Trakia Journal of Sciences, No 2, pp 143-146, 2024

Available online at:
https://trakia-uni.bg

ISSN 1313-3551 (online) doi:10.15547/tjs.2024.02.006

Original Contribution

RISK IN CYBER ENVIRONMENT

J. Aleksovski[1], N. Pirovski[2]*, I. Georgieva[3]

[1]Student, Faculty of Medicine, Trakia University, Stara Zagora, Bulgaria
[2]Department of Anatomy, Faculty of Medicine, Trakia University, Stara Zagora, Bulgaria
[3]Philosophy of Science Department, Institute of Philosophy and Sociology, Bulgarian Academy of Sciences, Sofia, Bulgaria

ABSTRACT

Introduction: Cyber environment is a new type of interaction media that implies a modification of existing risks and a new type of risks, covered by an instrument for risk evaluation. **Materials and methods:** Existing risk evaluation instruments, psychology risk questionnaires and cyber risks categories. **Results**: Instrument for cyber risk evaluation with a specific modifications of the existing physical and psychological risks and the new type: cyber risks. **Discussion**: Cyber environment is new, yet already widely used and powerful. This creates an opportunity for improved functionality, but also for increased risk. **Conclusion**: The risk of using cyber environment is not limited to the field of information. It is a complex, personal, bio-psycho-social risk with daily and mass exposure and diverse consequences. Its assessment is difficult and currently inadequate in the direction of underestimation.

Key words: risk, cyber, psychology, philosophy of medicine

INTRODUCTION

Risk is the opportunity to bear harm or loss that measures the probability and potential impact of an unwanted event, thus the probability of something negative to happen and the potential consequences if it occurs. Severity is calculated as the product of frequency and severity of the event. Risk can be evaluated in a number of different ways, depending on the context and the available information, expressed as probability or percentage. Risk is also a fundamental concept in many areas, including finance, insurance, health and security. It is important to evaluate and manage risk to reduce potential harm or loss. This can include prevention or mitigation, such as risk assessment tools, or risk transfer through the means of insurance. Cyber environment is a work environment in which cybernetic technologies are leading. It is also used as a term denoting anything related to computers, the Internet and their derivatives. Cybernetics is defined by the ways information and informatics systems are managed, and data is processed by computing machines. Physical risk is a situation that has an unwanted contact with a source of energy that can lead to damage or injury to people or the environment. Mental risk is a condition that has the potential to destroy the mentation of people or society as a whole. Cyber risk is a condition or action that has the potential for unwanted or sudden release of, or contact with a source of change in information technology systems, networks, or data that may result in damage or impairment of information security to an individual or society. The degrees of control are always the same, and the measures are modified according to the specific situation. The control steps are: remove source, prevent unwanted change, protect yourself, and stop operation.

The purpose of this report is to summarize the risks to individuals who use cyber environment. Risks for the person in cyber environment can have physical, psychological, personal and social aspects and can range from mild discomfort to death.

An effort is made to build a taxonomy of operational cyber security risks that attempts to identify and organize them into four classes: 1.

***Correspondence to:** *Nikola Pirovski, Department of Anatomy, Faculty of Medicine, Trakia University, Stara Zagora, Bulgaria, e-mail: nikola.pirovski@trakia-uni.bg*

Actions of people, 2. Systems and technology failures, 3. Failed internal processes, and 4. External events. Each class is broken down into subclasses, which are described by their elements. This approach is only focusing on the protection of information [1].

While there have been efforts to understand the cost of cyber attacks, the impact of systemic risk spreading across interdependent systems, associated with cyber attacks, remains a critical problem in need of further study [2].

MATERIAL AND METHODS

The existing risk evaluation instruments, psychology risk questionnaires and cyber risks can be separated into categories. The methodology is a heuristic [3] formation of goals, systematic thinking [4] and testing within the holistic approach [5].

RESULTS

The physical, psychological and cyber factors contribute to the risk in cyber environment with specific features.

The physical factors include unhealthy lifestyle with a risk of obesity, heart disease and diabetes; repetitive strain injuries (RSI)) of the muscles, tendons and nerves that can be caused by repeating the same movements, such as typing or using a mouse, causing pain, stiffness and numbness in the hands, wrists, arms, shoulders, neck or back; eye strain, dry or tired eyes, blurred vision, headache or neck and shoulder pain. The heat from laptops in the testicle area and from headphones in the head area is enough to adversely affect the health of the organs in these areas. Headphones in the form of earplugs create excessive sound pressure and damage hearing, powerful speakers are harmful to the point of a sonic weapon. The blue light of the monitor simulates the sky in daylight, deceives the brain and leads to insomnia and disruption of biorhythms.

