systems

MDPI

Article

The Influence of Threat Development on the Failure of the System's Symmetry

Ladislav Maris, Zuzana Zvakova *, Katarina Kampova and Tomas Lovecek

Faculty of Security Engineering, University of Zilina, 010 26 Žilina, Slovakia; ladislav.maris@fbi.uniza.sk (L.M.); katarina.kampova@fbi.uniza.sk (K.K.); tomas.lovecek@fbi.uniza.sk (T.L.)
* Correspondence: zuzana.zvakova@fbi.uniza.sk

Abstract: The existence or non-existence of a threat to a system is essential for its existence or essential for the functionality of the system. Even more crucial is the potential of the threat and its development, which leads to the failure of the symmetry of the system. What influences the development of such threats? What contexts influence the evolution of system threats? The development of threats is linked to the changing values of indicators that affect the state of the threat at a certain point in time. This development takes place in a constantly changing environment, therefore it is dynamically and causally linked. The system aims to maintain its order, however, the influence of the development of threats deflects it towards the entropy of the system. The paper is focused on the identification of the phases of the development of threats and their impact on the symmetry of a system. The paper presents a theoretical view of the impact of threat development on system symmetry failure.

Keywords: threat development; entropy; causality; threat level; system failure; system's symmetry

Citation: Maris, L.; Zvakova, Z.; Kampova, K.; Lovecek, T. The Influence of Threat Development on the Failure of the System's Symmetry. *Systems* **2021**, *9*, 74. https://doi.org/10.3390/systems9040074

Academic Editors: Yoshiki Shimomura and Shigeru Hosono

Received: 10 September 2021
Accepted: 18 October 2021
Published: 20 October 2021

1. Introduction

The concept of security is a common aspect of every language. Every individual has some general idea of what security means. However, in a professional context, the term security, despite the large body of literature, is often used intuitively or ambiguously, which causes the discussion to often suffer from considerable uncertainty. The versatility of the use of this term causes its eclectic interpretation. In various electronic reference books on security, more than 50 thousand connections with the word "security" or "safety" can be found [1,2].

In English-speaking countries, the term security is considered primarily a synonym for the reliability of the defense of traditional values, the defense, and, where appropriate, the promotion of vital interests. This understanding primarily applies to the state, state interests, and its goals. In the German sense, security is understood rather as an emphasis on securing values in a particular social system from external as well as internal threats. From the French point of view, it is primarily a matter of ensuring a state of rest in which there is no risk [3,4].

Security can be seen as a status or level of symmetry. The symmetry of the system is typical for its dynamics. This means that at the time when there are changes, there is also oscillation around the state of symmetry. Movement and development are part of the existence of the system, as well as its structure, relations, and functions. For this reason, we can define security as the guarantee of the symmetry of the here and now, but also its future, thus guaranteeing the development and movement [5]. This does not only apply to the term security, but also to the term safety. Safety means, mainly, accident avoidance, and it is the condition of not being in danger or of not being dangerous [5,6]. Ensuring the symmetry of the system is to ensure effective protective or defensive measures, regardless of the nature or origin of possible security threats. The article is focused on security, although the principles stated in it can also be modified for safety purposes.

Risk assessment has become an essential mechanism for enterprise security analysts by enabling the identification and evaluation of any threats, vulnerabilities, and risks to which organizations may be exposed [6]. Security assessment is the work of many authors, who mainly focus on individual methods and procedures by which they assess the level of risks or threats to selected objects. [7–9]. In the field of security, the method of fuzzy logic (fuzzy model) is well known for its probabilistic character, which can be applied to estimate the future development of risks [10–16]. Another important method is game theory and its application in various studies examining the level of security or defining various scenarios of the development of the threat of potential risks using e.g., Bayesian functions [17–20], or other statistical distribution and exponential distribution in the planned security risk scenario [21]. Risk assessment is applicable across the whole spectrum of security objects, whether there are threats to physical objects [22–24], information systems, or other financial systems [25].

In our paper, we address the area of security with a more comprehensive approach to understanding the evolution of threats beyond traditional security assessment, although it can be applied in a broader sense. The theory of threat development is more or less addressed in publications that focus on the interconnectedness of theory and best practice [26]. Other models offer another comprehensive view of security sciences in terms of possible security models and their basic principles [27]. Unique approaches to security research from the point of view of its essence are also beneficial, i.e., ontological approaches to security research [28]. For example, for the development of security from the point of view of environmental protection, the contribution of environmental protection and its sociological character is beneficial [29,30]. By analyzing these approaches, we have concluded that, simply by examining ontological concepts that allow the creation of general models of threat development, we can correctly apply the mentioned methods designed for the detailed assessment of security levels, especially in terms of possible development.

