an individual's perspective; yet, obviously, remaining within the social conventions.

The numerous quoted instances prove the level and nature of the Internauts' security culture remains low. Their involvement in the Dark web activities or cases of cyberbullying prove it. Such Internauts have a disturbed system of values and norms stemming from—among others—deranged socialisation. In view of the above, it should therefore be concluded that the third hypothesis, which assumes that the information security culture among Internet users can be improved in the process of education throughout life, was positively verified. The shaping of an acceptable system of values and norms, provision of knowledge development of media, information and digital competences and introduction to the safe web behaviours should be carried out through both formal and lifelong education. It is important to prepare the society not only for the participation in the social life via the modern media, but also for the role of the cyberspace makers, promoters of the positive changes and those who influence the changes in reality via the digital media.

The long-term purpose of such activities should be the creation of virtual space so that it fosters individual and social progress. It will be possible once the web users are prepared to comprehend and accept the challenges connected with their presence in the cyberspace, using the opportunities, countering threats and—in case of their occurrence—minimising the outcome.

BIBLIOGRAPHY

Babik W. (2016), *Kultura informacyjna a ekologia informacji współczesnego człowieka. Studium porównawcze*, [in:] H. Batorowska, Z. Kwiasowski (Eds.), *Kultura informacyjna w ujęciu interdyscyplinarnym: teoria i praktyka*, vol. 2, Kraków: Uniwersytet Pedagogiczny im. Komisji Edukacji Narodowej w Krakowie, pp. 45–54.

Batorowska H. (2013), *Od alfabetyzacji informacyjnej do kultury informacyjnej: rozważania o dojrzałości informacyjnej*, Warszawa: Wydawnictwo Stowarzyszenia Bibliotekarzy Polskich.

Batorowska H. (Ed.) (2015), *Kultura informacyjna w ujęciu interdyscyplinarnym: teoria i praktyka*, vol. 1, Kraków: Uniwersytet Pedagogiczny im. Komisji Edukacji Narodowej w Krakowie.

Batorowska H. (2018), *Kultura bezpieczeństwa informacyjnego*, Edukacja – Technika – Informatyka, no. 23(1), pp. 92–100.

Cieślarczyk M. (2006), *Kultura bezpieczeństwa i obronności*, Siedlce: Akademia Podlaska.

Cieślarczyk M., Filipek A., Świderski A.W., Ważniewska J. (2014), *Istota kultury bezpieczeństwa i jej znaczenie dla człowieka i grup społecznych*, Kultura Bezpieczeństwa, no. 1–2, pp. 17–58.

Fehler W. (2016), *O pojęciu bezpieczeństwa informacyjnego*, [in:] M. Kubiak, S. Topolewski (Eds.), *Bezpieczeństwo informacyjne w XXI wieku*, Siedlce: Uniwersytet Przyrodniczo-Humanistyczny w Siedlcach, pp. 25–43.

Filipek A. (2016), *Psychospołeczne i prakseologiczne aspekty jakości funkcjonowania systemu zarządzania kryzysowego*, Siedlce: Uniwersytet Przyrodniczo-Humanistyczny w Siedlcach.

Filipek A. (2017), *Rola edukacji w kształtowaniu kultury bezpieczeństwa informacyjnego*, [in:] H. Batorowska (Ed.), *Walka informacyjna. Uwarunkowania – incydenty – wyzwania*, Kraków: Uniwersytet Pedagogiczny im. Komisji Edukacji Narodowej w Krakowie, pp. 170–180.

Grodzka D. (2016), *Finansowanie społecznościowe*, Infos, no. 7, pp. 1–4.

Irving L.J. (1972), *Victims of groupthink: A psychological study of foreign-policy decisions and fiascoes*, Boston: Houghton Mifflin.

Jarmoszko S. (2016), *O kulturze bezpieczeństwa z perspektywy antropologicznej*, [in:] M. Faldowska, A.W. Świderski, G. Wierzbicki (Eds.), *Kultura bezpieczeństwa. Potrzeby i uwarunkowania*, vol. 3: *Kultura i wychowanie*, Siedlce: Uniwersytet Przyrodniczo-Humanistyczny w Siedlcach, pp. 7–33.

Jędrzejko M., Morańska D. (2013), *Pułapki współczesności*, part 1: *Cyfrowi Tubylcy. Socjopedagogiczne aspekty nowych technologii cyfrowych*, Dąbrowa Górnicza—Warszawa: Wyższa Szkoła Biznesu, Oficyna Wydawnicza Aspra-JR.

Jędrzejko M., Traper A. (2012), *Dzieci a multimedia*, Warszawa—Dąbrowa Górnicza: Oficyna Wydawnicza ASPRA-JR, Wyższa Szkoła Biznesu.

Kochan I., Jędrzejko M. (2018), *Cyberbullying wśród dzieci i młodzieży. Zjawisko, uwarunkowania, delegacje profilaktyczne*, [in:] M. Z. Jędrzejko, A. Szwedzik (Eds.), *Pedagogika i profilaktyka społeczna. Nowe wyzwania, konteksty, problemy*, Milanówek—Warszawa: Centrum Profilaktyki Społecznej—Oficyna Wydawnicza von Velke, Oficyna Wydawnicza Aspra-JR, pp. 103–120.

Korzeniowski L.F. (2017), *Podstawy nauk o bezpieczeństwie*, Warszawa: Difin.

Liderman K. (2012), *Bezpieczeństwo informacyjne*, Warszawa: Wydawnictwo Naukowe PWN.