Psychosomatic health is affected in different ways manifested through the symptoms listed below: Psychomotor state: reclusiveness, lethargy, and neglect. Perceptions and representations: less concentration on perceptions, stunting of imagination and dreaming, delusional ideas. Will: hypobulia and impulsivity, rearrangement of values. Intelligence: loss of skills for analysis, synthesis, interpretation, comparison. Consciousness: time, place and social event data de-updating; avatar-centered autopsychic orientation. Thinking: circumstantial, reasoning, vulnerable to suggestibility. Memory: difficult fixation and amnesia. Caution: aprosexia, difficulty holding and switchability. Emotions: ambivalent from mania during use to dysthymia and asthenia with withdrawal. An inner feeling of elitism, euphoria, when the dysfunctions are revealed- astonishment, anger.

Cyber effects can also cause social isolation. The cyber environment competes with the real social environment and can lead to isolation with potential negative effects on an individual's mental health and well-being. Exposure to large amounts of information through multimedia can be overwhelming, trigger mental fatigue and impair an individual's ability to process and retain information. Cyberbullying, Identity Theft, Malware, Spam, Phishing, SQL attacks, DoS attacks and Hacking, are specific new risks only possible via cyber environment. **(Figure 1)**

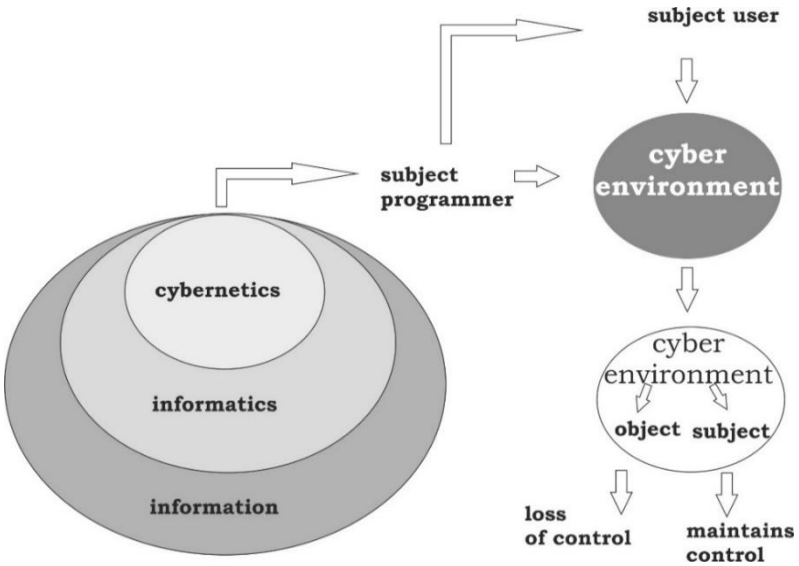

Figure 1. Cyber environment and the potential for loss of control and choice

DISCUSSION

Efforts to systematically advance the science of cyber risk must not only draw on computer science but also fields, such as behavioral science, economics, law, management, political science and many others, for a cross-disciplinary collaboration for each area [6]. Since it began offering cyber liability coverage in December 2011, the Texas Medical Liability Trust has received more than 150 cyber liability claims, most of which involved breaches of electronically protected health information [7].

Addressing cyber and privacy risks has never been more critical for organizations. While a number of risk assessment methodologies and software tools are available, they must be integrated into a holistic approach that combines several appropriate risk sources as input to risk mitigation tools for adequate Privacy Impact Assessment. Automated Cyber and Privacy Risk Management Toolkit addresses the above challenges by implementing and integrating three distinct software tools [8]. The term cybersickness is gaining popularity, however it was initially limited to a mix of symptoms including nausea, dizziness, fatigue and oculomotor [9]. There are significant effects of cybersickness on pupil size, cognition, psychomotor skills, and reading ability [10], which indicates that the syndromes associated with this problem are considerable.

