Human Factors in Software and Systems Engineering, Vol. 140, 2024, 19–25
https://doi.org/10.54941/ahfe1005033

Human Factors in Hybrid Threat Risk Assessment

Maryna Zharikova[1,2] and Stefan Pickl[1]

[1]University of Bundeswehr Munich, Neubiberg, 85579, Germany
[2]Kherson National Technical University, Kherson, 73008, Ukraine

ABSTRACT

The goal of the paper is to propose a user-centered approach to create a hybrid threat risk model that considers human errors to complement traditional risk models and increases risk assessment accuracy. The authors consider a place of human factors in hybrid threat risk assessment and indicate that human factors influence human vulnerability, which is a component of hybrid threat risk. The proposed approach to creating a hybrid threat risk assessment model contains the following main components: a database of direct human factors, a database of human errors, a method of human vulnerability assessment, and a method of human-centered hybrid threat risk assessment. The proposed approach is based on the use of the neural network, which determines the correlation between the database of direct human factors and the database of human errors to assess human vulnerability. The outcomes of the research will be beneficial for making decisions regarding personnel management strategies aimed at strengthening human vulnerability.

Keywords: Hybrid threat, Critical infrastructure, Human factors, Hybrid threat risk, User-centered risk assessment, Human vulnerability

INTRODUCTION

As critical infrastructure (CI) systems become more secure, it is often easier for fraudsters to "hack" a person. "To do this, they come up with new and increasingly sophisticated methods of "social scams", and they manage to deceive not only ordinary citizens but even experts in their field.

Successful implementation of hybrid threats (HTs) is facilitated by the human factor, low level of safety culture, and untrained specialists. Employees are truly the most powerful internal risk factor for companies. The main source of threats is traditionally the corporate email service, but attackers also target websites, instant messengers, social networks, and telephony used by employees (Ronchi, 2022).

HT is aimed at using human factors (for example, gullibility) for an attacker's purpose. Human factors include a broad range of errors in judgment from policy formation to governance and risk assessment resulting in an inability to recognize threats in the environment (Bone, 2021).

This paper considers a novel approach to HT risk assessment from a human factor (HF) perspective. The paper proposes an approach to create a user-centered HT risk model, which complements traditional HT risk models to consider how HFs can increase the risk.

LITERATURE REVIEW

To study the influence of HFs on HT risk, it is necessary first to understand what is meant by HTs and HT risk.

According to the NATO (NATO, n.d) website: "Hybrid threats combine military and non-military as well as covert and overt means, including disinformation, cyber-attacks, economic pressure, deployment of irregular armed groups and use of regular forces. Hybrid methods are used to blur the lines between war and peace and attempt to sow doubt in the minds of target populations. They aim to destabilize and undermine societies".

In our paper HT risk is considered for a CI object that can be affected by HTs (vulnerable CI object) and is a potential for loss, damage, or destruction of vulnerable CI object caused by HTs.

In the literature, HT risk assessment is defined as a function of three main components: threat, vulnerability, and consequences.

The threat component includes the attacker's perspective such as the attacker's motives and goals to perform an attack, as well as their capabilities containing available information, technologies, skills, and delivery options that the attacker may use (Sheikh, 2022).

The vulnerability component includes technical and human vulnerability (Korelcki, 2020).

The consequences component includes loss of confidentiality as a result of the attack, accessibility of information resources, etc. (Ganin et al., 2017).

The components mentioned above may in turn be composed of other subcomponents (Ganin et al., 2017).

The most common existing methods of HT risk assessment evaluate these components either by experts or based on measurable statistics as a number between the certain minimum and maximum values, for example on a 0–10 scale. To aggregate the component scores into a final risk score the following approaches are used:

- the component scores are multiplied to calculate the risk level;
- the weighting sum of component scores is used (Ganin et al., 2017);
- the arithmetic mean of the component scores is used (Omotosho, 2019).

Most existing methods of HT risk assessment don't take into account human factors. Our research contributes to closing an existing research gap. The link between HFs and HT risk assessment is still not fully understood.

To investigate the influence of HFs on risk assessment, it is necessary first to understand what these factors are. In the literature, HFs are divided into direct and indirect.

Direct factors directly characterize human behavior, thereby having a direct significant impact on CI security. There are various factors including biological factors (e.g. age, gender, size, handicaps), physical condition, mental condition (apathy, stress), competence (experience, skills, security awareness), and personality (ignorance, negligence) (Alavi, 2013; Ganin et al., 2017). All these factors contribute to human performance.

