ACIG
APPLIED CYBERSECURITY & INTERNET GOVERNANCE

NASK

Methodology of Quantitative Assessment of Network Cyber Threats Using a Risk-Based Approach

Artem Zhylin | The State Cyber Protection Centre of the State Service of Special Communications and Information Protection of Ukraine, The Cybersecurity and Application of Information Systems and Technology Academic Department at the Institute of Special Communication and Information Protection of the National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute" | ORCID: 0000-0002-4959-612X

Hanna Holych | The State Cyber Protection Centre of the State Service of Special Communications and Information Protection of Ukraine | ORCID: 0000-0003-0849-5127

Abstract

The methodology of a quantitative assessment of organisation's network cyber threats was developed in order to quantitatively assess and compare the cybersecurity threat landscape in conditions of limited data while applying the risk-oriented approach. It can be used either for assessing the level of network cyber threats of a particular organisation (as a quantitative measure of the criticality of cyber threats that are detected within the organisation's network) or for comparing the level of network cyber threats of several organisations during the same or different time periods, giving grounds for supporting the process of making managerial decisions regarding the organisation's cybersecurity strategy. The proposed scheme of the algorithm can be used to automate the calculation process. The assessment of network cyber threats that are considered in the article is not a full-fledged measure of the cyber risk because the methodology was developed considering the common circumstances of the deficiency of the risk context data. Nevertheless, the results of the methodology implementation partially reflect the overall level of the

Received: 13.02.2024

Accepted: 27.04.2024

Published: 15.07.2024

Cite this article as:
A. Zhylin, H. Holych "Methodology of quantitative assessment of network cyber threats using a risk-based approach," ACIG, vol. 3, no. 1, 2024, DOI: 10.60097/ACIG/190345

Corresponding author:
Hanna Holych, State Cyber Protection Centre of the State Service of Special Communications and Information Protection of Ukraine; E-mail: h.holych@cip.gov.ua;
0000-0003-0849-5127

organisation's cyber risk and are expected to be used in the case when the full-featured proper cyber threats assessment can't be organised for some reason.

Keywords

cyber risk, network cyber threats, quantitative assessment, risk-oriented approach, network cybersecurity domain, cyber threat landscape

1. Introduction

Assessment is a process that allows one to determine whether the implemented measures provide the expected impact and therefore contributes to establishing cause-and-effect relationships between actions and results. One of the fundamental issues in the field of cybersecurity is the assessment of the effectiveness (the degree of completeness of the realised impact) of the implemented cyber defence measures (countermeasures against cyber threats) that is conducted to check the validity and usefulness of such measures while mitigating cyber risks, as well as for the further adjustment of the organisation's general cybersecurity strategy. In this context, the determination of the organisation's approach to the assessment of cyber threats as well as their identification and analysis are among the main tasks of the risk management process.

Cyber threat assessment is an actual and popular area of scientific research because both the subjective and objective multivariate interpretation of the risk concept itself creates prerequisites for the absence of a uniform approach to its assessment and defining the main factors of direct influence. As of today, the organisation of the process of cyber threat assessment in conditions of limited contextual information and data (resulting in the inaccuracy of such an assessment), the determination of typical cyber threat characteristics that can be used during cyber threat assessment in conditions of such limitations, the instability of cyber threat landscape (resulting in the need for periodic risk factors (indicators) revision in order to maintain the relevance of such assessment) are among the typical problems in this field.

Common ways to solve such problems are the adaptation of popular methodologies and specific methods of cyber threat assessment (which are almost always used not separately, but in the context of risk definition as a more complex concept) and the creation of

individual adapted methodologies or methods of the cyber threat score formation, that is the topic of this work.

2. Theoretical Background

2.1. Literature Review

Currently, there is a research gap related to conducting cyber threat assessments based on network traffic, as most studies focus on cyber risk assessment, which is a more complex and comprehensive topic. More than that, according to the analysis of popular and scientific publications on the topic of cyber threat assessment based on network traffic, such assessments are not conducted solely using the indicators derived from network traffic analysis in any of the reviewed works. This is primarily because network traffic can be considered one of multiple data sources for such assessments [1–4], but a cyber threat assessment is a more complex process in general. At the same time, the need for the formation of quantitative indicators, even with limited resources and data [5], is confirmed by the active implementation of such indicators by well-known cybersecurity vendors [6–9] for making managerial decisions.

An explanation of the method of conducting cyber threat assessment based on indicators determined from the network traffic analysis results in combination with the data about vulnerabilities of organisation's assets is given in [10]. Research on the development of a methodology for forming a quantitative score representing the network security situation that is based on attack prediction algorithms is also quite common, for example, Hu *et al.* [11].

Publications related to conducting cyber threat assessment that is not based on network traffic (but in a related context) were also considered during the analysis [12–16]. They helped to more accurately interpret the theoretical interdependence of cybersecurity, cyber risk, cyber threat, and cyber defence indicators, the values of which are often determined or calculated based on the expression of one through the other.

In particular, the methodology [12] describes the dependence of the nature of a cyber threat on indicators of the state of society relations and confirms the relationship between the cyber threat and cybersecurity levels in such a way that the cyber threat level is a criterion for assessing the cybersecurity level. It is also specified that the criterion for assessing the cyber threat level should be mainly based on the nature of the cyber threats and requires the

consideration of their scale. Taking into account that organisations' countermeasures against cyber threats of various risk levels differ in the level of cyber attack neutralisation it can be concluded that the level of cyber attack neutralisation (cyber defence indicator) can be considered a criterion for assessing the cyber threat level.

A method for evaluating the effectiveness of measures aimed at ensuring the cybersecurity level of organisations' critical information infrastructure objects is proposed by Pyskun *et al*. [13]. While evaluating the effectiveness (along with the cybersecurity, system functional capacity, and cyber resilience indicators), the cyber risk probability indicator is proposed to be taken into account, which is determined as a combination of the cyber attack probability (that, in turn, depends on the cyber defence level) and its potential impact (amount of possible damage). Also, the criteria for assessing the cyber risk probability, cyber defence, potential impact, and the cyber attack probability are proposed with generalised recommendations on how to determine the levels by calculating the scores (without specifying the method of establishing the unambiguous correspondence of the calculated scores to specific criteria). On the one hand, such an approach makes the methodology more multi-purpose due to the lack of dependence on specific methods of calculating the scores, but on the other hand, it creates grounds for doubting the correctness of the correspondence of the calculated scores to specific criteria due to the same non-determinism of the methods of scores calculation and the lack of a described verification mechanism. In addition, this non-determinism has several levels of impact – firstly, on determining the correspondence with the criteria for the cyber attack probability and evaluating the amount of damage, then on the resulting cyber risk probability score.

In summary, the analysis of recent research publications confirms:

- the functional dependence between cyber security, cyber risk, cyber threats, and cyber defence indicators, which is relevant for understanding the applicability of the proposed approach to network cyber threat assessment in the context of determining its relationship with the other indicators. At the same time, based on the generally accepted functional dependence definition, the value of one indicator (independent or input) affects the value of another indicator (dependent or output). In our case, the definition of dependent and independent indicators is not static but varies according to the problem statement (definition of the main goals and objectives of the research, that must be completed in

order to achieve these goals) and the available input data, which are the basis for further calculations.
- the need to define an unambiguous approach for the realisation of every sequential stage of the assessment methodology, or to apply such a level of generalisation in relation to possible approaches that would not create prerequisites for doubts about the correctness of the results obtained at different stages and at the same time would allow a certain level of abstraction (i.e., with the possibility of flexible approach adaptation depending on individual factors).

2.2. Discussion of Common Cyber Risk Factors

Cyber threats, vulnerabilities, impact, likelihood, and predisposing conditions are typical cyber risk factors (according to [17–20]). Cyber risk factors can be decomposed in greater detail (e.g., cyber threats decomposed into cyber threat sources and cyber threat events) before conducting a cyber risk assessment to take into account a greater number of relevant attributes, which, in turn, contribute to increasing the objectivity of such an assessment. Therefore, cyber risk factors are characteristics used in cyber risk models as inputs to the cyber risk assessment process.

Figure 1 represents the cyber risk model based on the typical factors that are used in the work.

Taking into consideration that network cyber threat events form the only data source for the assessment, **it is more appropriate to consider cyber threat (rather than cyber risk) assessment** due to the lack of metrics that could define important cyber risk factors (such as vulnerabilities and predisposing conditions). The terms ‘cyber risk assessment’ and ‘cyber threat assessment’ are often used interchangeably, but in fact, they refer to distinct processes. While both assessments complement each other and are essential components of a robust cybersecurity strategy, they

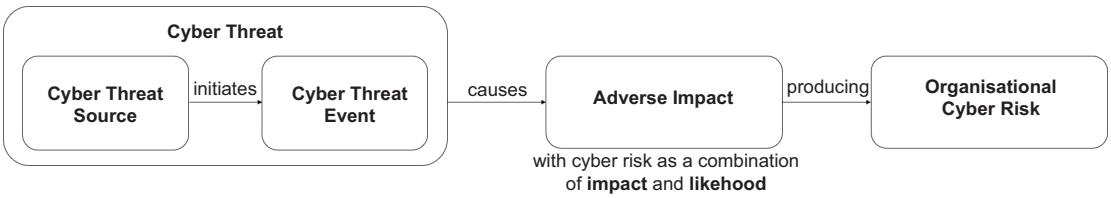

Figure 1. Cyber risk model.

serve different purposes and provide different insights. A cyber risk assessment offers a comprehensive view of an organisation's overall cyber risks, while a cyber threat assessment provides a focused analysis of the specific threats and threat actors targeting the organisation.