The existence or non-existence of a threat to a system is essential for its existence or essential for the functionality of the system. The inspiring guide offers a solution to the theory of security of information systems, namely a model of the theory of the development of insider risks, in which it also analyzes the decision signals in terms of simulations of activated threats [31]. Even more crucial is the potential of the threat and its evolution, which leads to the failure of the symmetry of the system. What influences the development of such threats? What contexts influence the evolution of system threats?

2. Materials and Methods

The main goal of the article is to present and describe a unique approach to examining the evolution of threats. The advantage of this approach is that it can be applied to the widest possible field of security objects, therefore it is a general model.

To ensure the complexity of the article, the first step in the process has been a thorough study and analysis of previous studies and publications. These were areas of security theory, securitology, prevention, and security incident resolution. In particular, the following key words were used to search for references: accident, theft, robbery, security system, security risk, security threat, security management, information security, business resilience, symmetry, system, security, and safety. The basis for the elaboration of the article was a total of 36 scientific and professional studies and publications from 2005 to 2021. In processing the article, we used 13 outputs published in the journal Symmetry Journals MDPI, as well as other publications included in the citation databases Web of Science and Scopus. Part of the initial work was focused on specific areas of security. These were mainly in management, risk management, IT, transport, and sociology. However, their focus was not an obstacle. The variability of the initial knowledge was positively reflected in a universal approach to understanding and better defining the symmetry of the system, and the process of development and the impact of security threats on it.

An important aspect of the study of system symmetry in terms of system threat is the ontological approach and an attempt to describe in general terms the loss of symmetry and,

conversely, the emerging asymmetry in the event of a system threat development. The need for a general understanding makes it possible to maintain basic concepts and subsequent application in specific models or more specific methods, e.g., risk assessment methods, risk development estimation methods, etc. A security threat is a specific, physically existing object, phenomenon, event, or process that can cause damage or injury. In the broadest sense, this refers to everything dangerous to the organization which could negatively change the level of its security. We also indicate threat events and phenomena that can occur in a relatively short time or have already occurred and can cause dramatic changes in the conditions of the existence of the reference object [32]. The term threat is often associated with the term danger—a phenomenon with the ability to harm a protected interest. Then, we can consider these two concepts as synonyms. In a simpler understanding of the term, we come from the definition of the IT security environment, whereby security threat means the potential cause of an adverse event that results in damage to the system and its assets. We cannot understand the threat (its existence and its development) within limited limits. The threat exists in an environment where relationships and ties exist. Such a dynamic system (environment) is influenced by various factors, e.g., objective and subjective factors, natural, human, and technical factors, cultural, political, legal, and economic factors, and others. Then, the study of the development of threats depends on the knowledge of many scientific disciplines, both natural, technical, and social. The law of causality stipulates that each event phenomenon necessarily has at least one cause, while the event as a consequence of the action of the cause becomes the cause of, respectively, other events and consequences. This makes it possible to accept a claim about the determining relationship between phenomena and events, not only in the past or in the present, but also in the future [33]. The basic accompanying phenomenon of causality is the time shift of the occurrence of the consequence (effect), i.e., the reaction to the action (cause). According to the laws of nature, reactions cannot occur simultaneously with action, and a reaction cannot occur earlier than an action.

The development of threats is conditioned by factors in a given environment and time. In terms of the possible development of the threat, we recognize 2 basic types of factors that cause a change in the state of the threat.

- Permanent factors that fundamentally and, especially in the long run, affect the state of threat. It is possible to predict them and thus predict the impact on the state of threat. These factors are relatively constant with few dynamics of change.
- Temporary factors have the potential to cause a change in the threat status in a shorter period. They act on threats dynamically and change their attributes, which have a dynamic effect on the security of the reference object. These conditional factors act unexpectedly on the threat level. The occurrence and impact of these factors are more difficult to predict and may be latent.

At the same time, a causal relationship of interaction applies. Volatile factors may be due to the long-term activity of persistent factors or persistent factors may be due to the activity of temporary factors. The result of these factors can be accelerating or retarding, i.e., they accelerate or slow down the development of the threat (Figure 1).

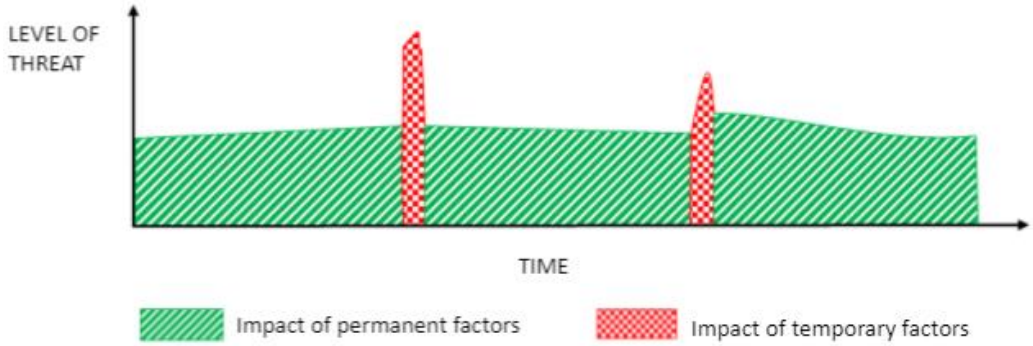

Figure 1. Effect of permanent and temporary factors on the degree of threat over time.

