UNIWERSYTET JANA DŁUGOSZA W CZĘSTOCHOWIE

Edukacyjna Analiza Transakcyjna 2024, nr 13

https://doi.org/10.16926/eat.2024.13.08

Zbigniew ŁĘSKI
https://orcid.org/0000-0003-4145-6955
Jan Długosz University in Częstochowa
Educational Transactional Analysis Research Team
e-mail: zleski@ujd.edu.pl

The Profile of Ego States and Experiencing Positive and Negative Feelings in the Context of Vulnerability to Cyber Threats

How to cite [jak cytować]: Łęski, Z. (2024). The Profile of Ego States and Experiencing Positive and Negative Feelings in the Context of Vulnerability to Cyber Threats. *Edukacyjna Analiza Transakcyjna*, *13*, 151–165.

Abstract

This article presents the results of the author's research, which analyzed the Ego State profiles of computer users and their tendencies to experience positive and negative emotions in the context of their potential vulnerability to cyber threats. The study employed the ACL Adjective Checklist, the SUPIN Positive and Negative Affect Scale, and a custom questionnaire designed to assess participants' susceptibility to cyber threats.

The research was conducted using the CAWI (Computer-Assisted Web Interviewing) technique on a group of 357 adults aged 18 to 76. For the ACL analysis, 206 surveys were selected based on results from the Com (Commonness) scale.

The findings did not reveal significant or clear relationships between the participants' Ego States and their vulnerability to cyber threats. However, such relationships were observed concerning the participants' affective traits. Positive affective traits serve as a protective factor in the context of cybersecurity, whereas negative traits increase susceptibility to cyber threats.

Keywords: Transactional Analysis, ego states, affective traits, emotions, cyber security.

Introduction

The social and psychological aspects of the subject matter pertaining to cyber security are not only very important but also very hard to analyse thoroughly. Technologies develop in an extraordinarily dynamic way. At the turn of the 21st century M. Castells (2003) wrote that the pace of changes makes it very had for scientists to explore nature, language and Internet limitations, and to explain how economiy and society based on this technology work. Unfortunately, despite the years that have gone by, his opinion still holds. Any conducted research quickly becomes obsolete due to the occurrence of new technological solutions. These, on the one hand, provide the users with new opportunities in the areas of work, entertainment or communication, and at the same time generate the areas of potential threats. The so-called IoT (Internet of Things) is developing rapidly. Nowadays, the exchange of data via the global net often happens automatically, and it is initiated by devices we use on a daily basis. Most modern cars are connected to the net, which makes it possible to monitor their functioning with the help of special applications. Monitoring systems accessible from every place of the globe are gaining popularity as well. Smart watches monitor our activity and health, saving information on this subject matter in the data cloud linked with the user's account. There are many more examples, and new devices with an option of access to the Internet regularly appear on the market. As a result, there is more and more data in the web and it is often sensitive.

Man as a subject in the cyber security chain

Analysing the aforesaid subject matter and trying to diagnose its state, technological solutions in the form of appropriate hardware and software security features are often put on the first place. Meanwhile, among all, M. Dun Cavelty et al. (2023) directly suggest that we should change our priorities while thinking about cyber security, not treating it as a technological problem + people, but a social one + technology. Thus, it is vital to focus on educating society in the area of cyber security, and on analyses that help to identify an individual's features impacting their vulnerability to cyber threats. S. M. Albladi and G. R. S. Weir (2017) conducted very interesting studies in this area. The results obtained by them show that important predictors of human vulnerability to cyber threats are personality features combined with such factors as users' trust, their competencies, motivation and earlier experiences with cyber threats. It was stated that diligence, being agreeable and neurotic significantly decrease the user's vulnerability to cyber threats in the context of social networking, whereas being extrovert significantly increases the probability of falling a victim to cyber attacks.

M. Bada and J.R.C. Nurse (2020) additionally draw the readers' attention to the fact that we should also analyse how society members perceive the matters of potential risk and how potential incidents linked with cyber security might impact their functioning.