2.3. Terminology

The terms used in the work, that have an interpretation different from that given in NIST or ENISA glossaries, are described by the following definitions (taking into account [21, 22]):

- **organisation's network cybersecurity domain** – a set of the organisational assets and resources that are the objects of the network cybersecurity policy of the organisation;
- **network traffic** – data (encapsulated in network packets) moving between individual hosts or nodes within the network;
- **network traffic monitoring and analysis tool** – a software, hardware, or software-hardware solution whose functionality allows the usage of signature or anomaly analysis methods to detect network cyber threat events in network traffic;
- **log management tool** – a software, hardware, or software-hardware solution whose functionality allows the transmission, storage, analysis, and deletion of logs obtained from the network traffic monitoring and analysis tool (-s);
- **network cyber threat event** – an information security event detected by the network traffic monitoring and analysis tools, that means the detection of an indicator of attack or an indicator of compromise in network traffic (that is, an attempt or the fact of the network cyber threat realisation), classified according to the taxonomy of network cyber threats and characterised by criticality and the likelihood of successful realisation;
- **indicator of attack** (IoA) – a proactive indicator that determines the procedure, technique, tactic (TTP), according to which a network cyber threat can be successfully realised;
- **indicator of compromise** (IoC) – a reactive indicator that identifies a network-level artifact (classified according to the list of types of network-level artifacts), that indicates the fact of the successful network cyber threat realisation;
- **network cyber threat** – a threat that is identified through the characteristics of a network cyber threat source and a network cyber threat event (or a set of such events), the successful implementation of which involves the occurrence of undesirable consequences (harmful impact).

2.4. Conceptual Model of the Organisation's Network Cybersecurity Domain

Figure 2 represents a conceptual model of the organisation's network cybersecurity domain, considering the external and internal cyber threat surfaces. Important relationships between the entities reflected in such a high-level concept are:

- conducting cyber attacks as a way of external and internal cyber threat realisation by cyber threat sources (in the context of this work cyber threats initiated by adversaries are considered);
- transferring of network cyber threat events to the log management tool, where they are analysed for the purpose of classification and realisation of additional calculation operations (in particular, calculation of the Network Cyber Threat Score).

2.5. Organisation's Network Cyber Threat Assessment Process

There are numerous risk assessment methods available [17, 18, 23–27] and depending on the specific one employed, a risk assessment may have a number of steps or phases, and each of these phases may have slightly different names. The assessment of network cyber threats that is considered in the article is not a full-fledged measure of the cyber risk because the methodology was developed considering the common circumstances of the deficiency of the risk context data. Since the network cyber threat events detected by network traffic monitoring and analysis tools are the only source of information considered for the assessment, and due to the lack of metrics that could define important cyber risk factors, cyber threat assessment (rather than cyber risk assessment) is reviewed in this work. Guided by the approach to risk assessment defined in [17, 19, 23, 25], the stages of the network cyber threat assessment process for this methodology can be defined (see Figure 3), namely:

- preparation for the assessment;
- conducting the assessment;
- interpreting and communicating assessment results;
- maintaining the assessment.

The aim of the stage of **preparation for the assessment** is to identify the context of the network cyber threat assessment, which includes:

- identification of the purpose of the assessment;
- identification of the assessment scope;

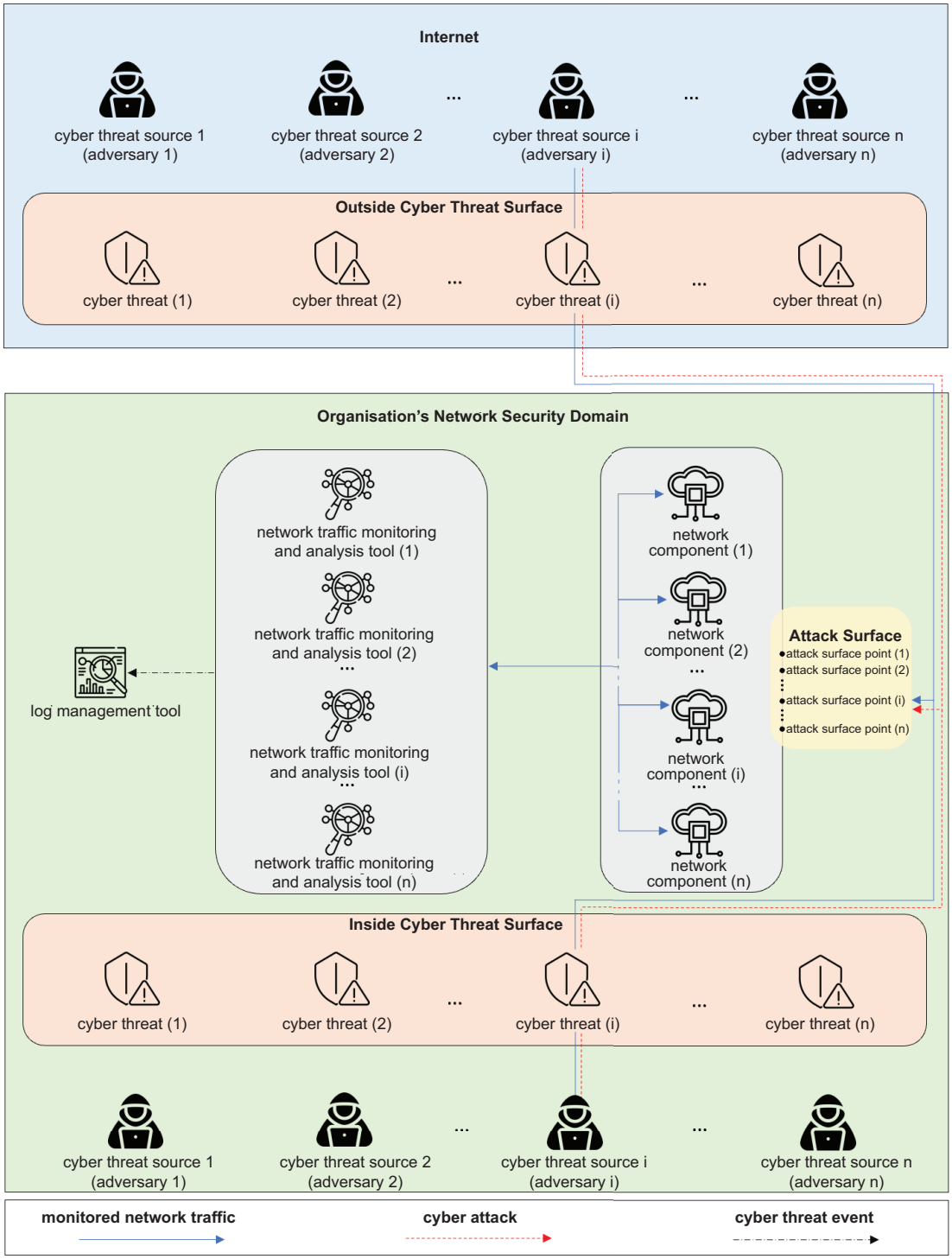

Figure 2. Conceptual model of the organisation`s network cybersecurity domain.

- identification of assumptions and constraints associated with the assessment;
- identification of information sources that are used as input data for conducting the assessment.

The aim of the stage of **conducting the assessment** is the calculation of the Network Cyber Threat Score, which includes:

- identification of the approach for classifying network cyber threats;
- identification of the network cyber threat characteristics, that are considered during the assessment;
- calculation of the Network Cyber Threat Score.

The aim of the stage of **interpreting and communicating assessment results** is a correct interpretation and understanding of the calculated Network Cyber Threat Score as well as a discussion of the obtained results in order to make effective managerial decisions, which includes:

- sharing the assessment results (e.g., executive briefings, assessment reports, dashboards);
- communicating assessment results in order to potentially make managerial decisions based on them.

The aim of the stage of **maintaining the assessment** is to track the trend of changes, to support making managerial decisions based on assessment results, and to incorporate any changes to the network cyber threat assessment approach if it needs to be actualised and updated, which includes:

- regular conduction of the organisation's network cyber threat assessment;
- regular review of the assessment approach.

3. Methods

3.1. Defining Common Network Cyber Threat Attributes

The purpose of the organisation's network cyber threat assessment is the calculation of a quantitative indicator that reflects the level of organisation's network cyber threats and can be used to compare the level of network cyber threats in different periods of time in order to monitor the trend of changes, as well as to support the managerial decision-making process (that means the implementation of such an indicator that would

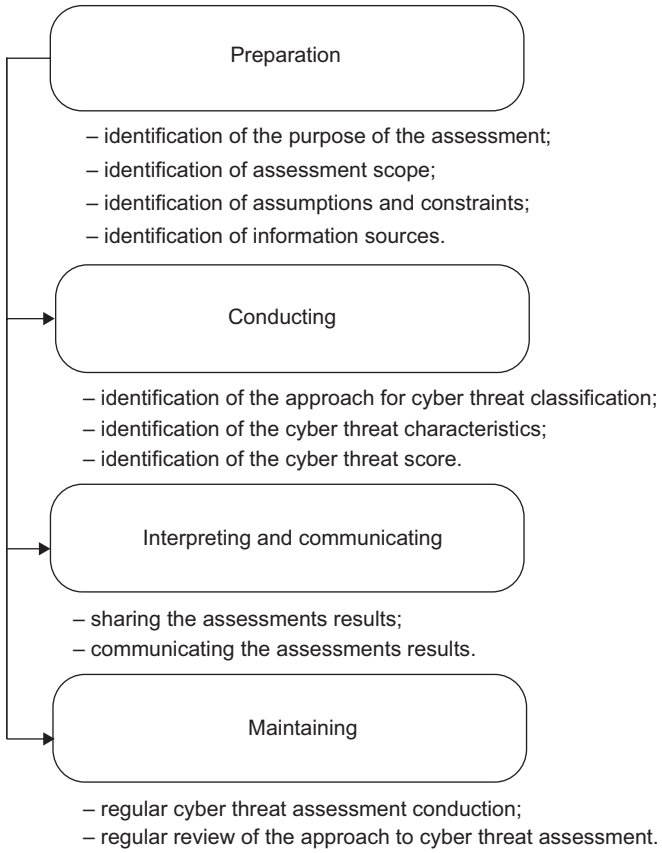

Figure 3. Stages of the network cyber threat assessment process.

be representative both for displaying the level of network cyber threats of a particular organisation and for comparing these levels between several organisations). Network cyber threat events, that are detected by network traffic monitoring and analysis tools, are the only **source of information considered for this assessment** in terms of the work.