Factors (parameters) acquire certain values at a given place and time. If these values reach a critical limit (critical threshold), they will significantly affect the degree of threat, and they can even trigger a cascade effect (snowball effect). If one factor acquires a critical value, it affects the other factor, which, when it reaches a critical value, affects the third factor, etc., resulting in an extreme change in threat. At the same time, it may be the case that the combination of selected factors in certain values may represent a change in the value of the threat, while the individual values of the factors may not reach a critical value, but their combination may allow this change.

The critical (threshold) value of the factor describes such a situation in which the factor occurs at the equilibrium threshold. This situation may or may not be reversible. The critical (threshold) value indicates the state when the observed phenomenon reaches the limit value.

For critical values in the fields of technology, in technical systems, the critical values of the factors of various elements or whole systems can be expressed by the numerical value of the monitored parameter. Then, changing this parameter (exceeding, decreasing) can mean the transition of the system from the state of failure to the state of accident, catastrophe, etc. We can use these critical values in a technogenic environment to express the reliability of technical elements or systems. In the environment, critical values can be used, for example, to assess the risk of toxic substances in the air, the environmental sustainability of the environment, etc. [34].

Approaching these values to these critical values increases the likelihood of the threat moving to a new state, which may pose an increased level of security threat.

Knowledge of the values of critical thresholds of factors is important to ensure a timely response and the prevention of critical situations that can lead to e.g., to escalating the voltage or even destroying the system, i.e., to activate the threat in a state which disturbs the security of the reference object.

An important step is the correct and timely identification of these factors and their critical values, which are associated with problems, in particular:

- selection of factors (relevance, adequate number);
- selection of critical (threshold) values of these factors (their parameters);
- selection of analytical method, e.g., comparative analysis;
- selection of prognostic method, e.g., forecast of value development, development scenarios, dominant factor and its dominant parameter, etc.

The perception of entropy (uncertainty, disorder) in physics is also appropriate to apply to the field of security and safety. Entropy is a function of disorder because it correlates with the random and fluctuating motion of the elements of the system (the security environment). An example could be increased "movement" in the security environment, the growth of social conflicts and tensions in the countries causes the elements to "vibrate" and more random movement begins–entropy grows in the environment. This perception is, according to [35], a new perception of the design role of entropy as a new paradigm of security research.

Based on these facts, we define the phases of security threats that have a major impact on the overall symmetry of systems.

3. Results

The security threat evolves and goes through the various stages of its existence. The dynamics of the security threat and its effect on the symmetry of the system can be determined by the development stages and the moments of change. The stages of a security threat are determined by the degree of the potential of the security threat, the action of permanent and unstable factors of the security threat, and factors of the security environment of the reference object. The moment of change expresses the change in the potential of the security threat, i.e., the change in the state of the factors of the security threat to the security environment. The transition of the development stage to the moment occurs when the symmetry of the system changes.

The course of the security threat can be divided into three phases and three moments. These describe key milestones that have a significant impact on the level of security threat potential and system symmetry breaches.

We do not include the period before the security threat occurs in the development stages of the threat. It is a period when the threat does not exist, therefore its potential level is zero. This means that there is no source of the security threat or its bearer, or that it exists but cannot adversely affect the symmetry of the system.

1. The moment of the threat.

The moment of occurrence of a security threat can be determined by the creation or emergence of a source or carrier of the security threat, which has the ability or can gradually acquire the ability or motivation to act negatively on the symmetry of the system.

2. The threat formation phase

The security threat formation phase is the period in which the existing security threat, characteristic of its bearer, acquires the potential to have a negative effect on the symmetry of the system. The potential of a security threat is dynamic and, as a rule, its level changes only after the moment of the occurrence of a negative event. Its level (in individual phases of torque) depends on the ability of the security threat carrier to be motivated.

3. The threat activation point

The moment of activation expresses the specific point from which the security threat is considered active. This moment is characterized by the achievement of threat factor thresholds. Activation can be intentional or unintentional by the threat holder. A trigger or event occurs here. In activating the security threat, the symmetry of the system is already broken. This disruption of symmetry can be latent and its manifestations can be detected only over time, together with the negative impact of the security threat during the threat phase.