From the point of view of a person as a user of new technologies, ones of the most dangerous threats in the area of cyber security are the so-called social engineering attacks. Their efficacy depends on the traits, awareness, knowledge and skills of an attacked individual. They are based on appropriately selected manipulation mechanisms which are to convince a potential victim to take a step that will consequently put them at risk. There might be various consequences – from lost data to a financial loss. In their research conducted in academic environments, E. Benavides-Austido et al. (2022) showed that students are more vulnerable to social engineering attacks than lecturers. One of many reasons given by the authors is overconfidence and lack of experience. At the same time, the research showed that persons who spend more time in front of their computer and are more tolerant towards potential risky behaviours are more vulnerable to social engineering attacks.

One type of social engineering attacks are frauds based on messages sent to potential victims, in which the sender convinces the addressee to pay a certain sum of money into their account in return for the promise of a significant profit or under the threat of disclosing compromising information. Among all, M. Ajayi (2022) conducted some research in this area. Having analysed discursive-manipulative strategies in over 200 e-mails and 50 messages in Nigeria, he identified discursive manipulating strategies such as a positive and negative false alarm, self-depreciation, language formulas, and references to theistic and religious contexts. The research concerned Nigerian society, but the issue of that type of fraud is present all over the world and works according to a similar scheme. The author of this publication also analysed this phenomenon in cooperation with M. Kurkowski, B. Gozdecki and W. Steingartner, studying the language of internet fraudsters from the angle of transactional analysis (2023). Further on, describing the results of their research, B.G. Anders et al. draw the readers' attention to the fact that users find it difficult to spot false e-mails and are not aware of consequences of careless sharing of personal information online. They also emphasise the need to employ educational strategies that aim at increasing the awareness and knowledge in users of new technologies.

Doubtlessly, apart from education, it is also necessary to introduce appropriate security at the hardware and software level. It shall be remembered though that especially in case of consumer devices, it is the user who turns on and configures a given device. Will they have enough awareness to use appropriate passwords? Will they care to update software regularly? D. Dave et al. focus on the importance of these aspects as in their conclusion from their own research analysing four main categories of threats, they identified the most important of them. These are malware attacks, social engineering attacks, network security vulnerabilities and data breaches (2023).

At the end, it is worth mentioning that among solutions that are to improve the state of cyber security there are also those that are trying all the time, often with the use of artificial intelligence, to look for all the information on potential threats in order to react to it as quickly and efficiently as possible. One of such sources of information are social media, and the publication by A. Alevizopoulou et al. (2021) gives an example of such a solution. The authors designed, implemented and evaluated a system which monitors Twitter in order to identify information on cyber threats linked with the Internet of Things.

Transactional Analysis and emotional states in the context of cyber security

One might write endlessly about cyber security, yet it seems that the aforementioned facts and publications unanimously confirm the need to draw more attention to man as a subject using new technologies. This publication attempts to analyse the impact of undertaking risky behaviours by the users of new technologies due to such user traits as their tendency to accept particular affective states and their profile of ego states understood according to the concept of transactional analysis.

M. M. Tugade and B. L. Fredrickson (2007) draw the readers' attention to the fact that experiencing positive emotions correlates positively with the inner location of control, the feeling of satisfaction with one's life or one's self-esteem. Thus, it seems it may be assumed that it shall correlate negatively with an individual's vulnerability to cyber threats. In order to take care of one's security, it takes certain energy and engagement, which demands motivation, patience and self-control from an individual. B. L. Fredrickson also writes about the broaden and build theory (2001), according to which positive emotions have long-term consequences for human development. They are tools for building social relations and bonds, build mental resilience and stimulate an individual's self-development. R. M. Ryan and E. L. Deci (2000) also mention the role of positive emotions as one of the factors influencing intrinsic motivation, self-development or initiative. On the other hand, J. J. Gross emphasises the importance of knowing how to regulate emotions as that skill helps an individual to decrease negative emotions and take rational and effective decisions, acting efficiently.

Taking into account the aforesaid assumptions, it can be stated that positive emotions and positive thinking shall have a positive impact on an individual's security in the world of new technologies.