Network cyber threat events can be discovered through the implementation of signature and (or) anomaly analysis methods when writing rules for detecting indicators of attacks or indicators of compromise in network traffic, that are applied to a network traffic monitoring and analysis tool. Since the quality of the written rules, according to which the network cyber threat events are detected, directly affects the quality of the subsequent events classification, **it is important to maintain and support the detection engineering**

process, which means developing, updating, validating, and testing the rules.

Network cyber threat events are the manifestations of cyber threats in a network environment that need to be detected, categorised, and mitigated [28, 29]. Network cyber threat attributes refer to specific characteristics or properties associated with network cyber threats that help in identifying, analysing, and understanding the nature and behaviour of the threats. As mentioned earlier, considering a greater number of relevant attributes contributes to increasing the objectivity and accuracy of the network cyber threat assessment process. Since the network cyber threat events detected by network traffic monitoring and analysis tools are the only source of information considered for the assessment in this work, it is essential to consider the key network cyber threat attributes to classify such events. Figure 4 represents the common network cyber threat attributes that are described in Table 1.

Figure 4. Network cyber threat attributes.

Table 1. Network cyber threat attributes.

Attribute name	Attribute description
src_ip	Source IP address of the network cyber threat event.
src_port	Source port of the network cyber threat event.
dest_ip	Destination IP address of the network cyber threat event.
dest_port	Destination port of the network cyber threat event.
vendor_signature	Signature of the network cyber threat event, defined by the author of the network cyber threat event detection rule.
taxonomy_category	Category of the network cyber threat event, defined after classification by the taxonomy.
taxonomy_type	Type of the network cyber threat event, defined after classification by the taxonomy.
severity	Severity of the network cyber threat event (can be defined either according to vendor_severity attribute (severity 'by default' that is defined by the author of the network cyber threat event detection rule) or reclassified using the individual approach).

3.2 Developing the Taxonomy of Network Cyber Threats

Currently, there are different ways in which to classify threats [30, 31] and it is worth noting that the categorisation is not always clear-cut. When dealing with the topic of threat event classification **it is not possible to determine which the best or correct classification is** because organisations defining a taxonomy are usually driven by different needs and have different expectations. It is determined in NIST [17] that the **network cyber threat event classification can be carried out at one of the levels of detail necessary for describing such an event**, depending on the existing assessment requirements. Description of the network cyber threat events can be general (e.g., phishing, distributed denial-of-service attack, etc.), more specific (identification of involved tactics, techniques, and procedures), or highly specific (relating to specific information systems, technologies, organisations, roles, or locations).

It would seem that creating a unified Network Cyber Threats Taxonomy is crucial for improving the detection, classification, and response to network cyber threats. It fosters standardisation, enhances collaboration, supports automation, and, ultimately, leads to a more cohesive and effective cybersecurity posture across organisations and even industries. However, while a uniform Network Cyberthreats Taxonomy offers numerous benefits, there are many scenarios where developing or modifying different taxonomies can be advantageous. The tailored approach ensures that the diverse and evolving nature of cyber threats is adequately addressed in various contexts.

Considering [32–35], the **Network Cyber Threat Taxonomy was developed** (see Table 2). It allows to correlate the detected network cyber threat events with the corresponding cyber threat types and categories (i.e., to classify the detected network cyber threat events). The aim of the proposed Network Cyber Threat Taxonomy is not to enable the community to reach a consensus on a reference taxonomy, but rather to propose one of the possible implementation options and additionally emphasise the significance and criticality of a properly adopted taxonomy in the task of threat classification.

3.3. Calculating, Normalisation, and Interpretation of the Network Cyber Threat Score

During the selection of the method for calculating the Network Cyber Threat Score, a comparative analysis was conducted between the qualitative and quantitative approaches [36–39].

Table 2. Network cyber threat taxonomy.

Cyber threat category	Cyber threat category description	Cyber threat type	Cyber threat type description
Malware infection	Detection of network artifacts or network behaviour that indicate a malware infection. Malware, also referred to as malicious code and malicious logic, is an overarching term used to describe any software or firmware intended to perform an unauthorised process that will have an adverse impact on the confidentiality, integrity or availability of a system.	**stealer**	Detection of network activity that indicates known stealer infection.
		spyware	Detection of network activity that indicates known spyware infection.
		RAT	Detection of network activity that indicates known RAT infection.
		trojan	Detection of network activity that indicates known trojan infection.
		worm	Detection of network activity that indicates known worm infection.
		browser malware	Detection of network activity that indicates known browser malware infection.
		cryptomining malware	Detection of network activity that indicates known cryptomining malware infection.
		post-exploitation tool	Detection of network activity that indicates known post-exploitation tool infection.
		loader (dropper)	Detection of network activity that indicates known loader infection.
		as-a-service malware tool	Detection of network activity that indicates known as-a-service malware tool infection. *Example: detection of malware-as-a-service tool, phishing-as-a-service tool, ransomware-as-a-service tool infection.*
		proxy malware	Detection of network activity that indicates known proxy malware infection.
		rootkit	Detection of network activity that indicates known rootkit infection.
		ransomware	Detection of network activity that indicates known ransomware infection.
		misused legitimate tool	Detection of network activity that indicates s known legitimate tool that is often misused.
		malware (unclassified)	Detection of network activity that cannot be directly attributed to known malware type but still indicates malware infection. *Example: detection of anomalous network behaviour, related to malware infection.*

(*continues*)

Table 2. Continued.

Cyber threat category	Cyber threat category description	Cyber threat type	Cyber threat type description
Threat Actors activity	Detection of network artifacts, related to targeted activity. These are artifacts of sophisticated, long-term cyber attack campaigns (usually involve a series of coordinated and targeted attacks) that are typically carried out by a well-resourced and highly skilled threat actors and focus on specific organisations/entities or whole geographic regions.Categories of cybersecurity Threat Actors, that are considered: • State-sponsored actors • Cybercrime actors • Hacker-for-hire actors • Hacktivists	**malicious network connection**	Detection of network connections to the malicious infrastructure that can be attributed to the known Threat Actor.
Suspicious network activity	Detection of network artifacts or anomalous behaviour that indicates suspicious network activity. Suspicious network activity means a potentially unwanted activity that cannot be clearly identified as a malicious one but can cause undesirable impact. When observed in conjunction with other artifacts or behaviour, they can help identify and investigate true positive security incidents or intrusions.	**anomalous network traffic behaviour**	Detection of network anomalies (spikes, unexpected or unusual communication patterns and so on). *Example: detection of anomalous network behaviour, that indicates data hoarding or network misconfiguration.*
		accessing configuration file	Detection of network activity that indicates access to a configuration file.
		suspicious network connection	Detection of network activity that indicates suspicious (potentially malicious) connections. *Example: detection of connections to a free web hosting service/a non-existent page, the usage of anonymous services, detection of suspicious user-agent string or content type.*
		scanning	Detection of network activity that indicates scanning. *Example: detection of web scanning, port/ping scanning.*

(*continues*)

Table 2. Continued.

Cyber threat category	Cyber threat category description	Cyber threat type	Cyber threat type description
Malicious network activity	Detection of network artifacts or behaviour, that indicates malicious network activity. Malicious network activity means unwanted activity that causes undesirable impact (disruption or exploiting systems, data, or network resources).	**malware distribution**	Detection of network activity that indicates malware distribution.
		disrupting availability	Detection of network activity that indicates availability disruption. Availability disruption means making relevant data, services, or other resources unavailable for access by users of a system or service. This can be accomplished by exhausting the service and its resources or overloading the components of the network infrastructure. *Example: detection of dos, ddos attempts.*
		unauthorised login	Detection of network activity that indicates unauthorised login attempts (includes one try or multiple tries). *Example: detection of default credentials login, brute force attempts.*
		file download/ upload	Detection of network activity that indicates file upload or download attempt.
		threats against data	Detection of network activity that indicates threats against data. *Example: detection of data leak, data exfiltration (breach) attempts.*
		directory/path traversal	Detection of network activity that indicates directory/path traversal attempt.
		injection	Detection of network activity that indicates injection attempt. *Example: detection of command, code, sql, xss, php injection attempts.*
		webshell	Detection of network activity that indicates webshell upload or download attempt.
		remote code execution	Detection of network activity that indicates remote code execution attempt.
		malicious network connection	Detection of network activity blacklisted by the reputation.

The qualitative approach relies on non-numerical descriptive data and subjective analysis [40], and involves expert opinions, insights, and experiences to evaluate cyber threats. The main advantage of adopting the qualitative approach is that it can be applied in

situations where quantitative data are limited or unavailable. Conversely, the quantitative approach relies on measurable data and statistical techniques, utilises metrics, scores, and other numerical values derived from data analysis to assess threats. The main advantage of adopting the quantitative approach lies in reducing biases [41] by relying on numerical data and statistical methods.