4. The threat effect phase

The security threat phase is a period when an activated security threat adversely affects the symmetry of the system. This phase may give the impression that it does not cause a negative consequence; however, the very activation of the security threat and its effect is negative for the symmetry of the system. The action of a security threat probably causes small-scale damage, hidden damage, or damage that will only become apparent over time, e.g., leakage of information, harmful effects of chemicals on human health, etc. The effect of the security threat is characterized by a deepening imbalance in the system, which leads to the emergence of asymmetry of the system.

5. The incidence formation point

The incidence formation point is a specific point when there is a degree of imbalance in the system, which leads to a failure of the symmetry of the system. From the moment that a negative event occurs, it is no longer possible to reverse the initiated event. From this

point on, it is only possible to apply measures to mitigate the harmful effects of the negative event, and thus it is possible to act on the asymmetry that has entered so that it does not deepen or so that its consequences are minimal.

6. The incidence effect phase

During the incidence effect phase, the potential of the security threat decreases. However, the course of a negative event and the events associated with it can result in the emergence of additional threats and thus cascade to the emergence of partial asymmetries. By interfering with the action of a negative event, it is possible to mitigate the negative consequences and create conditions for the return of the new symmetry of the system. Without intervention, irreversible damage to the system can occur.

The length of the development phases of a security threat is influenced by the action of permanent and unstable factors of the security threat as well as by the factors of the security environment of the reference object. The course of security threats may be relatively constant or may have a more or less steep course of ascent or descent during the individual phases. Figure 2 shows the possible course of a security threat.

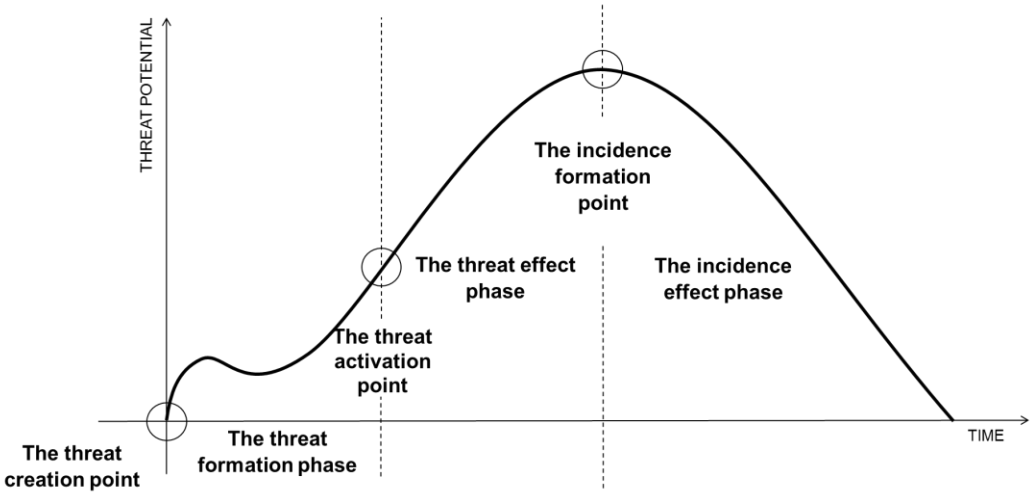

Figure 2. Example of a graphical representation of the course of security threat phases.

Example of the text representation of the threat phases

- The threat creation point—recruitment of an employee into an employment relationship;
- The threat formation phase—the employee moves into the company, and legally and legitimately obtains information, e.g., on the system of protection. The harmful potential of an employee as a carrier of a security threat is growing. This gives the employee the ability to cause damage to the company;
- The threat activation point—indicates a point or event that triggers a security threat, e.g., deterioration of the employee's financial situation, dissatisfaction with working conditions, or detection of deficiencies in the company's security. It is possible to assume a reduction in the level of employee loyalty;
- The threat effect phase—in this case, it can manifest itself in the targeted acquisition of information about the company;
- The incidence formation point—occurs when an employee provides information about a business to a third party, e.g., to make a profit or for personal revenge. A security incident has already occurred, the information has leaked, but the company does not know about it yet and the leak of information has not yet manifested itself;
- The incidence effect phase—the phase in which the leakage of information manifests, e.g., deterioration of the company's position on the market, damage to goodwill, or theft in the company, if the leaked information affected the object protection system.

This example subsumes the human factor, as a weak link threatening the symmetry of the system, inappropriate regime measures, and information security. If we focus exclusively on security, it is possible to cite as an example the neglect of the role of physical protection in the system of object protection.