This article also takes into account ego states understood according to the concept of transactional analysis, which was created by E. Berne. Transactional analysis was developed in the 50s of the 20th century as a psychotherapeutic concept. Its indisputable advantage is simple and clear terminology, which makes it possible to understand phenomena analysed with its use also for people outside scientific circles. TA assumes the existence of three basic ego states: the Parent ego state, the Adult ego state and the Child ego state. According to the founder, Eric Berne, these are sets of thoughts, feelings and behaviours. The Parent ego state consists in imitating the behaviour and feelings of parents or other important people; the Child ego state consists in recreating childhood emotions and behaviours; the Adult ego state is the reaction based on an objective assessment of a situation with the use of skills and resources at one's disposal. This division constitutes the so-called first-order structural analysis (2005). Further divisions are made if there is a need of more complex analyses. This publication uses the so-called functional analysis that distinguishes additional subcategories within the Parent and Child ego states (Stewart & Joines, 2016):

— The Normative Parent ego state controls and sets norms.
— The Nurturing Parent ego state ensures support and care.
— The Adapted Child ego state teaches how to adapt to social expectations and norms.
— The Free Child ego state is responsible for joy, creativity and spontaneity.

The Parent ego state is not subject to further division here.

Using the concept of transactional analysis in the context of analysing the behaviour of users of new technologies is not a new idea. It can be even said that there are already certain achievements and traditions in this field. For example, the research by A. Pierzchała in which she analyses communication on internet forums, identifying, among others, the users' ego states from the level of which they send their messages (2010). The author of this publication also has got certain achievements in this field as he analysed the phenomenon of projecting the user's ego state profile on new media (Łęski, 2016). Thus, the potential of transactional analysis in this field has already been proven and this publication is the search for further areas where this concept can be applied.

Methodological assumptions

The aim of this research was determining the relations occurring between the profile of ego states studied from the perspective of transactional analysis at the level of functional analysis, and predilections for experiencing positive and negative feelings in the context of vulnerability to cyber threats understood as a predilection for undertaking potentially risky activities in cyberspace. The research was conducted with the help of the CAWI (Computer-assisted web interviewing) questionnaire technique. It rendered 357 fully completed questionnaires.

The following research problems were formed:

1. What is the relation between the charges' ego states and their affective traits (experiencing positive and negative feelings)?
2. What is the relation between the charges' ego states understood from the point of view of transactional analysis and their vulnerability to cyber threats?
3. What is the relation between affective traits (experiencing positive and negative feelings) and the charges' vulnerability to cyber threats?

The research uses the following tools:

1. The Adjective Checklist (ACL) by H.G. Hough, A.B. Heilbrun Jr – Polish normalisation (Martowska, 2012)
2. The Positive and Negative Affect Schedule (PANAS) by D. Watson and L. A. Clark – Polish adaptation of the scale (SUPIN) (Brzozowski 2010)
3. The Questionnaire of Vulnerability to Cyber Threats developed by the author for the purposes of this publication.

The Adjective Checklist (ACL) is a tool destined to research teenagers and adult people. The Polish normalization of the ACL was performed by the team of the Psychological Testing Laboratory of the Polish Psychological Association. The ACL serves to diagnose various dimensions of human personality, and it has its sources in the works of H. G. Gough, who, in 1952, published a list of 300 adjectives destined to evaluate some personality dimensions. The ACL contains 37 scales divided into 5 parts, and this publication uses the fourth part containing five scales constructed on the basis of the concept of E. Berne's transactional analysis.

1. Controlling Parent – CP
2. Nurturing Parent – NP
3. Adult – A
4. Free Child – FC
5. Adapted Child – AC

Additionally, the Com (commonness) scale was taken into account, which allowed for rejecting the answers that in the authors' opinion might have been provided randomly.

It is important to note that the research described in this publication was conducted in Poland using the Polish version of the ACL textbook, published in 2012. The Polish translations for the Ego States in the ACL manual did not fully align with their English counterparts. For example, the term Controlling Parent was translated as "Rodzic Krytyczny" (literally, Critical Parent), Free Child as "Dziecko Spontaniczne" (literally, Spontaneous Child), and Adapted Child as

“Dziecko Uległe” (literally, Submissive Child). In 2016, with the publication of the Polish edition of *Transactional Analysis Today* by S. I. Stewart and V. Joines (*Analiza transakcyjna dzisiaj*), these translations were revised to reflect the original English terminology. This publication adheres to the standardised terminology introduced in 2016.