Indirect factors entirely depend on external issues such as organizational issues but influence the direct factors. Indirect factors are beyond the person's direct control but can give motivation and opportunities for work (Block, 2015). These are such factors as adequate budget, culture, communication, security policy enforcement, human resource management policy, and management support (Alavi, 2013; Balfe, 2014).

Direct and indirect HFs can be managed to some degree by the organization to reduce HT risk. When analyzing past HA events, it is easier to track direct HFs' influence on CI objects' vulnerability than indirect HFs' influence. The dependency of direct HFs on vulnerability is usually more obvious. Indirect factors may not be as readily identified during an investigation of past HAs, as they tend to require a deeper level of analysis (Balfe, 2014). In our research, we take into account only direct factors.

Human factors can be positive or negative (Dul, 2010). For example, creativity, motivation, teamwork, communication, and leadership are all factors that can have a positive impact on human performance. However, bias, conflict, stress, burnout, and turnover are all factors that can have a negative effect. It's important to be aware of both the positive and negative human factors to ensure the success of your project. In this paper we consider negative factors increasing risk.

HFs can be unintentional or intentional (Wan Ismail, 2022). Unintentional factors include unconscious errors due to inattention. Intentional factors are associated with situations where CI workers act in conjunction with and in the interests of the attacker. Such factors could be the deliberate transfer of secret information to an attacker. In this paper, we dwell on unintentional factors that can be managed.

So, in this paper, we consider negative, direct, unintentional HFs in connection to HT risk assessment.

Block and Pickl (Block, 2014) distinguish some HFs influencing human performance. They use AMO (ability, motivation, and opportunity) theory according to which the performance of an individual is a function of ability, motivation, and opportunity to perform the job. In (Block, 2014) the ability is understood in a broader sense as knowledge, skills, and abilities (KSA).

In (Alefari, 2020) the factors of human performance are extended. AMO are treated as the main factors of human performance, but there are also secondary factors that impact employee performance through the main factors.

Some works are investigating the influence of HFs on human performance. (Jamshidi, 2021; Lázaro et al., 2024). However, at present there is almost no work considering the influence of HFs on HT risk assessment. This paper attempts to shed some light on this issue.

HUMAN FACTORS IN HYBRID THREAT RISK ASSESSMENT

Fig. 1 shows TH risk components based on the literature review above and the place of HFs in HT risk assessment. HFs influence human vulnerability, which is a component of HT risk.

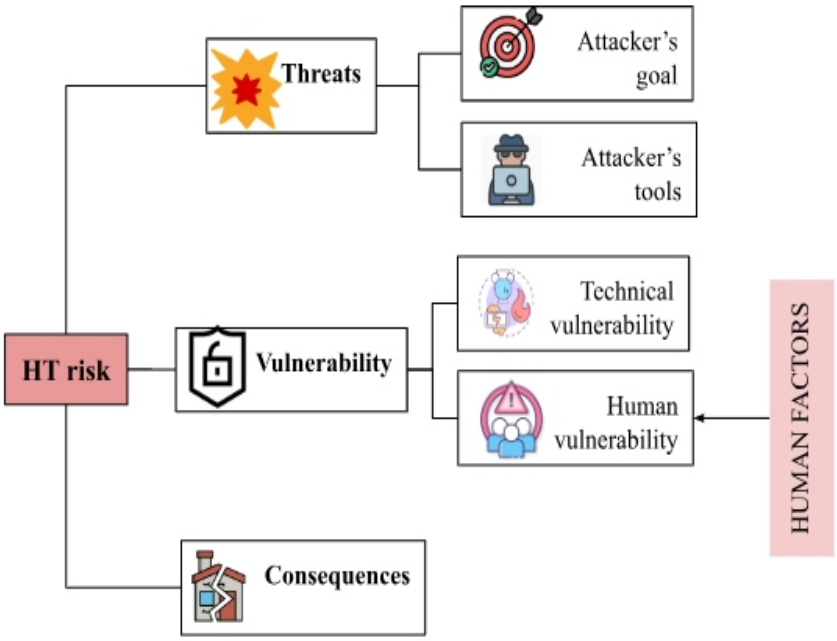

Figure 1: Hybrid threat risk components.

As HT risk is considered for vulnerable objects affected by HTs, then the components connected with the vulnerability of these objects and the consequences for them will be considered as internal risk components, and the components connected with the threats will be considered as external risk components.

We can manage only internal risk parameters to reduce risk, but we can not manage external parameters related to the attacker. One of the ways to manage internal risk parameters is by influencing HFs (for example, by increasing the level of staff competence through various workshops and trainings), which can reduce human vulnerability, and therefore HT risk.