It is of the belief that there is no way to completely eliminate subjectivity in risk scoring [42] even with a fully quantitative methodology. In practice, the combination of both approaches is often used for a more comprehensive and balanced assessment of network cyber threats. However, in this work, the quantitative approach was preferred because it offers clear, quantitatively defined results that facilitate comparison and prioritisation.

To achieve the assessment goal, two values of the Network Cyber Threat Score (maximum and average) are proposed to be calculated, with each being more representative of specific cases.

The maximum value of the organisation's Network Cyber Threat Score ($S_{threat(max)\_normalized}$) is proposed to be used as a quantitative indicator that reflects the level of network cyber threats of a specific organisation. It takes the value of the maximum score among all the calculated normalised Network Cyber Threat Scores $S_{threat(i)\_normalized}$. In this case, $S_{threat(max)\_normalized}$ score value provides insight into the most critical network cyber threat that has been detected in the organisation's network traffic during the defined time period.

The average value of the organisation's Network Cyber Threat Score ($S_{threat(avg)\_normalized}$) is proposed to be used as a quantitative indicator that can be implemented to compare the network cyber threat levels of several organisations. It takes the average value among all the calculated normalised Network Cyber Threat Scores ($S_{threat(i)\_normalized}$). In this case, ($S_{threat(avg)\_normalized}$) score value provides a general understanding of the organisation's network cyber threat landscape.

The Network Cyber Threat Score $S_{threat(i)}$ is proposed to be calculated using the mixed method, considering the network cyber threat characteristics (that are defined by network cyber threat event characteristics, namely severity and likelihood of successful realisation [43, 44]):

$$S_{threat(i)} = S_{detection(i)} \times (S_{severity(i)} + S_{likelihood(i)} + S_{frequency(i)}) \quad (1),$$

where: i = 1,2,...,n, n – the total number of network cyber threat types that are detected and taken into account during the assessment time period;

$S_{detection(i)}$ – **detection factor**, which is represented by the quantitative detection score value of the network cyber threat (see Table 3);

$S_{severity(i)}$ – **severity factor**, which is represented by the quantitative severity score value of the network cyber threat (see Table 4);

$S_{likelihood(i)}$ – **likelihood factor**, which is represented by the quantitative likelihood score value of the network cyber threat (see Table 5);

$S_{frequency(i)}$ – **frequency factor**, which is represented by the quantitative frequency score value of the network cyber threat (see Table 6).

Table 3. Categories of the Network Cyber Threat Detection Score values ($S_{detection(i)}$).

Qualitative value	Quantitative value	Category description
Detected	1	Cyber threat is considered detected if some alert (from any security monitoring or analysis hardware/software tool operating within the organisational network) that indicates the cyber network threat type presence during the assessment period exists, i.e., the **number of detections is not equal to zero**.
Not Detected	0	Cyber threat is considered not detected if any alert (from any security monitoring or analysis hardware/software tool operating within the organisational network) that indicates the cyber network threat type presence during the assessment period doesn`t exists, i.e. **the number of detections is equal to zero**.

Table 4. Categories of the Network Cyber Threat Severity Score values ($S_{severity(i)}$).

Qualitative value	Quantitative value	Category description
Low	1	Cyber threat is within the low severity level if **it has no impact at all or potentially minor impact** on the stable, reliable, and regular functioning of the organisation's informational, electronic communicational, information and communication systems, and technological systems of the organisation.
Medium	2	Cyber threat is within the medium severity level if **it has a potentially moderate impact** on the stable, reliable, and regular functioning of the organisation's informational, electronic communicational, information and communication systems, and technological systems of the organisation.
High	3	Cyber threat is within the high severity level if **it has a potentially severe impact** on the stable, reliable, and regular functioning of the organisation's informational, electronic communicational, information and communication systems, and technological systems of the organisation.

Table 5. Categories of the Network Cyber Threat Likelihood Score values ($S_{likelihood(i)}$).

Qualitative value	Quantitative value	Category description
Low	1	Cyber threat is within the low likelihood level if it is **detected in the organisation`s inbound network traffic that gives grounds to characterise the successful implementation of its potential impact** on the stable, reliable, and regular functioning of the organisation's informational, electronic communicational, information and communication systems, and technological systems of the organisation **with a low level of confidence**.
High	2	Cyber threat is within the high likelihood level if it is **detected in the organisation`s outbound network traffic that gives grounds to characterise the successful implementation of its potential impact** on the stable, reliable and regular functioning of the organisation's informational, electronic communicational, information and communication systems, and technological systems of the organisation **with a high level of confidence**.

Table 6. Categories of the Network Cyber Threat Frequency Score values ($S_{frequency(i)}$).

Qualitative value	The method of normalisation of the absolute value of detections	Quantitative value	Category description
Low	$S_{frequency(i)} = \log_{10}(x+1)$	$0 < S_{frequency(i)} \leq 1$	The frequency of detections is low if the absolute value of detections of this network cyber threat type (x) meets the condition: $1 \leq x \leq 10$
Medium		$1 < S_{frequency(i)} < 2$	The frequency of detections is medium if the absolute value of detections of this network cyber threat type (x) meets the condition: $10 < x < 100$
High		$S_{frequency(i)} \geq 2, S_{frequency(max)} = 3$ For $S_{frequency(i)} \geq 3$: $S_{frequency(i)} = S_{frequency(max)}$	The frequency of detections is high if the absolute value of detections of this network cyber threat type (x) meets the condition: $x \geq 100$

In this formula, the multiplicative and additive approaches are combined [45, 46]. The multiplicative component $S_{detection(i)}$ represents the detection confidence. The additive component represents a balanced combined effect of the severity ($S_{severity(i)}$), likelihood ($S_{likelihood(i)}$), and frequency ($S_{frequency(i)}$) factors, where each factor is added to reflect their contribution to the overall Network Cyber Threat Score value.

Taking into account the difference in the impact of severity, likelihood, and frequency factors on the resulting score, **weighting**

coefficients $w_{severity}$, $w_{likelihood}$, and $w_{frequency}$ **were determined** [47] by the method of individual expert assessment. A subject matter expert (SME) assessment approach is often criticised because of potential biases [48] based on experiences or affiliations, which can influence the assessment results, as well as because of the need to consider and assess the level of expertise related to a specific narrow research topic. However, the competent management of these considerations helps to maximise the benefits of using the SME assessment approach [49]: credibility, reliability (despite a certain degree of subjectivity, involving experts adds authority and trustworthiness to the findings), and insight (SMEs can provide precise and credible evaluations based on their experience and a thorough understanding of nuanced complex topics).

In the scoring method, x_{ij} – is the weighting coefficient of the i-th factor that is defined by the j-th expert, $i = \overline{1,n}$, $j = \overline{1,m}$. Herewith, n – is the total number of the factors, that are compared, m- is the total number of experts (in our case, $n = 3$, $m = 5$).

Thus, a group of five SMEs was selected, whose task was to determine the weighting coefficients $w_{severity}$, $w_{likelihood}$, and $w_{frequency}$ (by the method of direct assessment expressed in points), considering the condition that the sum of these weighting factors should be 10 points.

Using the **coefficient of variation** (V) we can analyse the extent of variability of determined expert scores $w_{severity}$, $w_{likelihood}$, and $w_{frequency}$ and therefore check their reliability (the relative dispersion of data points in a data series around the mean). It is calculated according to the formula:

$$V = \frac{\sigma}{\overline{x}} \times 100\% \qquad (2),$$

where: V – coefficient of variation;

σ – mean squared deviation (MSD) of expert scores that is calculated according to (3);

$\overline{x}$ – arithmetic mean of expert scores that is calculated according to (4).

$$\sigma = \sqrt{\frac{\sum_{j=1}^{m} \left(x_{i,j} - \overline{x} \right)^2}{m-1}} \qquad (3),$$

where: σ – mean squared deviation (MSD) of expert scores;

$x_{i,j}$ – score of the *i*-th factor that is defined by the *j*-th expert;

$\bar{x}$ – arithmetic mean of expert scores;

m – the total number of experts.

$$\bar{x} = \frac{\sum x_{i,j}}{n} \quad (4),$$

where: $\bar{x}$ – arithmetic mean of expert scores;

$x_{i,j}$ – score of the *i*-th factor that is defined by the *j*-th expert;

n – the total number of factors that are evaluated.

The calculated values of variation coefficients *V* (see Table 5) indicate low values of variation for $w_{severity}$, $w_{likelihood}$ (that means the high homogeneity of the respective data sets (low variability) and that the arithmetic mean value is a reliable characteristic for them), as well as a moderate value of variation for $w_{frequency}$ (that means moderate homogeneity of the corresponding data set and the fact that instead of the arithmetic mean value, it is more appropriate to choose the mode or median as a characteristic of the distribution centre).

Therefore, the resulting weighting coefficients for the *i*-th factors, pre-assessed according to the experts' scores (w_i), are determined by the modes (by the values that are most often found in the sets of weights ($x_{i,j}$) for the *i*-th factors, assessed by the scores of the *m* number of experts, i.e., have the highest frequency $f(w_{i,j})$.

Table 7. The defined values of the weighting coefficients for the Network Cyber Threat Score factors and the values of variation coefficients.