The ACL consists of 300 adjectives ordered alphabetically. All the adjectives together with the instruction are placed on one A4 sheet of paper, both sides. The task of a charge is to choose adjectives which in their opinion relate to them the most.

The reliability of the tool within the analysed scales for women ranges from 0.67 (CP) to 0.78 (FC). For men, the alpha values range from 0.61 (CP) to 0.79 (NP). Sten standards are developed separately for women and men aged 15-69.

The Positive and Negative Affect Schedule (PANAS) is a tool that serves to measure the intensification of positive and negative emotions. It has four different versions and is destined to measure both current emotional states (versions S20 and S30) and stable affective traits (versions C20 and C30). This study uses C30 version consisting of 30 entries and serving to study relatively stable affective traits.

The PANAS version used in this research consists of two scales:

PA-15 – positive feelings
NA-15 – negative feelings

Both of the above scales consist of 15 adjectives each, placed on one-A4 sheet of paper, and the charge’s task is to relate to each adjective at a five-score scale from *slightly or not at all* (1) to *very much* (5), according to the instruction that says, “Read every word and think how you GENERALLY or USUALLY feel. Then, tick the right answer.”

The reliability of the tool in its C30 version is high. Cronbach’s alpha equals 0.89 for the PA scale, and 0.95 for the NA scale for the group of women, and for men it is 0.86 for PA and 0,94 for NA respectively. Sten standards are developed separately for women and men.

The Questionnaire of Vulnerability to Cyber Threats is the author’s tool developed for the purposes of this publication. It consists of 16 statements referring to potentially risky behaviours on the Internet or rules concerning cyber security. The questionnaire was drawn in such a way so as to have a possibility to correlate each statement separately, and also as one scale rendering a general result of vulnerability to cyber threats. Cronbach’s alpha equals 0.7 for this scale. It should be emphasised that this tool has an experimental form and shall be improved during further research conducted by the author.

The charges were also asked about their age, sex and education, and their self-esteem in the area of operating new technologies was checked too.

The report on research results

As mentioned, the research was conducted using the CAWI (Computer-Assisted Web Interviewing) questionnaire technique. Among the 357 fully completed questionnaires, 276 were completed by women and 81 by men. The participants' ages ranged from 18 to 76, with the highest number of responses from those at the younger end of this range. The average age of respondents was 28.5 years, with a median age of 23. A total of 167 respondents held higher education degrees, while 190 had completed secondary education. The majority assessed their skills in using new technologies as very high (94 respondents) or high (131 respondents). An average skill level was reported by 99 respondents, while low and very low skill levels were reported by 26 and 7 respondents, respectively.

The ACL analysis, based on grouping by frequency (number of selected adjectives) and results on the Com (Commonness) scale, was conducted on 206 questionnaires completed by respondents aged 19 to 76 (average age of 29, median age of 23). This group included 167 women and 39 men. In terms of education, 95 respondents in this group held higher education degrees, while 112 had completed secondary education. Regarding their self-assessed technological skills, 43 rated them as very high, 81 as high, 59 as average, 20 as low, and only 3 as very low.

Given the nature of the conducted research and the distribution of the data in the studied population, the Spearman rank correlation coefficient was employed to explore potential relationships between the variables. This non-parametric method was chosen due to its suitability for data that do not meet the assumptions of normal distribution. While the results of the analysis revealed few statistically significant and clearly observable correlations, they do highlight certain noticeable trends. These trends provide valuable insights and suggest directions for future, more in-depth analyses.

Analysing the correlation between the charges' ego states and their affective traits, there was only one significant correlation coefficient whose value points to a slight yet noticeable correlation where r=0.226; p=0.001. It is the coefficient illustrating the correlation between positive affective traits (the PA scale) and the Adult ego state (A). Due to the implementation of the ACL list to determine the respondents' ego states, the analysis was carried out on the sample of N=206.