- The threat creation point—it may be inappropriate to set criteria for the selection of a physical protection provider with emphasis on eligibility with regard only to the lowest price for the service;
- The threat formation phase—for example, the performance of physical protection by persons who are not sufficiently professionally, physically, or mentally competent;
- The threat activation point—detection of inappropriate or insufficient physical protection by potential perpetrators;
- The threat effect phase—can be manifested by monitoring the physical protection mode, finding weak points in the mode, and aiming to attack the object;
- The incidence formation point—an attack on an object using knowledge of the shortcomings of the performance of physical protection;
- The incidence effect phase— the attack itself and the consequent loss or damage that is caused to the protected interest.

Security threats can act in the reference object for a long time, in a hidden way, and with a high degree of potential security threat; they have a negative effect.

The course of a security threat must always be perceived concerning a particular system and its symmetry in a particular situation. These stages of the existence of a security threat can also be referred to as the security threat life cycle. The security threat does not necessarily go through all stages of development. Under the influence of factors of the internal and external security environment of the system, the following may occur [36]:

- The course of all development phases of the security threat, the emergence and impact of a negative phenomenon;
- To detect and mitigate (secure) a security threat to a security threat with minimal potential;
- To detect and eliminate a security threat, its source, carrier, motivation, and ability to act negatively.

This can be achieved by:

- Implementing measures to ensure the early detection of an emerging (formed), activated, and/or already existing security threat;
- Using measures that have an impact on the ability of the security threat to act negatively on the reference object;
- Using measures that have an impact on the motivation of the security threat holder.

At the point of origin of the system's asymmetry, the security threat can be detected and treated, but also re-created, shaped, and activated. If a security threat is present in the system, then when it is detected and treated, the development of this security threat must return at least until the moment of activation. In the event of a negative event and its effect, it is no longer possible to treat the threat, but it is possible to act to minimize the harmful consequences (Figure 3).

Security threats are always cyclical, the occurrence of which is connected with another cycle (e.g., with a specific phase in the production process). Repeating this cycle repeats the security threat.

Security threat identification is based on the search, identification, and naming of unwanted negative events and unwanted phenomena—consequences that can damage the symmetry of the system and identify their causes.

The ideal moment for the identification of a security threat, concerning ensuring the required degree of symmetry of the system, is the period before its occurrence as well as the phase of origin and formation of the security threat. To ensure that the threat is identified at these stages, it is crucial to provide sufficiently detailed information about the security situation as well as the external and internal factors of the system's security environment.

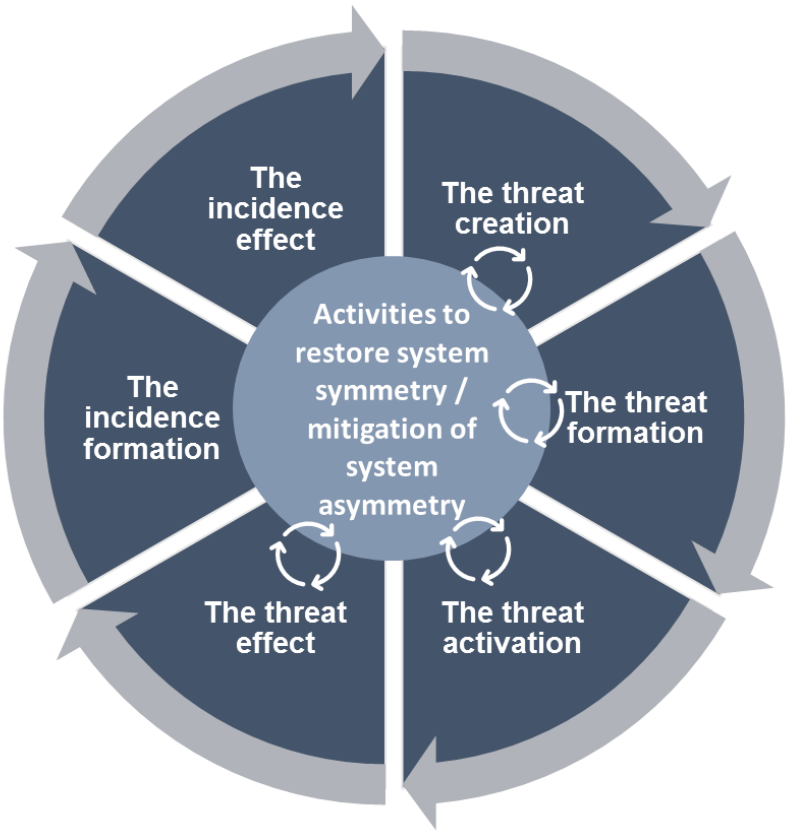

Figure 3. Cyclicality and dynamics in the developmental phases of a security threat.

Security threats that are detected after activation can be addressed. There is a possibility that activated security threats, regardless of the degree of harmful potential, despite detection, will not be possible to stop or it will not be possible to completely reverse their negative impact. This means that the asymmetry of the system occurs, but its extent or size will be smaller.