Taking into account that vulnerability can be technical and human (Fig. 1), it can be concluded that the security of CI is not solely a technical problem, it also depends on humans who use the system and behave a certain way within the system environment. HFs need to be considered in HT risk assessment. Still, the task is challenging as it is difficult to quantify the factors, which are often uncontrollable, into a measuring scale (Alavi, 2013).

HFs in risk assessment are about considering where people's actions could go wrong leading to serious consequences, the factors that make this more likely, and how to reduce risk. Managing HFs is understanding their influence on risk and timely decision-making. The risk assessed taking into account HFs will be further called human-centered HT risk.

HUMAN-CENTERED HYBRID THREAT RISK ASSESSMENT

We propose an approach to human-centered HT risk assessment based on a method of human vulnerability assessment. The main components of the proposed approach are the following:

- Database of direct HFs (HFDB);
- Database (DB) of errors;
- Method of human vulnerability assessment;
- Method of human-centered HT risk assessment.

HFDB is collected separately for each vulnerable CI object, representing information about the background of personnel (education, experience, skills, etc.) servicing this object.

DB of errors is also collected separately for each vulnerable CI object, representing retrospective information about the errors of personnel leading to failures of this object.

It is obvious that direct HFs, information about which is contained in the HFDB, influence the number, frequency, and severity of the errors, information about which is contained in the DB of errors. The number, frequency, and severity of the errors, in turn, reflect the human vulnerability of the CI object being internal HT risk factors.

The proposed method of human vulnerability assessment for a certain CI object consists of the following steps:

1) Processing DB of errors and obtaining the generalized indicators such as the frequency in time of the errors, level of their negative influence on the CI object, etc.
2) Determining the correlation between direct HFs from HFDB and generalized indicators obtained from DB of errors.
3) Determining the probability of the errors based on the dependency obtained in the second step (this probability is converted then into a human vulnerability assessment).

To get the correlation in the second step we propose to use a neural network (NN) (Fig. 2). The input for the training data set (DS) contains direct HFs, and the output for the training DS is the generalized indicators of the errors obtained in the first step of the method of human vulnerability assessment.

The trained NN allows us, knowing the direct HFs, to determine the probability of error, and therefore human vulnerability of CI object.

The proposed method of human-centered HT risk assessment consists of the following steps:

1) Assessment of probability (possibility) of HA;
2) Assessment of the vulnerability of CI object;
3) Assessment of consequences;
4) Assessment of human-centered HT risk.

The first three steps provide an assessment of risk parameters. In the fourth step, the human-centered HT risk is represented as a point in a three-dimensional parameter space and to assess the risk, we propose the approach described in (Pickl, 2023).

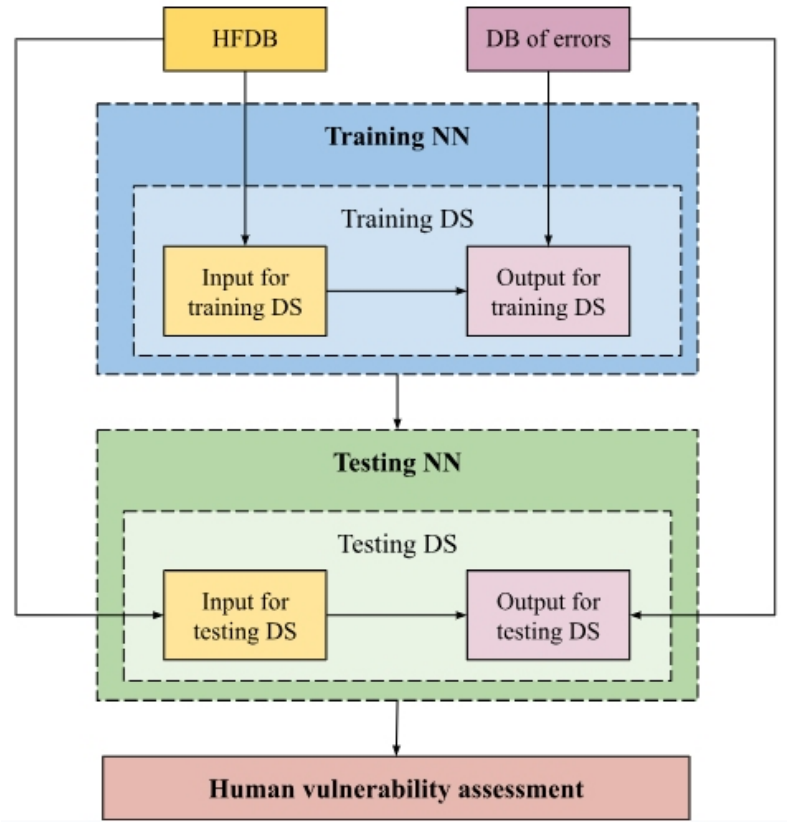

Figure 2: Neural network-based method of human vulnerability assessment.