Weight score of the *i*-th factor	Score of the *j*-th expert					$\bar{x}$	σ	*V*	Frequency of the weight score ($f(w_{ij})$)	Resulting weight score (w_i)
	j = 1 w_{i1}	*j* = 2 w_{i2}	*j* = 3 w_{i3}	*j* = 4 w_{i4}	*j* = 5 w_{i5}					
i = 1, w_{1j} ($w_{severity}$)	$x_{1,1}$ 5	$x_{1,2}$ 6	$x_{1,3}$ 6	$x_{1,4}$ 5	$x_{1,5}$ 6	5.6	0.55	9,82%	$f(w_{1j} = 5) = 2$ $f(w_{1j} = 6) = 3$	6
i = 2, w_{2j} ($w_{likelihood}$)	$x_{2,1}$ 4	$x_{2,2}$ 3	$x_{2,3}$ 3	$x_{2,4}$ 3	$x_{2,5}$ 3	3.2	0.45	14,06%	$f(w_{2j} = 3) = 4$ $f(w_{2j} = 4) = 1$	3
i = 3, w_{3j} ($w_{frequency}$)	$x_{3,1}$ 1	$x_{3,2}$ 1	$x_{3,3}$ 1	$x_{3,4}$ 2	$x_{3,5}$ 1	1.2	0.45	37,5%	$f(w_{3j} = 1) = 4$ $f(w_{3j} = 1) = 1$	1

Taking into account the determined weights from Table 7 equation (1) takes the form:

$$S_{threat(i)} = S_{detection(i)} \times ((w_{severity} \times S_{severity(i)}) + (w_{likelihood} \times S_{likelihood(i)}) + (w_{frequency} \times S_{frequency(i)})) \quad (5)$$

For convenient interpretation of the Network Cyber Threat Score value, **normalisation** (converting the calculated values to the required scale) is applied by using the linear scaling formula [50]:

$$S_{threat(i)\_normalized} = \left(\frac{S_{threat(i)} - S_{threat(min)}}{S_{threat(max)} - S_{threat(min)} \right) \times \left(S_{threat(max)\_normalized} - S_{threat(min)\_normalized} \right) + S_{threat(min)\_normalized} \quad (6),$$

where: $S_{threat(min)} = 1 \times ((6 \times 1) + (3 \times 1) + (1 \times 0.3)) = 9.3$ (the minimal value of not normalised range);

$S_{threat(max)} = 1 \times ((6 \times 3) + (3 \times 2) + (1 \times 3)) = 27$ (the maximum value of not normalised range);

$S_{threat(min)\_normalized} = 1$ (the minimal value of normalised range);

$S_{threat(max)\_normalized} = 100$ (the maximum value of normalised range).

Considering that $S_{threat(i)\_normalized}$ values for not detected network cyber threats correspond to the same $S_{threat(i)}$ values and are equal to zero, we get normalised (see Table 8) interpretable (see Table 9) ranges of the Network Cyber Threat Score [0,100].

The boundary values in Tables 8 and 9 are preliminary and almost evenly distributed, but in practice, they should be chosen in accordance with the determined level of risk tolerability [51–55] and revised regularly as the risk landscape evolves [56]. Setting boundaries helps in categorising and prioritising risks accurately [57, 58]. That's why setting the tolerability level should be tailored to the unique context [59] and be established periodically by decision makers at a strategic level in accordance with the external risk environment of the organisation and relevant justification, that in some cases becomes a contractual objective.

The average value of the organisation's Network Cyber Threat Score ($S_{threat(avg)\_normalized}$), as a normalised average score of all detected

Table 8. Normalised ranges of the Network Cyber Threat Score values.

Detection categories	Severity categories	Likelihood categories	Frequency categories	Resulting category (not normalised values)	Resulting category (normalised values)
Not Detected (0)	*	*	*	Undefined (0)	
Detected (1)	Low (6)	Low (3)	Low (1)	Informational (9.3, 10]	Informational (1, 4.9]
			Medium (2)	Informational (10, 11)	Informational (4.9, 10.5)
			High (3)	Informational [11, 12]	Informational [10.5, 16.1]
	Low (6)	High (6)	Low (1)	Low (12, 13]	Low (16.1, 21.7]
			Medium (2)	Low (13, 14)	Low (21.7, 27.3)
			High (3)	Low [14, 15]	Low [27.3, 32.9]
	Medium (12)	Low (3)	Low (1)	Medium (15, 16]	Medium (32.9, 38.5]
			Medium (2)	Medium (16, 17)	Medium (38.5, 44.1)
			High (3)	Medium [17, 18]	Medium [44.1, 49.7]
	Medium (12)	High (6)	Low (1)	Medium (18, 19]	Medium (49.7, 55.3]
			Medium (2)	Medium (19, 20)	Medium (55.3, 60.8)
			High (3)	Medium [20, 21]	Medium [60.8, 66.4]
	High (18)	Low (3)	Low (1)	High (21, 22]	High (66.4, 72]
			Medium (2)	High (22, 23)	High (72, 77.6)
			High (3)	High [23, 24]	High [77.6, 83.2]
	High (18)	High (6)	Low (1)	Critical (24, 25]	Critical (83.2, 88.8]
			Medium (2)	Critical (25, 26)	Critical (88.8, 94.4)
			High (3)	Critical [26, 27]	Critical [94.4, 100]

Table 9. Categories of Network Cyber Threat Score values (interpretation).

Qualitative value	Quantitative value	Description
Undefined level	$S_{threat(i)\_normalized} = 0$	If the calculated **Network Cyber Threat Score value** is **within the undefined level**, this **indicates** that **there were no network cyber threat type detections** in the organisation`s inbound or outbound network traffic during the evaluated time period.
Informational level	$1 < S_{threat(i)\_normalized} \leq 16.1$	If the calculated **Network Cyber Threat Score value** is **within the informational level**, this **indicates** that **a low criticality network cyber threat type with a low likelihood level of successful realisation** was detected in the organisation`s inbound network traffic during the evaluated time period. The information level category doesn`t require the organisation's response to take measures related to the detected cyber threat type, as it potentially doesn`t cause a significant impact on the stable, reliable, and regular functioning of the organisation's informational, electronic communicational, information and communication systems, and technological systems. It is recommended to familiarise with the results of the Network Cyber Threat Score calculation to mitigate the potential cyber risk.
Low level	$16.1 < S_{threat(i)\_normalized} \leq 32.9$	If the calculated **Network Cyber Threat Score value** is **within the low level**, this **indicates** that **a low criticality network cyber threat type with a high likelihood level of successful realisation** was detected in the organisation`s outbound network traffic during the evaluated time period. The low level category doesn`t require the organisation's response to take measures related to the detected cyber threat type, as it potentially doesn`t cause a significant impact on the stable, reliable, and regular functioning of the organisation's informational, electronic communicational, information and communication systems, and technological systems. It is recommended to familiarise with the results of the Network Cyber Threat Score calculation to mitigate the potential cyber risk.
Medium level	$32.9 < S_{threat(i)\_normalized} \leq 66.4$	If the calculated **Network Cyber Threat Score value** is **within the medium level**, this **indicates** that **a medium criticality network cyber threat type** was detected in the organisation`s inbound or outbound network traffic during the evaluated time period. The medium-level category requires the organisation's response to take measures related to the detected cyber threat type, as it can potentially cause a significant impact on the stable, reliable and regular functioning of the organisation's informational, electronic communicational, information and communication systems, and technological systems. It is recommended to familiarise with the results of the Network Cyber Threat Score calculation to mitigate the potential cyber risk.

(*continues*)

Table 9. Continued.

Qualitative value	Quantitative value	Description
High level	$66.4 < S_{threat(i)\_normalized} \leq 83.2$	If the calculated **Network Cyber Threat Score value** is **within the high level**, this **indicates** that **a high criticality network cyber threat type with a low likelihood level of successful realisation** was detected in the organisation`s inbound network traffic during the evaluated time period. The high-level category requires the immediate organisation's response to take measures related to the detected cyber threat type (localising and eliminating the potential consequences), as it can potentially cause a significant impact on the stable, reliable, and regular functioning of the organisation's informational, electronic communicational, information and communication systems, and technological systems. It is recommended to familiarise with the results of the Network Cyber Threat Score calculation to mitigate the potential cyber risk.
Critical level	$83.2 < S_{threat(i)\_normalized} \leq 100$	If the calculated **Network Cyber Threat Score value** is **within the critical level**, this **indicates** that **a high criticality network cyber threat type with a high likelihood level of successful realisation** was detected in the organisation`s outbound network traffic during the evaluated time period. The critical level category requires the immediate organisation's response to take measures related to the detected cyber threat type (localising and eliminating the consequences), as it can have a significant impact on the stable, reliable and regular functioning of the organisation's informational, electronic communicational, information and communication systems, and technological systems. It is recommended to familiarise with the results of the Network Cyber Threat Score calculation to mitigate the cyber risk.

network cyber threats is proposed to be calculated using the formula of the arithmetic mean, since the individual values of the averaged feature (normalised Network Cyber Threat Scores) and their number in the aggregate are known:

$$S_{threat(avg)\_normalized} = \frac{1}{k} \times \sum_{i=1}^{k} S_{threat(i)\_normalized} \quad (7),$$

where: $i = 1, 2, ..., k$, k – the number of network cyber threat types, the classification of network cyber threat events according to which is taken into account during the assessment and for which the absolute number of detected cyber threat events is a non-zero value, meaning $x \neq 0$; $\sum_{i=1}^{k} S_{threat(i)\_normalized}$ – the sum of the detected normalised Network Cyber Threat Scores.

The arithmetic mean is commonly used in various risk assessment and scoring methodologies as it provides an intuitive and easily interpretable measure of the central tendency. Since the individual Network Cyber Threat Scores are normalised, they are on a comparable scale, making the arithmetic mean an appropriate measure. By averaging all normalised Network Cyber Threat Scores, the arithmetic mean accounts for the cumulative impact of all the detected threats and appears to be a consistent metric, meaning that changes in individual normalised Network Cyber Threat Score values will proportionately affect the overall average and contribute equally, avoiding bias from extreme values. Therefore, it can serve as a baseline metric for comparing changes in the organisation's network cyber threat landscape over time as well as for comparing network security postures of different organisations.

Table 10 represents categories, according to which the calculated average value of the organisation's Network Cyber Threat Score is proposed to be interpreted.