Marczyk M. (2014), *Bezpieczeństwo teleinformatyczne wobec ataków terrorystycznych*, [in:] M. Górka (Eds.), *Cyberbezpieczeństwo jako podstawa bezpiecznego państwa i społeczeństwa XXI w.*, Warszawa: Difin, pp. 48–61.

Melosik Z. (2007), *Mass media i przemiany kultury współczesnej*, [in:] B. Siemieniecki (Ed.), *Pedagogika medialna*, vol. 1, Warszawa: PWN, pp. 59–75.

Monks C.P., Coyne I. (2012), *Przemoc i mobbing w szkole, w domu, w miejscu pracy*, Warszawa: Wydawnictwo Naukowe PWN.

Naruszewicz-Duchlińska A. (2015), *Nienawiść w czasach Internetu*, Gdynia: Novae Res Wydawnictwo Innowacyjne.

Ormsby E. (2019), *Darknet*, Warszawa: Znak.

Pacewicz A., Ptaszek G. (Eds.), (2019), *Model Edukacji Medialnej, Informacyjnej i Cyfrowej*, Retrieved November 23, 2020 from https://fina.gov.pl/wp-content/uploads/2019/12/memic_publikacja.pdf

Potejko P. (2009), *Bezpieczeństwo informacyjne*, [in:] K. A. Wojtaszczyk, A. Materska-Sosnowska (Eds.), *Bezpieczeństwo państwa*, Warszawa 2009: Oficyna Wydawnicza ASPRA-JR, pp. 193–211.

Pręgłowski M.P. (2012), *Zarys aksjologii Internetu. Netykieta jako system norm i wartości sieci*, Toruń: Wydawnictwo Adam Marszałek.

Sadłowska-Wrzesińska J. (2018), *Kultura bezpieczeństwa pracy: rozwój w warunkach cywilizacyjnego przesilenia*, Warszawa: Oficyna Wydawnicza Aspra-JR.

Siedlanowski P. (2018), *Patologia na piedestale. Próba oceny zjawiska patostreamu, jego źródeł i wpływu na rozwój dzieci i młodzieży*, [in:] M. Z. Jędrzejko, A. Szwedzik (Eds.), *Pedagogika i profilaktyka społeczna. Nowe wyzwania, konteksty, problemy*, Milanówek—Warszawa: Centrum Profilaktyki Społecznej — Oficyna Wydawnicza von Velke, Oficyna Wydawnicza ASPRA, pp. 121–136.

Szymański M., Jaworski E. (2014), *Religijność człowieka jeszcze realna czy już wirtualna*, [in:] J. Bednarek, A. Andrzejewska (Eds.), *Zagrożenia cyberprzestrzeni i świata wirtualnego*, Warszawa: Difin, pp. 186–197.

Taras B. (2013), *Agresja. Studium semantyczno-pragmatyczne*, Rzeszów: Wydawnictwo Uniwersytetu Rzeszowskiego.

Wallace P. (2016), *The psychology of the Internet*, Cambridge: Cambridge University Press.

Wojciszke B. (2003), *Postawy i ich zmiana*, [in:] J. Strelau (Ed.), *Psychologia. Podręcznik akademicki*, vol. 3: *Jednostka w społeczeństwie i elementy psychologii stosowanej*, Gdańsk: GWP, pp. 79–106.

SELECTED ELEMENTS OF THE INTERNET USERS' INFORMATION SECURITY CULTURE

Summary

The article analyses the Internauts' information security culture and discusses the theoretical fundaments of this psycho-social phenomenon. Three hypotheses was formulated, assuming that: (1) Internet users represent varying levels and nature of the information security culture, (2) there is a close relationship between Internet users' information security culture and their online activity, and (3) the information security culture of Internet users can be improved in the education process. All hypotheses were positively verified. This verification was based on the method of analyzing the literature on the subject and the available statistical data as well as the method of synthesis. The author examined the information security culture elements regarding the Internet users. The quoted examples allowed a conclusion the level and character of the Internauts' information security culture is varying and related to their activities in the cyberspace. The necessity to upgrade individual qualifications through formal and lifelong education was also indicated.

Keywords: security; security culture; education; Internet; web.

WYBRANE ELEMENTY KULTURY BEZPIECZEŃSTWA INFORMACYJNEGO UŻYTKOWNIKÓW INTERNETU

Streszczenie

Celem artykułu była analiza kultury bezpieczeństwa informacyjnego użytkowników Internetu. Sformułowano trzy hipotezy zakładające, że: (1) użytkownicy Internetu prezentują zróżnicowany poziom i charakter kultury bezpieczeństwa informacyjnego; (2) istnieje ścisły związek między kulturą bezpieczeństwa informacyjnego użytkowników Internetu a ich aktywnością w sieci oraz (3) kulturę bezpieczeństwa informacyjnego użytkowników Internetu można doskonalić w procesie edukacji. Wszystkie hipotezy zostały zweryfikowane pozytywnie. Weryfikacji tej posłużyły metoda analizy literatury przedmiotu i dostępnych danych statystycznych oraz metoda syntezy. W artykule poddano analizie poszczególne elementy kultury bezpieczeństwa informacyjnego w odniesieniu do użytkowników sieci. Przywołane przykłady pozwoliły stwierdzić, że poziom i charakter kultury bezpieczeństwa informacyjnego internautów jest zróżnicowany i pozostaje w związku z przejawianymi przez internautów aktywnościami w cyberprzestrzeni. Wskazano także na konieczność podnoszenia kwalifikacji w tym zakresie w toku edukacji formalnej i ustawicznej.

Słowa kluczowe: bezpieczeństwo; kultura bezpieczeństwa; edukacja; Internet.