Examples include threats associated with the loss of sensitive data (personal data, know-how, trade secrets, inside information, etc.). If there is a hacker attack on the information system (enterprise), this attack can be hidden for a long time (in the operation phase) and can gradually collect interest information, access, and competencies without the knowledge of the information system administrator. When an attack is detected, sensitive data may not be disclosed, misused, or provided to an unauthorized person, so the planned negative event and the intended action will not occur to the attackers. The fact that the security of the information system has been compromised and that information may have leaked creates a sense of insecurity and damages the company's reputation, despite the detection of a security threat and the prevention of a negative event.

4. Discussion

If a negative event occurs, the security threat that caused it usually ceases to exist. Its life cycle ends with the occurrence of a negative event and its action. However, a negative event does not exclude the emergence of a new security threat with a seemingly identical source. The new security threat may be of the same nature as the security threat that was terminated. The difference between threats is in the security situation, in the security environment, in the time of action, and the state of readiness of the reference object and thus also in the duration of individual phases of the security threat, speed of onset of the threat, and potential for the threat to cause asymmetry. Newly regained equilibrium—new symmetry is another system that may (but need not) be complemented by experience with a security threat whose life cycle has been completed.

The transition of the system between the states of symmetry and asymmetry, the course of the security threat and its cyclicality, and the degree of effectiveness of measures to reduce the size of asymmetry are areas that provide space for professional and scientific discussion as well as further research. Space for further research provides the penetration of these areas in the form of examining the applicability of various measures in the various stages of security threat development and the degree of effect on the security threat and protection of the system against asymmetry.

By applying our approach in examining the ontological nature of threat development, we assume that the existing methods of threat assessment, with regards to risks, meets the basic perception of threats to the assessed reference object of its possible development (maintenance of symmetry or direction to the collapse of the system (state of asymmetry)) or not exceeding this limit (maintaining the symmetry of the system).

For a broader discussion, the applicability of the symmetric model is at a general level. We assume that our perception of the reference object as a system and the effect of threats (risks) on this system (reference object) has its ontological justification. We believe that, by applying, for example, to specific threats (e.g., the development of the security risk of a cyberattack on an information system), we will better understand and thus better contribute to the perception and essence of security of the assessed system.

The authors, whom we mentioned especially in the first chapter, more or less address the issue of assessing threats and risks, designing methods for dealing with these risks, and describing the nature of relationships within the perception of system symmetry, system development dynamics, etc. We hope that our contribution will support a better understanding of the assessment of the current state of reference objects in terms of their stability of existence and timely action against system crashes.

Further basic research or application solutions will be beneficial and can confirm and partially supplement the ontological understanding of system security in terms of perception of its symmetry.

5. Conclusions

The development of threats is linked to the changing values of indicators, the values of which affect the state of threat. The evolution of threats is therefore dependent on these indicators and a causal relationship is established between cause and effect. Because this development takes place in a dynamically changing environment, the threats themselves are part of this environment, and, therefore, we perceive them as dynamic. Interesting is the so-called entropic view of the development of threats, which is related to the arrangement or non-arrangement of risk factors. Each threat can be in a different state, which is, for us, important for the reference object. We can describe and identify this state within the development of the threat to the so-called phases of the course. The individual phases can be changed or repeated. By identifying, assessing, and anticipating the development of threats, we can effectively influence the level of security.

In our paper, we address security with a broader approach to understanding how threats evolve beyond traditional security assessments, although they can be applied in a broader sense. The theory of threat development is more or less addressed in publications that focus on networking theory and best practices. Current approaches to security assessment focus primarily on the evolution of the risk and not on the evolution of the threat as such. The broader context needs to be taken into account. The authors, which we also mentioned especially in Chapter 1, focus mainly on risk and assessment in a narrower context. Our approach is more ontological.

Finally, it is worth noting that high-quality and effective threat management (if possible) is a starting point and an integral part of effectively strengthening the resilience elements of reference objects to these threats. The strengthening of the complex elements of the system's resilience depends on the level of control and the availability of the necessary resources. In a broader context, however, resilience should be considered a necessary aspect of threat management with regards to overall risk management, which significantly

contributes to minimizing losses or minimizing the failure of the symmetry of the system and the consequent adverse impact on society or the selected organization.

Author Contributions: Conceptualization, L.M., Z.Z., K.K. and T.L.; methodology, L.M. and Z.Z.; validation, K.K., T.L. and L.M.; formal analysis, L.M.; investigation, L.M. and Z.Z.; resources, L.M. and Z.Z.; data curation, K.K.; writing—original draft preparation, L.M. and Z.Z.; writing—review and editing, K.K. and T.L.; visualization, Z.Z.; supervision, L.M. and K.K.; project administration, T.L.; funding acquisition, K.K. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by The Ministry of Education, Science, Research and Sport of the Slovak Republic and Slovak research and development agency grant number APVV-20-0457 Monitoring and Tracing of Movement and Contacts of Persons in Medical Facilities.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data sharing is not applicable to this article.