4. Results

According to the methodology, presented in the work, a scheme of the algorithm was developed (see Figure 5) for the automated calculation of the Network Cyber Threat Score, where: j – the overall number of detected network cyber threat events during the assessment period; n – the number of network cyber threat types, the classification of network cyber threat events according to which is taken into account during the assessment (according to the taxonomy, proposed to use in this work, n = 30); k – the number of network cyber threat types, the classification of network cyber threat events according to which is taken into account during the assessment and for which the absolute number

Table 10. Categories of the average value of the organisation's Network Cyber Threat Score ($S_{threat(avg)\_normalized}$).

Qualitative value	Quantitative value	Description
Undefined level	$S_{threat(avg)\_normalized} = 0$	The calculated value of the average value of the organisation's Network Cyber Threat Score is **undefined**.
Low level	$1 < S_{threat(avg)\_normalized} \leq 32.9$	The calculated value of the average value of the organisation's Network Cyber Threat Score is **within the low-level** range.
Medium level	$32.9 < S_{threat(avg)\_normalized} \leq 66.4$	The calculated value of the average value of the organisation's Network Cyber Threat Score is **within the medium-level** range.
High level	$66.4 < S_{threat(avg)\_normalized} \leq 100$	The calculated value of the average value of the organisation's Network Cyber Threat Score is **within the high-level** range.

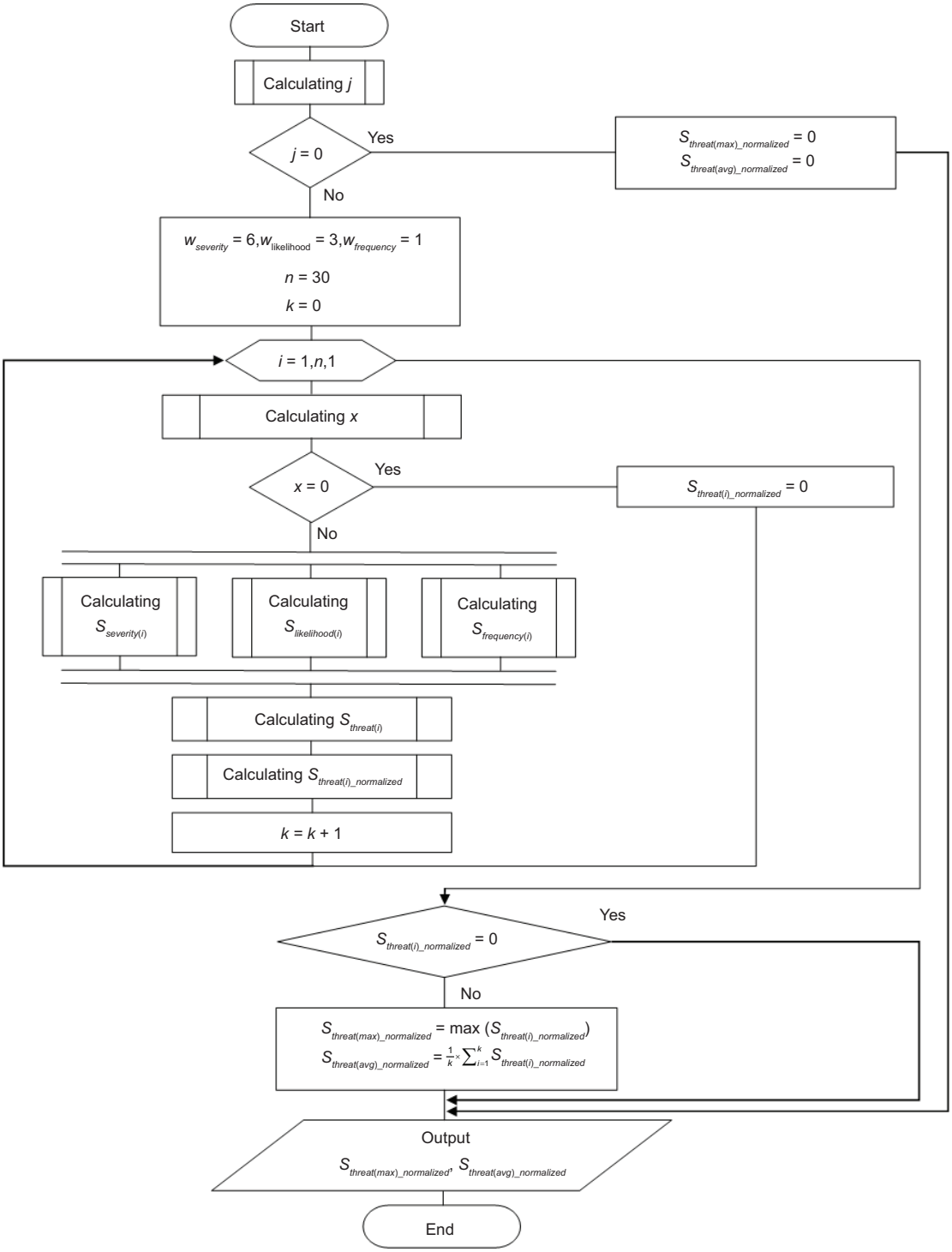

Figure 5. A scheme of the algorithm.

of detected cyber threat events is a non-zero value, meaning $x \neq 0$; k – the absolute number of detected network cyber threat events, that are classified by network cyber threat types according to the taxonomy, proposed to use in this work.

The algorithm's scheme formalises the inputs, processes, and outputs needed to grasp and implement the steps involved in calculating the maximum ($S_{threat(max)\_normalized}$) and average ($S_{threat(avg)\_normalized}$) values of the Network Cyber Threat Score. By following these steps, the algorithm can be applied and automated for the purpose of conducting the organisation's network cyber threat assessment process more effectively, delivering real-time insights into the network's security posture and allowing for timely responses.

Taking into consideration the conceptual model of the organisation's network cybersecurity domain (presented in Figure 2), the algorithm scheme (presented in Figure 5) was validated in practice by its implementation in the log management tool of a specific organisation, allowing for the automated calculation of the Network Cyber Threat Score.

The dashboard was also developed for the log management tool, used within the organisation (see Figure 6). It visualises the results of the custom correlation searches that classify network cyber threat events with regard to the categories and types outlined in the Network Cyber Threat Taxonomy and contains the detailed results of the Network Cyber Threat Score calculation with all the related metrics. Grouping panels together and arranging them in a logical and visually appealing layout makes the dashboard easy to interpret. Therefore, the presented visualisation example can be used as one of the options for displaying the results of the algorithm implementation and for monitoring the Network Cyber Threat Score value (continuously or at scheduled intervals) to check for exceeding certain thresholds. It can be applied for sharing information developed in the execution of the cyber threat assessment during the stage of communicating and sharing assessment information. In particular, the dashboard panel contains:

1. the results of calculating the maximum and average values of the Network Cyber Threat Score (single value visualisation);
2. distribution of the number of detected cyber threat events by cyber threat categories (pie chart visualisation);
3. timechart of the number of detected cyber threat events by cyber threat categories (single value visualisation with trend indicator);

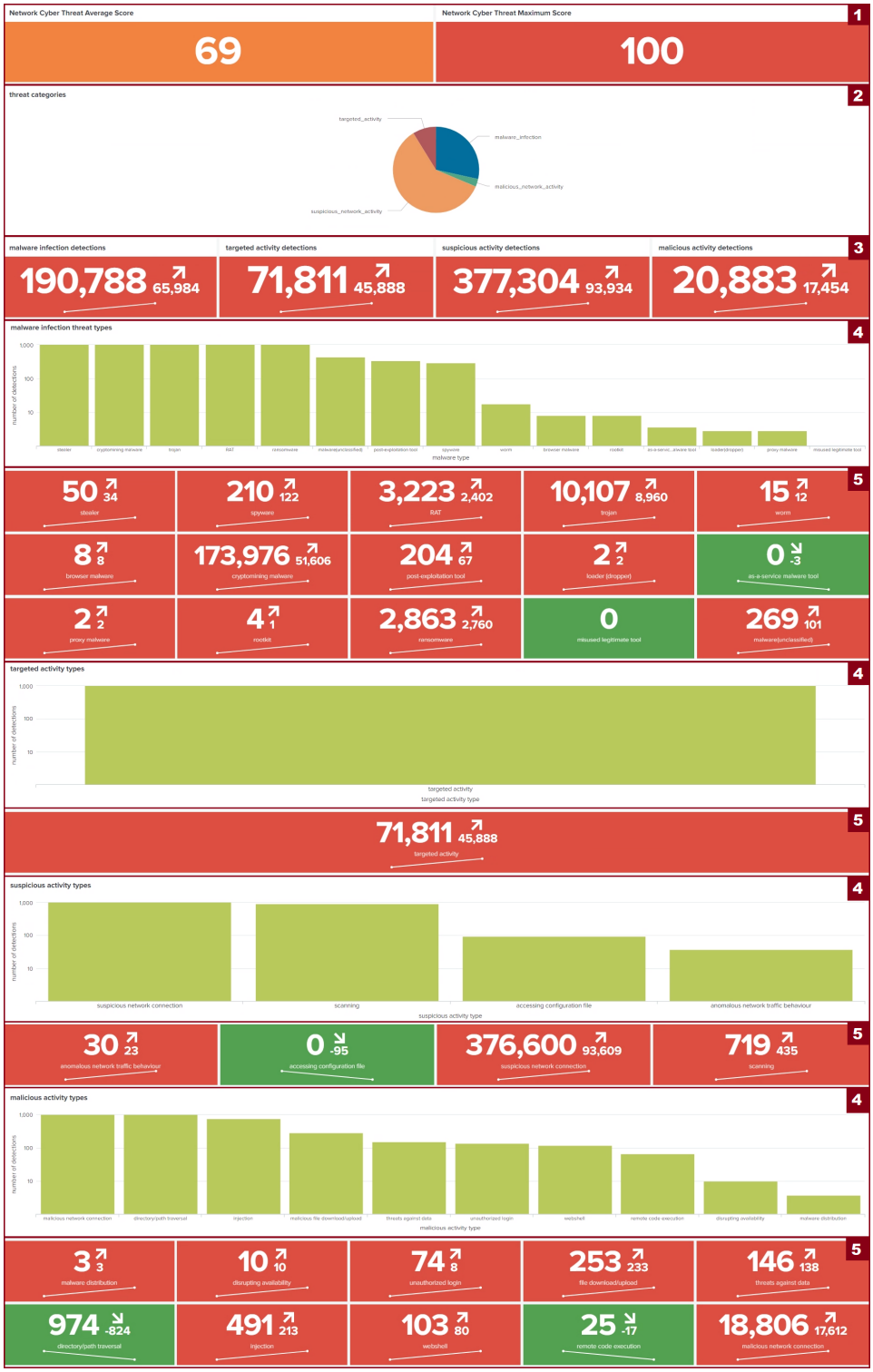

Figure 6. A dashboard panel.