CONCLUSION

Cyber environment involves a combination of physical, psychological and information hazards and brings new dimensions to risk. The various cyber risks can be summarized as follows: 1. personal - overload, isolation, depersonalization, devaluation; 2. hardware failure, 3. software failure, data loss, data theft, data modification, data misuse (financial or image); 4. blocking communication and social functioning. These possibilities are actively used for hybrid attacks. The mental changes resemble those characteristics of organic damage to the brain after the use of psychoactive substances, and are summed up in the syndrome of screen addiction, with apathetic and autistic personality changes, stripping of instincts and impulsivity similar to characteristics of mental retardation and dementia. In children, a differential diagnosis with autism is necessary. The most severe form of psychological risk is the screen addiction syndrome.

The risk of using cyber environment is not limited to the field of information. It is a complex, personal, bio-psycho-social risk with daily and mass exposure and diverse consequences. Its assessment is difficult and currently inadequate in the direction of underestimation. There are similar examples in the history of medicine, like the first introduction of the heroin to the public.

Cyber environment is a powerful tool for the transformation of society, which, with wrong social planning, could become a dangerous experiment.

Multimedia is highly addictive when used for entertainment or relaxation, and by immature individuals. This needs to be recognized, promoted and prevented.

Levels of control: 1. Remove the source - only for a limited part of the population, new strict regulations according to the risk assessment for others. 2. Prevent unwanted change- hard to offset in hybrid attack, need a robust real world standard of operation, 3. Protect yourself- use and recovery schedule, limited use, security devices and programs, new profession- cyber security guard, 4. Stop work - communication and busy information projects need maximum cyber security, what needs to be regulated is its use for entertainment and relaxation.

Slow social reaction, strong resistance to restrictions and weak control of the existing ones lead to a pandemic of screen addiction and massive cyber-fraud (deluge of madness). Out-of-control risk leads to accidents and the need to build and operate treatment and rehabilitation structures.

ACKNOWLEDGMENT

1. Project of the Medical Faculty of Trakia University №16/2022 Visualization of formal complexes in Wushu through graphic figures of their steps.
2. Contemporary Issues and Discussions in the Philosophy and Sociology of Medicine (2021-2024). Institute of Philosophy and Sociology. Bulgarian Academy of Sciences. Department Philosophy of Science. Project manager: assoc. prof. Julia Vasseva-Dikova

REFERENCES

1. Cebula, J. J., & Young, L. R., A taxonomy of operational cyber security risks. *Software Engineering Institute, Carnegie Mellon University*, 2010.

2. Welburn, J.W., Strong, A.M., Systemic Cyber Risk and Aggregate Impacts. *Risk Anal*. Aug; 42(8):1606-1622, 2022.
3. Gigerenzer, G., Gaissmaier, W., Heuristic Decision Making Center for Adaptive Behavior and Cognition. *Max Planck Institute for Human Development, 14195 Berlin, Annu. Rev. Psychol.*. 62:451–82, 2011.
4. Sandbrook, M., Systems thinking- so what? a first person view., *Science & Technologies*, Volume XI, Number 6: SOCIAL STUDIES, Systems Learning, Schumacher Institute, Bristol, UK., pp.15-19, 2021.
5. Feurer, R., Chaharbaghi K., Defining Competitiveness: A Holistic Approach. *Management Decision*, Vol. 32 No. 2, pp. 49-58, 1994.
6. Falco, G., Eling, M., Jablanski, D., Weber, M., Miller, V., Gordon, L. A., Wang, S., Schmit, J., Thomas, R., Elvedi, M., Maillart, T., Donovan, E., Dejung, S., Durand, E., Nutter, F., Scheffer, U., Arazi, G., Ohana, G., Lin, H. Cyber risk research impeded by disciplinary barriers. *Science*, 366(6469), 1066-1069, 2019.
7. Nuzback, K., Cyber crimes. *Tex Med*. Jul 1;110(7):27-33, 2014
8. Gonzalez-Granadillo, G., Menesidou, S. A., Papamartzivanos, D., Romeu, R., Navarro-Llobet, D., Okoh, C., Nifakos,. S, Xenakis, C., Panaousis, E., Automated Cyber and Privacy Risk Management Toolkit. *Sensors (Basel)*, Aug 15;21(16):5493, 2021.
9. Yang, AHX., Kasabov, N., Cakmak, YO., Machine learning methods for the study of cybersickness: a systematic review. *Brain Inform.* 2022;9(1):24.
10. Kourtesis, P., Amir, R., Linnell, J., Argelaguet, F., MacPherson, SE., Cybersickness, Cognition, & Motor Skills: The Effects of Music, Gender, and Gaming Experience. *IEEE Trans Vis Comput Graph*. Published online February 22, 2023.