Acknowledgments: The article was supported by The Ministry of Education, Science, Research and Sport of the Slovak Republic and Slovak research and development agency grant number APVV- 20-0457 Monitoring and Tracing of Movement and Contacts of Persons in Medical Facilities.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Murzda, K. Bezpečnosť: Teoretická konštrukcia a sociálny systém. In *Bezpečnostní Teorie a Praxe (Security: Theoretical Construction and Social System*; Policejní akademie České republiky v Praze: Praha, Czech Republic, 2005; p. 249.
2. Ivančík, R.; Baričičová, Ľ. Gnozeologické pramene skúmania bezpečnosti v 21. storočí. In *Policajná Teoria a Prax (Gnoseological Sources of Security Research in the 21st Century*; Policejní akademie České republiky v Praze: Praha, Czech Republic, 2020; pp. 20–46.
3. Porada, V. *Bezpečnostní Vědy*; Vydavatelství a Nakladatelství Aleš Čeněk, s.r.o.: Plzeň, Czech Republic, 2019; p. 780.
4. Mušinka, M. Možnosti hodnotenia bezpečnostných hrozieb. In *Vojenské Reflexie*; Akadémia ozbrojených síl generála M. R. Štefánika: Liptovský Mikuláš, Slovakia, 2020; Volume 1, pp. 82–98.
5. Siser, A.; Maris, L.; Rehak, D.; Pellowski, W. The use of expert judgement as the method to obtain delay time values of passive barriers in the context of the physical protection system. In Proceedings of the 52nd Annual IEEE International Carnahan Conference on Security Technology (ICCST); International Carnahan Conference on Security Technology Proceedings, Montreal, QC, Canada, 22–25 October 2018; pp. 126–130.
6. Titko, M.; Luskova, M. Analysis of Risks Associated with Transport Infrastructure Elements Failure due to Extreme Weather Events. In Proceedings of the 20th International Scientific Conference Transport Means, Juodkrante, Lithuania, 5–7 October 2016; pp. 207–212.
7. Anysz, H.; Apollo, M.; Grzyl, B. Quantitative Risk Assessment in Construction Disputes Based on Machine Learning Tools. *Symmetry* **2021**, *13*, 744. [CrossRef]
8. Seo, S.; Kim, D. Study on Inside Threats Based on Analytic Hierarchy Process. *Symmetry* **2020**, *12*, 1255. [CrossRef]
9. Madžarević, A.R.; Ivezić, D.D.; Tanasijević, M.L.; Živković, M.A. The Fuzzy–AHP Synthesis Model for Energy Security Assessment of the Serbian Natural Gas Sector. *Symmetry* **2020**, *12*, 908. [CrossRef]
10. Artuğer, F.; Özkaynak, F. A Novel Method for Performance Improvement of Chaos-Based Substitution Boxes. *Symmetry* **2020**, *12*, 571. [CrossRef]
11. Petrović, D.V.; Tanasijević, M.; Stojadinović, S.; Ivaz, J.; Stojković, P. Fuzzy Model for Risk Assessment of Machinery Failures. *Symmetry* **2020**, *12*, 525. [CrossRef]
12. Gong, K.; Chen, C. A Programming-Based Algorithm for Probabilistic Uncertain Linguistic Intuitionistic Fuzzy Group Decision-Making. *Symmetry* **2019**, *11*, 234. [CrossRef]
13. Wang, Y.; Zhang, R.; Qian, L. An Improved A* Algorithm Based on Hesitant Fuzzy Set Theory for Multi-Criteria Arctic Route Planning. *Symmetry* **2018**, *10*, 765. [CrossRef]
14. Zhang, H.; Sun, Q. An Integrated Approach to Risk Assessment for Special Line Shunting Via Fuzzy Theory. *Symmetry* **2018**, *10*, 599. [CrossRef]
15. Hadacek, L.; Lovecek, T.; Scurek, R.; Zeegers, M.H. Assessment of Fence Systems Usiing Fuzzy Modeliing. *Commun.-Sci. Lett. Univ. Zilina* **2015**, *17*, 3–8.
16. Kutaj, M.; Boros, M. Development of educational equipment and linking educational process with research. In Proceedings of the 9th International Conference on Education and New Learning Technologies, Barcelona, Spain, 3–5 July 2017; pp. 5172–5177.
17. Zhang, Z.-X.; Wang, L.; Wang, Y.-M. An Emergency Decision Making Method for Different Situation Response Based on Game Theory and Prospect Theory. *Symmetry* **2018**, *10*, 476. [CrossRef]
18. Cui, Y.; Quddus, N.; Mashuga, C.V. Bayesian network and game theory risk assessment model for third-party damage to oil and gas pipelines. *Process. Saf. Environ. Prot.* **2020**, *134*, 178–188. [CrossRef]