4. distribution of the number of detected cyber threat events by cyber threat types (histogram visualisation);
5. timechart of the number of detected cyber threat events by cyber threat types (single value visualisation with trend indicator).

5. Discussion

A uniform approach to calculating the organisation's Network Cyber Threat Score that involves a fixed set of factors, an assessment scale for each factor, and an algorithm for combining these factors cannot simultaneously satisfy the needs of different organisations. Therefore, the creation of an adapted methodology is a necessary step in order to take into account additional factors, determine the required level of their decomposition and select a convenient combining algorithm for conducting such an assessment.

The automated calculation of the maximum and average values of the Network Cyber Threat Score according to the methodology presented in the work allows determining the quantitative indicators that **partially reflect the overall level of the organisation's cyber risk** (because network traffic analysis can detect only a certain range of cyber threats and cannot replace a complex approach to conducting a cyber risk assessment). It can be implemented **for comparing the level of network cyber threats during different time periods** to monitor the trend of changes, as well as **for supporting the process of making managerial decisions regarding the organisation's cybersecurity strategy** (namely, planning new and improving existing preventive protection measures). The methodology of calculating the Network Cyber Threat Score is also flexible enough to be adopted by various organisations by adjusting it to their own Network Cyber Threat Taxonomy. According to their requirements, the scoring of some cyber threat types and categories (the Network Cyber Threat Severity Score values) can be adjusted to produce the most appropriate results.

In terms of limitations, it is important to take into consideration the factors that directly affect the objectivity of the calculated scores:

- the technical component, namely the functional capabilities (methods of analysis) of the available network traffic monitoring and analysis tools that are in use;
- the quality of the detection rules applied directly to the existing network traffic monitoring and analysis tools for detecting network events, classified as cyber threats.

The greater the number of methods or their combinations used by the available network traffic monitoring and analysis tools, as well as the better the quality of implemented detection rules, the greater the number of network events, classified as cyber threats, can be detected and the more accurate these detections will be (in terms of increasing the number of True Positive alerts).

Currently, some simplifications of the risk-based approach are being applied to conduct the network cyber threat assessment process within the discussed methodology. Future research directions include decomposing the current procedure to define categories of Network Cyber Threat Severity and Likelihood Scores, as well as considering the other possible characteristics of network cyber threats to quantify and account for them in the calculation of the Network Cyber Threat Score.

Acknowledgements

We are thankful to our colleagues who offered their perspectives during informal discussions, which have enriched our understanding and interpretation of the researched data. First and foremost, our sincere thanks go to Mike Harbison (Engineer at Palo Alto Networks UNIT 42 team), whose guidance and insightful feedback were instrumental in shaping the research. We are also grateful to Ganna Korniychenko (Senior Threat Intelligence Analyst at KPMG UK) whose expertise and constructive suggestions significantly enhanced the quality of our work. This work is a result of the collaborative spirit and collective effort of all involved, and we are profoundly grateful for each contribution.

References

[1] Y. Yuan, W. Xu, "Network security situation based on big data environment." 6th International Workshop on Advanced Algorithms and Control Engineering (IWAACE 2022), 2022, doi: 10.1117/12.2653255.

[2] J. Zhang, H. Feng, B. Liu, D. Zhao, "Survey of technology in network security situation awareness," *Sensors*, vol. 23, no. 5, p. 2608, 2023, doi: 10.3390/s23052608.

[3] B. Zhou, B. Sun, T. Zang, Y. Cai, J. Wu, H. Luo, "Security risk assessment approach for distribution network cyber physical systems considering cyber attack vulnerabilities," *Entropy*, vol. 25, no. 1, p. 47, 2023, doi: 10.3390/e25010047.

[4] M.S. Kacar, K. Oztoprak, "Network security scoring." IEEE 11th International Conference on Semantic Computing (ICSC), 2017. [Online]. Available: https://

www.researchgate.net/publication/315872054_Network_Security_Scoring. [Accessed: Jun. 15, 2023].

[5] T. Ali, M. Al-Khalidi, Rabab Al-Zaidi, "Information security risk assessment methods in cloud computing: Comprehensive review," *The Journal of Computer Information Systems*, pp. 1–28, 2024, doi: 10.1080/08874417.2024.2329985.

[6] Imperva. (2023). *Cyber Threat Index. Cyber Security Statistics & Trends*. [Online]. Available: https://www.imperva.com/cyber-threat-index/. [Accessed: Aug. 22, 2023].

[7] NordVPN. (2020). *Cyber Risk Index.* [Online]. Available: https://s1.nordcdn.com/nord/misc/0.13.0/vpn/brand/NordVPN-cyber-risk-index-2020.pdf. [Accessed: Aug. 29, 2023].

[8] M. Khudyntsev, O. Lebid, M. Bychenok, A. Zhylin, A. Davydiuk, "Network monitoring index in the information security management system of critical information infrastructure objects," in *Information and Communication Technologies and Sustainable Development*, S. Dovgyi, O. Trofymchuk, V. Ustimenko, L. Globa, Eds., Lecture Notes in Networks and Systems, Springer, Cham, 2022, pp. 270–290.

[9] V. Kravets, "Comparative analysis of the cybersecurity indices and their applications," *Theoretical and Applied Cybersecurity*, vol. 1, no. 1, pp. 97-102, 2019, doi: 10.20535/tacs.2664-29132019.1.169090.

[10] R. Xi, X. Yun, Z. Hao, Y. Zhang, "Quantitative threat situation assessment based on alert verification," *Security and Communication Networks*, vol. 9, no. 13, pp. 2135–2142, 2016, doi: 10.1002/sec.1473.

[11] H. Hu, H. Zhang, Y. Liu, Y. Wang, "Quantitative method for network security situation based on attack prediction," *Security and Communication Networks*, vol. 2017, no. 1, pp. 1–19, 2017, doi: 10.1155/2017/3407642.

[12] I. Kozubtsov, O. Chernonoh, L. Kozubtsova, M. Artemchuk, I. Neshcheret, "Selection of individual indicators for assessing the ability of the information security and cybersecurity system to function in special communication information and communication systems," *Cybersecurity: Education, Science, Technique*, vol. 16, no. 4, pp. 19–27, 2022, doi: 10.28925/2663-4023.2022.16.1927.

[13] I. Pyskun, Y. Tkach, V. Khoroshko, Y. Khokhlachova, A.R.A. Ayasrah, A.F. Al-Dalvash, "Quantitative assessment and determination of the level of cyber security of state information systems," *Ukrainian Scientific Journal of Information Security*, vol. 26, no. 3, pp. 131–138, 2020, doi: 10.18372/2225-5036.26.14974.

[14] L. Kozubtsova, Y. Khlaponin, I. Kozubtsov, "Methods of evaluation of efficiency of implementation of cyber security measures of critical information infrastructure bodies of the body. Modern information technologies in the sphere of security and defence," *Modern Information Technologies in the Field of Security and Defense*, vol. 41, no. 2, pp. 17–22, 2021, doi: 10.33099/2311-7249/2021-41-2-17-22.

[15] B. Metin, S. Duran, E. Telli, M. Mutlutürk, M. Wynn, "IT Risk Management: Towards a System for Enhancing Objectivity in Asset Valuation That Engenders a Security Culture," *Information*, vol. 15, no. 1, 2024, doi: 10.3390/info15010055.

[16] V.L. Buriachok, V.B. Tolubko, V.O. Khoroshko, S.V. Tolupa, *Information and Cyber Security: Socio-Technical Aspect*. State University of Information and Communication Technologies, Kyiv, 2015.

[17] Joint Task Force Transformation Initiative. (2012). *Guide for Conducting Risk Assessments.* [Online]. Available: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-30r1.pdf. [Accessed: Apr. 15, 2023].

[18] ENISA. (Feb. 21, 2023). *Interoperable EU Risk Management Toolbox*. [Online]. Available: https://www.enisa.europa.eu/publications/interoperable-eu-risk-management-toolbox. [Accessed: Jun. 10, 2023].

[19] D. Landoll, *The Security Risk Assessment Handbook: A Complete Guide for Performing Security Risk Assessments*, CRC Press, Boca Raton, FL, 2021.

[20] N. Yalcin, B. Kılıç, "Information security risk management and risk assessment methodology and tools." International Conference on Cyber Security and Computer Science (ICONCS 2018), 2019. [Online]. Available: https://www.researchgate.net/publication/330170264_Information_Security_Risk_Management_and_Risk_Assessment_Methodology_and_Tools. [Accessed: Jun. 15, 2023].