The Adult ego state in transactional analysis is responsible for rational, logical thinking, objective and adequate understanding of reality and decision taking based on reliable and objective analysis of available information. Currently we also talk about the Integrated Adult ego state that is able to use all the individual's ego states in a harmonious way. Z. Wieczorek (2017) was one of the authors writing about the integration of the Adult ego state, while G. Žvelc introduced the concept of the Mindful Adult (2010). The positive correlation observed here points to the fact that persons using the Adult ego state more often, at the same time have a tendency to think positively about themselves and others. As it has been mentioned in the previous parts of this article, positive thinking offers strength and motivation for self-development. And the outcome of this self-development is a well-formed Adult ego state.

Unfortunately, there have been no clear and significant correlations observed between the respondents' ego states and their vulnerability to cyber threats. The result in relation to the scale of vulnerability that contains all the statements of the questionnaire is statistically insignificant. It is similar in case of pairing with particular statements of the questionnaire. There is one exception, namely a correlation between the Controlling Parent ego state and the statement, "The computer that I work on is always equipped with up-to-date security software (antivirus, firewall, etc.)." In this case r=0.186; p=0.007. As it can be seen, the result is statistically significant at the level of 0.05 accepted for social sciences, but the value of the correlation coefficient is very low and points to a very weak correlation (J. F. Hemphill, 2003, writes more about various approaches to the interpretation of the value of the correlation coefficient in psychometrics). Nevertheless, it should be emphasized that this correlation in this very place seems expected and most certainly justified. The Controlling Parent is based to a large extent on standards and rules, and regular security software upgrade is one of the most important rules which are repeated in the context of cyber security.

There were also two more statistically significant results – the correlation between the statement, "In social media I like showing my friends regularly what I do, where I go, what I watch, etc." and the Adult and Free Child ego states. The coefficients equalled there r=0.15; p=0.03 and r=0.142; p=0.04 respectively. The value of the coefficients is even lower here than in the case described above and likewise it can at most testify to a very weak correlation. While in the case of the Free Child ego state this correlation might have been justified (spontaneity, willingness to share impressions, acting under the influence of impulse – not necessarily thought over, etc.), it is puzzling in the case of the Adult ego state. Of course, it could be written that due to the low value of the coefficient it can be assumed that the result is not bounding and it should not be analysed any further. Nevertheless, it is statistically significant. It seems that it might point to the need to work on that statement in further research projects or to the necessity of its analysis together with other variables. Sharing every moment thoughtlessly in social media constitutes a serious threat to an individual's security and very often not only cyber security. At the same time though, it can also concern, for example, only the area of interests and omit sensitive and potentially dangerous content. It can also focus only on the user's job. Finally, it can be subject to different rules that minimize potentially negative outcomes. For example, caring to include in the group of friends that have access to such information only those that are really known to the user and trustworthy, or an appropriate selection of information and the choice of dates on which particular pieces of information are published. In other words, in fact we deal here with two types of users, which was not fully taken into account while developing the research tool. On the one hand, there are those that from the level of the Free Child ego state post a lot of information on themselves, not even thinking where these messages go and how they may be used. On the other hand, there are those who purposefully and knowingly, from the level of the Adult ego state, promote certain content and post new messages with the care about the rules concerning cyber security.

The next question posed in the methodological part of this article regards potential correlations between affective traits of the respondents and their vulnerability to cyber threats. With regard to the scale of vulnerability that comprises all the statement of the questionnaire, the correlation coefficients both with the scale of positive feelings and the scale of negative feelings are statistically significant. In case of positive feelings (PA) r=-0.175, p=0.001. In case of negative feelings (NA) r=0.195, p=0.0001. Thus, as it can be seen, in both cases we deal with slight correlations, while the PA scale correlates negatively and the NA scale positively. The obtained results confirm the considerations contained in the earlier sections of this paper, saying that experiencing positive emotions can act protectively against cyber threats. A statistically significant negative correlation between positive affective traits and vulnerability to cyber threats suggests that persons with a higher level of positive emotions may be less vulnerable to such threats. It is consistent with the aforesaid broaden and build theory by Fredricson (2001) that emphasizes that positive emotions contribute to developing mental resilience and building social bonds, which, as a result, might impact an individual's ability to manage risk effectively. As for the positive correlation between negative affective traits and vulnerability to cyber threats, it confirms the earlier theses suggesting that negative emotions might decrease motivation to act in the area of cyber security, which increases vulnerability to threats. The results fully correspond with the earlier research that points to the importance of emotions and emotional regulation in the context of cyber security. They confirm the theoretical assumptions that positive emotions and the ability to regulate them are key to ensure better protection against cyber threats, whereas negative emotions might foster greater vulnerability to such threats.