19. Kubas, J.; Vel'as, A.; Siser, A. Implementation of multi-criteria decision making as the method used to achieve optimal level of security in local municipalities. In Proceedings of the 2nd International Conference on Physical Education, Belgrade, Serbia, 12–13 May 2017.
20. Velimirovic, J.; Janjic, A. Risk Assessment of Circuit Breakers Using Influence Diagrams with Interval Probabilities. *Symmetry* **2021**, *13*, 737. [CrossRef]
21. Reyes, J.; Gómez-Déniz, E.; Gómez, H.; Calderín-Ojeda, E. A Bimodal Extension of the Exponential Distribution with Applications in Risk Theory. *Symmetry* **2021**, *13*, 679. [CrossRef]
22. Kampová, K.; Loveček, T. Uncertainty in Quantitative Analysis of Risks Impacting Human Security in Relation to Environmental Threats. In *Understanding and Managing Threats to the Environment in South Eastern Europe*; Book Series: NATO SPS; Springer International Publishing: Cham, Switzerland, 2010; p. 349. [CrossRef]
23. Hudakova, M.; Luskova, M. Global environment impacts on enterprise risk management. In Proceedings of the 16th International Scientific Conference on Globalization and Its Socio-Economic Consequences, Rajecké Teplice, Slovakia, 5–6 October 2016; pp. 694–701.
24. Figuli, L.; Jangl, S.; Papan, D. Modelling and Testing of Blast Effect On the Structures. In *World Multidisciplinary Earth Sciences symposium (WMESS)*; PTS 1–4. Book Series: IOP Conference Series-Earth and Environmental Science; IOP Publishing: Bristol, UK, 2016; Volume 44, p. 052051.
25. Dolfin, M.; Leonida, L.; Muzzupappa, E. Forecasting Efficient Risk/Return Frontier for Equity Risk with a KTAP Approach—A Case Study in Milan Stock Exchange. *Symmetry* **2019**, *11*, 1055. [CrossRef]
26. Blokland, P.; Reniers, G. An Ontological and Semantic Foundation for Safety and Security Science. *Sustainability* **2019**, *11*, 6024. [CrossRef]
27. Reniers, G.; Landucci, G.; Khakzad, N. What safety models and principles can be adapted and used in security science? *J. Loss Prev. Process. Ind.* **2020**, *64*, 104068. [CrossRef]
28. Hofreiter, L.; Byrtusova, A.; Zvakova, Z.; Jangl, S. Ontological Aspects of Security Protection. In Proceedings of the 3rd International Conference on Management Innovation and Business Innovation (ICMIBI 2016), PT 2 Book Series, Manila, Philippines, 1–2 June 2016; Volume 58, pp. 9–14.
29. Rebecca, B. Emotion, vulnerability, ontology: Operationalising 'ontological security' for qualitative environmental sociology. *Environ. Sociol.* **2020**, *6*, 132–142. [CrossRef]
30. Boros, M.; Lenko, F. Possibility of transmission system disruption by intruder. In Proceedings of the 13th International Scientific Conference on Sustainable, Modern and Safe Transport (TRANSCOM), Žilina, Slovakia, 29–31 May 2019; Volume 40, pp. 1266–1272.
31. Martinez-Moyano, I.J.; Rich, E.; Conrad, S.; Andersen, D.F.; Stewart, T.R. A behavioral theory of insider-threat risks. *ACM Trans. Model. Comput. Simul.* **2008**, *18*, 2. [CrossRef]
32. Hofreiter, L.; Zvaková, Z. *Teória Bezpečnosti*, 1st ed.; European Association for Security: Kraków, Poland, 2019; p. 258.
33. Lukáš, L. *Teorie Bezpečnosti II*; Radim Bačuvčík—VeRBuM: Zlín, Czech Republic, 2020; ISBN 978-80-88356-06-6.
34. Hofreiter, L.; Byrtusová, A. *Indikátory Bezpečnosti*; Radim Bačuvčík—VeRBuM: Zlín, Czech Republic, 2016; ISBN 978-80-87500-82-8.
35. Volner, Š. *Bezpečnosť V 21. Storočí*; IRIS: Bratislava, Slovakia, 2009; ISBN 978-80-89256-36-5.
36. Hofreiter, L. *Manažment Ochrany Objektov*; EDIS—Vydavateľstvo Žilinskej Univerzity: Žilina-Vlčince, Slovakia, 2015.