[21] National Institute of Standards and Technology. (Apr. 22, 2024). *Glossary*. [Online]. Available: https://csrc.nist.gov/glossary. [Accessed: Apr. 15, 2023].

[22] ENISA. (2024). *Glossary of Terms*. [Online]. Available: https://www.enisa.europa.eu/topics/risk-management/current-risk/bcm-resilience/glossary. [Accessed: Apr. 15, 2023].

[23] National Institute of Standards and Technology. (2018). *Risk management framework for information systems and organizations*. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf. [Accessed: Apr. 15, 2023].

[24] J. Sokol. (Feb. 25, 2021). *The OWASP risk rating methodology and SimpleRisk*. [Online]. Available: https://www.simplerisk.com/blog/owasp-risk-rating-methodology-and-simplerisk. [Accessed: Jun. 16, 2023].

[25] ENISA. (2022). *Risk management standards: Analysis of standardisation requirements in support of cybersecurity policy.* [Online]. Available: https://www.enisa.europa.eu/publications/risk-management-standards. [Accessed: Jun. 10, 2023].

[26] J. Dobaj, C. Schmittner, M. Krisper, G. Macher, "Towards integrated quantitative security and safety risk assessment," in *Computer Safety, Reliability, and Security,* A. Romanovsky, E. Troubitsyna, I. Gashi, E. Schoitsch, F. Bitsch, Eds., Turku, Lecture Notes in Computer Science, Springer Cham, 2019, pp. 102–116.

[27] S. Bhamidipati, *Examining approaches to quantifying cyber risk for improved cybersecurity management*, Massachusetts Institute of Technology, 2019. [Online]. Available: https://dspace.mit.edu/bitstream/handle/1721.1/124233/1144933199-MIT.pdf?sequence=1&isAllowed=y. [Accessed: Jun. 20, 2023].

[28] G.-Y. Shin, S.-S. Hong, J.-S. Lee, I.-S. Han, H.-K. Kim, H.-R. Oh, "Network security node-edge scoring system using attack graph based on vulnerability correlation," *Applied Sciences*, vol. 12, no. 14, 2022, doi: 10.3390/app12146852.

[29] O. Korchenko, V. Hnatyuk, E. Ivanchenko, S. Hnatyuk, N. Seilova, "Method for cyber incidents network-centric monitoring of cyber incidents in modern information & communication systems," *Information Protection*, vol. 18, no. 3, pp. 229–247, 2016, doi: 10.5815/ijcnis.2017.06.04.

[30] ENISA. (2022). *Threat landscape methodology*. [Online]. Available: https://www.enisa.europa.eu/publications/enisa-threat-landscape-methodology. [Accessed: Jun. 10, 2023].

[31] M. Benmalek, "Ransomware on cyber-physical systems: taxonomies, case studies, security gaps, and open challenges," *Internet of Things and Cyber-Physical Systems*, vol. 4, pp. 186–202, 2024, doi: 10.1016/j.iotcps.2023.12.001.

[32] ENISA. (2018). *Reference incident classification taxonomy*. [Online]. Available: https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy. [Accessed: Apr. 29, 2023].

[33] Europol. (2017). *Common taxonomy for law enforcement and the national network of CSIRTs*. [Online]. Available: https://www.europol.europa.eu/cms/sites/default/files/documents/common_taxonomy_for_law_enforcement_and_csirts_v1.3.pdf. [Accessed: Apr. 29, 2023].

[34] ENISA. (2016). *Threat taxonomy*. [Online]. Available: https://www.enisa.europa.eu/topics/cyber-threats/threats-and-trends/enisa-threat-landscape/threat-taxonomy/view. [Accessed: Apr. 29, 2023].

[35] *Threat landscape: Trends and methods. Cyber-threat landscape and end-user requirements*, 31 Aug. 2018. [Online]. Available: https://cyber-trust.eu/wp-content/uploads/2020/02/D2.1.pdf. [Accessed: Jun. 16, 2024].

[36] ZenGRC. (Aug. 10, 2023). *NIST Cyber Risk Scoring.* [Online]. Available: https://reciprocity.com/blog/nist-cyber-risk-scoring/. [Accessed: Aug. 20, 2023].

[37] M. Krisper. (2021). *Problems with risk matrices using ordinal scales*. [Online]. Available: https://arxiv.org/pdf/2103.05440. [Accessed: Jun. 16, 2023].

[38] V. Evrin. (Apr. 28, 2021). *Risk assessment and analysis methods: Qualitative and quantitative*. [Online]. Available: https://www.isaca.org/resources/isaca-journal/issues/2021/volume-2/risk-assessment-and-analysis-methods. [Accessed: Jun. 16, 2023].

[39] *About TDR threat scores.* [Online]. Available: https://www.watchguard.com/help/docs/fireware/12/en-us/Content/en-US/services/tdr/tdr_threat_scores.html. [Accessed: Jun. 16, 2023].

[40] S. Ekung, "Limitations of risk identification tools applied in project management in the Nigerian construction industry," *Malaysian Construction Research Journal*, vol. 30, no. 1, pp. 73–85, 2020.

[41] A.N. Kia, F. Murphy, B. Sheehan, D. Shannon, "A cyber risk prediction model using common vulnerabilities and exposures," *Expert Systems with Applications*, vol. 237, 2024, doi: 10.1016/j.eswa.2023.121599.

[42] RiskWatch. (Jan. 31, 2024). *Risk scoring methodology.* [Online]. Available: https://www.riskwatch.com/risk-scoring-methodology/. [Accessed: Jun. 16, 2023].

[43] ENISA. (2019). *EU Cybersecurity Certification Framework: Methodology for sectoral cybersecurity assessments*. [Online]. Available: https://www.enisa.europa.eu/publications/methodology-for-a-sectoral-cybersecurity-assessment. [Accessed: Jun. 10, 2023].

[44] C. Borrett, "Threat level index for advanced persistent threats (APT) - European repository of cyber incidents," German Institute for International and Security Affairs, 2022, doi: 10.7802/2494.

[45] T. Mahler, Y. Elovici, Y. Shahar, "A new methodology for information security risk assessment for medical devices and its evaluation," *Computer Science: Cryptography and Security*, 2020, doi: 10.48550/arXiv.2002.06938.

[46] EuRepoC. (2023). *Methodology*. [Online]. Available: https://eurepoc.eu/methodology/. [Accessed: Jun. 16, 2023].

[47] B. Sohval, *A deep dive in scoring methodology*, SecurityScorecard, 2024. [Online]. Available: https://securityscorecard.com/wp-content/uploads/2024/01/EBOOK-MethodologyDeepDive-3.0_v2-1.pdf. [Accessed: Jun. 16, 2023].

[48] J. de Wit, W. Pieters, P. van Gelder, "Bias and noise in security risk assessments: An empirical study on the information position and confidence of security professionals," *Security Journal*, vol. 37, pp. 170–191, 2023, doi: 10.1057/s41284-023-00373-6.

[49] S. Facchinetti, S.A. Osmetti, C. Tarantola, "A statistical approach for assessing cyber risk via ordered response models," *Risk Analysis*, vol. 44, no. 2, pp. 425–438, 2023, doi: 10.1111/risa.14186.

[50] K. Ostrovska, R. Beday, "Productivity study of volume data normalization methods," *System Technologies*, vol. 3, no. 128, pp. 165–175, 2020, doi: 10.34185/1562-9945-3-128-2020-15.

[51] M. Dekker, L. Alevizos, "A threat-intelligence driven methodology to incorporate uncertainty in cyber risk analysis and enhance decision-making," *Security and Privacy*, vol. 7, no. 1, 2023, doi: 10.1002/spy2.333.

[52] B. Gokkaya, L. Aniello, E. Karafili, B. Halak, "A methodology for cybersecurity risk assessment in supply chains," *Computer Security, ESORICS 2023 International Workshops*, pp. 26–41, 2024, doi: 10.1007/978-3-031-54129-2_2.

[53] C. Cioaca, C.-G. Constantinescu, M. Boscoianu, R. Lile, "Extreme Risk Assessment Methodology (ERAM) in aviation systems," *Environmental Engineering and Management Journal*, vol. 14, no. 6, pp. 1399–1408, 2015, doi: 10.30638/eemj.2015.152.

[54] P. Nakamura, *Implementing a quantitative risk management methodology in a cyber exercise*, Master's Thesis, JAMK University of Applied Sciences, 2020. [Online]. Available: https://www.theseus.fi/bitstream/handle/10024/354191/Masters_Thesis_Nakamura_Petteri.pdf?sequence=2&isAllowed=y. [Accessed: Jun. 19, 2023].

[55] *Science for disaster risk management 2017: knowing better and losing less*, K. Poljanšek, M. Ferrer, M. De Groeve, T. Clark, Eds., Luxembourg, Publications Office of the European Union, 2017.

[56] A.P. Duka, "Risk mapping in the organization's integrated risk management system," *Effective Economy*, no. 10, 2017.

[57] *Threat actors' attack strategies. Work Package 2: Cyber–threat landscape and end–user requirements*, Dec. 31, 2018. [Online]. Available: https://cyber-trust.eu/wp-content/uploads/2020/02/D2.5.pdf. [Accessed: Jun. 16, 2023].

[58] ENISA. (2019). *Online platform for security of personal data processing*. [Online]. Available: https://www.enisa.europa.eu/publications/reinforcing-trust-and-security-platform. [Accessed: Jun. 10, 2023].

[59] D.W. Hubbard, R. Seiersen, D.E. Geer Jr, S. McClure, *How to Measure Anything in Cybersecurity Risk,* 2nd Edition, New Jersey: John Wiley & Sons, 2023.