Analysing the correlations between the tendency to feel positive and negative emotions and particular statements allowed for observing a few interesting results, which confirm the conclusions mentioned above even more strongly. They are all presented in Table 1.

Table 1
A summary of significant correlations between the PA and NA scales and the statements linked with potential vulnerability to cyber threats

Statements:	**PA**	**NA**
The computer that I work on is always equipped with up-to-date security software (antivirus, firewall, etc.).	**0.115***	**-0.046**
Before I click on the "OK" button on the screen, I always read and check what I will confirm in this way.	**0.109***	**-0.047**
I distinguish messages that might be a form of Internet fraud or contain malware.	**0.211****	**-0.127***
I can effectively search for and select information on the Internet.	**0.254****	**-0.151****
In my Internet comments I happen to react with anger and aggression.	**-0.110***	**0.232****
If I get an e-mail message, e.g. from the Polish Post with the information that I shall click on the link within to confirm that I want to receive a package, I will simply click on it.	**-0.156****	**0.122***
Inviting people I have never met to the group of friends/ followers on social media portals is in fact OK.	**-0.072**	**0.198****
I try to use good passwords, containing combinations of various signs, different for every important service I use.	**0.162****	**-0.098**
In social media I like showing my friends regularly what I do, where I go, what I watch, etc.	**0.059**	**0.159****

* Significant correlation at the level of 0.01
** Significant correlation at the level of 0.05

Source: own research

Although the obtained values of correlation coefficients point to weak correlations, clearly there is a consistency and a recurring pattern here, according to which positive feelings foster activities improving the respondents' cyber security, and negative feelings increase the risk of vulnerability to cyber threats. Clearly, this trend is evident when we take into account the statements concerning one's ability to spot messages that might be a form of Internet fraud, the declaration about one's ability to effectively search for and select information, one's tendency to react with anger and aggression in their online relations. In each of the cases above there were statistically significant results with mutually opposing values (positive versus negative).

Sumary and conclusions

This article aimed at the attempt to look at the issue of an individual's vulnerability to cyber threats from the perspective of their tendency to experience positive or negative feelings and people's ego states in the context of transactional analysis. The results obtained are satisfying, looking from the perspective of affective traits. The author's assumptions deriving from scientific texts concerning the impact of positive and negative emotions on human functioning and development, stating that positive emotions shall positively correlate with activities increasing security, contrary to the negative ones have been confirmed. At the same time, the research did not show any clear and significant correlations that could be related to the influence of the respondents' ego states on their vulnerability to cyber threats. One would expect positive correlations between activities improving security and the Adult ego state, but unfortunately no such correlations have been proven. A question that one should pose at this moment is whether it means that there are no such correlations or a methodological mistake was made. It seems worth considering some further studies in this area but with the use of a different tool than the ACL. The ACL is a very complex questionnaire, offering the possibility of analysis on many different scales. The CR (Critical Parent) scale has a rather low reliability (Cronbach's alpha coefficient equals 0.61) and the textbook suggests excluding it from individual diagnosis. In fact, the minimum acceptable value in social and psychological studies is 0.7, while for clinical studies and individual diagnosis it is at least 0.8 (see e.g. Nunnally, Bernstein,1994, pp.264-265). Meanwhile, in the research in question, as for the area of ego states, most of the respondents obtained the highest result just in the area of the Critical Parent (CP) ego state, which, taking into account the abovementioned value of Cronbach's alpha coefficient, calls into question the reliability of the whole analysis concerning the respondents' profile of ego states. What is more, in the future it is worth considering a search for more complex correlations, where ego states can have a function of intermediary variables.