CONCLUSION

The functioning of CI is influenced by HFs that increase the vulnerability of CI objects. In the presented work, we propose an approach to assess the influence of these factors on HT risk. The proposed approach is based on the use of the NN, which determines the correlation between HFDB and DB of human errors to assess human vulnerability. This assessment is considered as one of the HT risk components. The outcomes of the research will be beneficial for making decisions regarding personnel management strategies aimed at reducing the negative impact of direct HFs on the human vulnerability of CI objects to HTs.

As a future work, we are going to develop a decision support system based on human-centered HT risk assessment to reduce human vulnerability.

REFERENCES

Alavi, R., Islam, S., Jahankhani, H., Al-Nemrat, A. (2013) Analyzing Human Factors for an Effective Information Security Management System. International Journal of Secure Software Engineering, 4(1), doi: 10.4018/jsse.2013010104.

Alefari M, Almanei M, Salonitis K. A System Dynamics Model of Employees' Performance. Sustainability. 2020; 12(16):6511. https://doi.org/10.3390/su12166511

Balfe, N., Leva, M. (2014). Human factors analysis in risk assessment: A survey of methods and tools used in industry. Contemporary Ergonomics and Human Factors 2014. 77–84.

Block, J., Pickl, S. The mystery of job performance: A system dynamics model of human behavior. In Proceedings of the 32nd International Conference of the System Dynamics Society, Delft, The Netherlands, 2014; Curran Associates, Inc.: Red Hook, NY, USA, 2015.

Bone, J. and Kachroo, G. (2021). Human Factors A Cognitive Risk Framework for Cybersecurity and Enterprise Risk Management National Science Foundation Senior Personnel. Research Proposal · August 2021 doi: 10.13140/RG.2.2.29337.54887.

Dul, J, Human Factors: Spanning the Gap between Om & Hrm (2010). ERIM Report Series Reference No. ERS-2010-020-LIS, Available at SSRN: https://ssrn.com/abstract=1619693.

Ganin, A. A., Quach, P., Panwar, M., Collier, Z. A., Keisler, J. M., Marchese, D., and Linkov, I. (2017) Multicriteria Decision Framework for Cybersecurity Risk Assessment and Management. This article is a U.S. Government work and is in the public domain in the USA. doi: 10.1111/risa.12891.

Jamshidi, R., & Sadeghi, M. E. (2021). Neural network based human reliability analysis method in production systems. Journal of applied research on industrial engineering, 8 (3), 236–250.

Korelcki, Z., ADÁMKOVÁ, B. (2020) Human Factor Failure in Hybrid Warfare and its Impact on Airport Security. Proceedings of 2nd International Conference CNDGS'2020.

Lázaro, F. L., Nogueira, R. P. R., Melicio, R., Valério, D., Santos, L. F. F. M. (2024) Human Factors as Predictor of Fatalities in Aviation Accidents: A Neural Network Analysis. Appl. Sci., 14, 640. https://doi.org/10.3390/app14020640

NATO. n.d. Countering Hybrid Threats. Last updated August 18, 2023, https://www.nato.int/cps/en/natohq/topics_156338.htm#:~:text=To%20deter%20hybrid%20threats%2C%20NATO,its%20deterrence%20and%20defence%20posture.

Omotosho, A., Haruna, B. A., Olaniyi, O. M., Omotosho, A., and Ayemlo B. (2019) Threat modeling of Internet of Things health devices, J. Appl. Secur. Res., vol. 0, no. 0, pp. 1–16.

Pickl, S.; Zharikova, M.; Barbeito, G. (2023) Reliability Modeling with Industry 4.0 Reliability and risk analysis in critical infrastructure protection. Elsevier 35–43.

Ronchi, A. M. (2022). Human Factor, Resilience, and Cyber/Hybrid Influence. Information & Security. Volume 53, No. 2.

Sheikh, Z. A. and Singh, Y. A. (2022) A hybrid threat assessment model for security of cyber physical systems. 7th international conference on parallel, distributed and grid computing.