The observed correlations are particularly interesting and valuable, as they indicate an increasing cybersecurity risk with higher levels of negative affect, while positive affect plays a significant protective role in this context. Maintaining cybersecurity requires positive emotional states, such as engagement, motivation, and initiative. This seems to be an important yet underestimated aspect of ensuring cybersecurity. Therefore, alongside training focused specifically on cybersecurity skills and competencies, greater emphasis should be placed on workshops that develop social skills and the ability to recognize and regulate emotions, particularly among the younger generation.

In conclusion, these studies have confirmed the importance of positive affective traits with regard to care about one's own security. At the same time, they have not confirmed the correlation between vulnerability to cyber threats and the profile of the respondents' ego states, at the same time showing the direction of further research and analyses, not dismissing the potential that the concept of transactional analysis brings in this regard.

References

Ajayi, T. M. (2022). Discursive-manipulative strategies in scam emails and SMS: The Nigerian perspective. *Lodz Papers in Pragmatics, 18*(1), 175–195. https://doi.org/10.1515/lpp-2022-0008.

Albladi, S. M., & Weir, G. R. S. (2017). Personality traits and cyber-attack victimisation: Multiple mediation analysis. *2017 Internet of Things Business Models, Users, and Networks*, 1-6. https://doi.org/10.1109/CTTE.2017.8260932.

levizopoulou, S., Koloveas, P., Tryfonopoulos, C., & Raftopoulou, P. (2021). Social media monitoring for IoT cyber-threats. In *2021 IEEE International Conference on Cyber Security and Resilience (CSR), Workshop on Data Science for Cyber Security (DS4CS @ IEEE CSR)*, Rhodes, Greece, July. IEEE.

Bada, M., & Nurse, J. R. C. (2020). The social and psychological impact of cyberattacks. [In:] V. Benson & J. Mcalaney (Eds.), *Emerging cyber threats and cognitive vulnerabilities* (pp. 73–92). Academic Press. https://doi.org/10.1016/B978-0-12-816203-3.00004-6.

Benavides-Astudillo, E., Silva-Ordoñez, L., Rocohano-Rámos, R., Fuertes, W., Fernández-Peña, F., Sanchez-Gordon, S., & Bastidas-Chalan, R. (2022). Analysis of vulnerabilities associated with social engineering attacks based on user behavior. In M. Botto-Tobar, S. Montes León, P. Torres-Carrión, M. Zambrano Vizuete, & B. Durakovic (Eds.), *Applied Technologies. ICAT 2021. Communications in Computer and Information Science* (Vol. 1535). Springer, Cham. https://doi.org/10.1007/978-3-031-03884-6_26.

Berne E. (2005). *Dzień dobry i co dalej*. Rebis.

Brzozowski, P. (2010). *Skala uczuć pozytywnych i negatywnych SUPIN. Polska adaptacja skali PANAS Davida Watsona i Lee Anny Clark. Podręcznik*. Pracownia Testów Psychologicznych Polskiego Towarzystwa Psychologicznego.

Castells M. (2003). *Galaktyka Internetu.* Rebis.

Dave, D., Sawhney, G., Aggarwal, P., Silswal, N., & Khut, D. (2023). The new frontier of cybersecurity: Emerging threats and innovations. *2023 29th International Conference on Telecommunications (ICT)*, 1-6. https://doi.org/10.48550/arXiv.2311.02630.

Dunn Cavelty, M., Eriksen, C., & Scharte, B. (2023). Making cyber security more resilient: Adding social considerations to technological fixes. *Journal of Risk Research, 26*(7), 801-814. https://doi.org/10.1080/13669877.2023.2208146.

Fredrickson, B. L. (2001). The role of positive emotions in positive psychology: The broaden-and-build theory of positive emotions. *American Psychologist, 56*(3), 218–226. https://doi.org/10.1037/0003-066X.56.3.218.

Gross, J. J. (2002), Emotion regulation: Affective, cognitive, and social consequences. *Psychophysiology, 39*, 281–291. https://doi.org/10.1017/S0048577201393198.

Hemphill, J. F. (2003). Interpreting the Magnitudes of Correlation Coefficients. *American Psychologist*, *58*(1), 78–79. https://doi.org/10.1037/0003-066X.58.1.78.

Łęski, Z. (2016). *Duch w maszynie… Kim jest dla nas komputer? Charakterystyka relacji w języku analizy transakcyjnej*. Wydawnictwo AJD w Częstochowie.

Łęski, Z., Kurkowski, M., Gozdecki, B., & Steingartner, W. (2024). Czy można zakochać się w Jessice? — czyli o Nigeryjskim Przekręcie z perspektywy Analizy Transakcyjnej. *Przegląd Policyjny, 152*(4), 249–261. https://doi.org/10.5604/01.3001.0054.4340.

Martowska K. (2012). *Lista przymiotnikowa ACL. Harrison G. Gough, Alfred B. Heilburn, Jr. Polska normalizacja. Podręcznik.* Pracownia Testów Psychologicznych Polskiego Towarzystwa Psychologicznego.

Nunnally, J. C., & Bernstein, I. H. (1994). *Psychometric theory* (3rd ed.). McGraw-Hill.

Pierzchała A. (2010). Rodzic, Dorosły, Dziecko – jak można opisać komunikację na forach internetowych. In M. Sokołowski (Eds.). *Oblicza Internetu. (Re)definiowanie sieci.* Wydawnictwo PWSZ w Elblągu.

Ryan, R. M., & Deci, E. L. (2000). Self-determination theory and the facilitation of intrinsic motivation, social development, and well-being. *American Psychologist, 55*(1), 68–78. https://doi.org/10.1037/0003-066X.55.1.68.

Sanders, B. G., Dowland, P. S., & Furnell, S. (2009). An assessment of people’s vulnerabilities in relation to personal and sensitive data. W *Advances in Communications, Computing, Networks and Security: Proceedings of the MSc/MRes programmes from the School of Computing, Communications and Electronics, 2007-2008* (Vol. 6, p. 124). University of Plymouth.

Stewart, I., & Joines, V. (2016). *Analiza transakcyjna dzisiaj*. Rebis.

Tugade, M. M., & Fredrickson, B. L. (2007). Regulation of positive emotions: Emotion regulation strategies that promote resilience. *Journal of Happiness Studies, 8*, 311–333. https://doi.org/10.1007/s10902-006-9015-4.

Wieczorek, Z. (2017). Język zmiany w analizie transakcyjnej. *Edukacyjna Analiza Transakcyjna, 6*, 145–156. https://doi.org/10.16926/eat.2017.06.09.

Žvelc, G. (2010). Relational schemas theory and transactional analysis. *Transactional Analysis Journal, 40*(1), 8–17. https://doi.org/10.1177/036215371004000103.

Profil stanów ja a przeżywanie uczuć pozytywnych i negatywnych w kontekście podatności na cyberzagrożenia

Streszczenie

W niniejszym artykule opisano wyniki badań własnych autora, w których dokonano analizy profilu stanów Ja użytkowników komputera oraz jego tendencji do przeżywania uczuć pozytywnych i negatywnych, w kontekście jego ewentualnej podatności na cyberzagrożenia. W badaniach wykorzystano listę przymiotnikową ACL, skalę uczuć pozytywnych i negatywnych SUPIN oraz kwestionariusz autorski do weryfikacji podatności badanych na cyberzagrożenia.

Badania prowadzone były techniką ankietową CAWI na grupie 357 osób dorosłych w wieku od 18 do 76 lat, przy czym do analizy przy pomocy listy ACL, na podstawie wyników w skali Com (Typowość) wytypowano 206 ankiet.

Uzyskane wyniki nie wykazały istotnych i wyraźnych zależności pomiędzy stanami Ja badanych a podatnością na cyberzagrożenia. Zależności takie zaobserwowano jednak w odniesieniu do cech afektywnych badanych. Pozytywne cechy afektywne są czynnikiem chroniącym w kontekście cyberzagrożeń, podczas gdy cechy negatywne zwiększają podatność badanych w tym zakresie.

Słowa kluczowe: analiza transakcyjna, stany Ja, cechy afektywne, emocje, cyberbezpieczeństwo.