Research Square

Preprints are preliminary reports that have not undergone peer review.
They should not be considered conclusive, used to inform clinical practice,
or referenced by the media as validated information.

A comparative analysis of threat models in the context of cyber threat attribution

Viktor Szulcsányi

szulcsanyi.viktor@uni-obuda.hu

Óbuda University

Sándor Magyar

University of Public Service

Research Article

Keywords: Cyber threats, attribution, CTI, indicators, threat actors, attribution model

Posted Date: September 15th, 2025

DOI: https://doi.org/10.21203/rs.3.rs-7496589/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License.
Read Full License

Additional Declarations: No competing interests reported.

A comparative analysis of threat models in the context of cyber threat attribution

Viktor Szulcsányi · Sándor Magyar

Received: date / Accepted: date

Abstract The role of cyberspace in geopolitical conflicts - as the experience of recent decades clearly demonstrates - is continually expanding. The activities of state sponsored and other cyber actors are becoming increasingly frequent, complex, and sophisticated. To understand and analyze a potential cyberattack in detail, it is essential to identify and select an appropriate analytical framework. There are currently several frameworks and models for analyzing cyber threats, but these were developed for different purposes and primarily focus on technical analysis. However, when analyzing a complex attack, we must also consider additional non-technical aspects that are not or are only partially covered by the known models. This research aims to conduct a comparative analysis of publicly available threat models and frameworks, with a particular focus on their applicability in the context of cyber threat attribution. The study evaluates the applicability of individual frameworks during attribution based on a uniquely created set of criteria. The purpose of the comparative analysis is to understand the strengths, weaknesses, and shortcomings of individual models in light of the identification of cyber actors behind cyber threats.

Keywords Cyber threats · attribution · CTI · indicators · threat actors · attribution model

Viktor Szulcsányi
Doctoral School on Safety and Security Sciences, Óbuda University, Budapest, Hungary
E-mail: szulcsanyi.viktor@uni-obuda.hu

Sándor Magyar
Institute of National Security, Ludovika University of Public Service, Budapest, Hungary
E-mail: magyar.sandor@uni-nke.hu

1 Introduction

In the digital age, cyberspace has become a critical area for political, economic, and military activities, making its protection an essential part of our daily lives. Cybersecurity is strategically vital for both nation-states and private-sector actors. With the development of cyber threats at the operational and technical levels, incident management and the field of Cyber Threat Intelligence (CTI), which analyzes and evaluates cyber threats, are also constantly adapting new methods and procedures to expand capabilities and defend against malicious cyber activities. Key to the success of these processes is the real-time detection of attacker activity, predicting potential attacks, and analyzing and understanding incidents that have already occurred in detail, with the aim of not only mitigating the damage caused by individual cybersecurity incidents, but also strengthening preventive capabilities against future threats and supporting related strategic processes. [1] Cyber events can have a significant impact on the geopolitical situation in certain regions, which is why understanding and attributing cyber threats has become a critical element of security for a given nation or industrial sector. The motivations and technical characteristics of cyber actors generally differ significantly from one another. The primary goal of state-sponsored APT groups is to conduct intelligence and espionage operations that support their nation's interests. Their activities are generally characterized by a high level of planning and preparation, adherence to OPSEC procedures, efforts to make their activities difficult to detect, and a focus on persistence. In sharp contrast, hacktivist groups select their targets on a much more ideological basis and most often openly claim responsibility for attacks aimed at causing disruption or drawing atten-

tion to various political or social situations or events. These differences are reflected in the technical characteristics of cyberattacks, their timing, their targets, and other attributes that can be critical factors in identifying and attributing the activity. Different threat models can provide a structured framework for identifying and analyzing the attributes of a potential attack, including the cyber actor's toolkit, the techniques and infrastructure they employ, and other factors contributing to the attack. With their help, incident response professionals can identify patterns in the available data set, thereby facilitating the process of determining the attacker. Advanced Persistent Threats (APTs) use defined TTPs to conduct their attacks. Identifying these patterns is vital to enhancing threat detection and response. Frameworks play a key role in mapping and analyzing APT activities. [2] CTI frameworks, such as the Diamond Model, MITRE ATT&CK, and Cyber Kill Chain, aid in analyzing and understanding cyber threats. [3] Frameworks such as MITRE ATT&CK, the Unified Kill Chain, and the Diamond Model of Intrusion Analysis offer different perspectives and analytical tools for understanding attacker behavior. However, it is essential to note that there is no universally applicable CTI framework, as each organization has its own unique needs and environment. [4] This study aims to examine and evaluate the strengths, limitations, and applicability of threat models in light of the criteria necessary for realistic attribution.

2 Methods

This study is a comparative analysis that aims to compare publicly available, well-known threat models based on their ability to support the attribution of cyber activities. The background to the study was to determine the extent to which each framework can support the identification of the groups behind cyberattacks and how they contribute to the implementation of technical, operational, and strategic-level analyses. During the research, I used both qualitative and quantitative methods, combining the processing of theoretical literature with practical evaluation criteria. Data collection relied primarily on secondary sources, including scientific articles, materials from professional organizations dealing with cybersecurity, periodic industry reports, and white papers. Quantitative analyses were primarily used to examine the prevalence of individual frameworks. Based on the information processed, eight different threat models were identified and evaluated. As part of the data collection process, other less prevalent models were also explored; however, they did not ultimately form a central part of the analysis. An essential consideration in the selection process was that, of the models that showed significant similarities, only those that best met the specified evaluation criteria were used in the study. The criteria used in the comparative analysis were developed on the basis of individual criteria, taking into account not only technical indicators but also other aspects that facilitate attribution. For each model, I rated the compliance with the specified criteria on a four-point scale (Not applicable, Low, Medium, High), and I provided brief professional explanations for the ratings, taking into account the documentation available for the model, examples of the application of the framework, and previously published scientific publications. My own research activity included compiling a set of criteria used as a basis for comparison, evaluating the analysis results, and creating a new six-dimensional attribution model that integrates the strengths of the different models. During the analysis, I sought to identify the limitations and strengths of each model in other contexts. I defined the dimensions of the new framework based on the common intersection and practical shortcomings of existing frameworks.

3 A proposed methodology for the analysis of the activities of attack groups

Attacker groups—also known as cyber threat actors — are organized, usually well-coordinated groups that carry out cyber attacks in a deliberate and targeted manner. We consider any cyber actor to be an attacker group if it:

- carries out targeted cyber activities,
- exhibits repetitive attack patterns,
- and has identifiable motivations (e.g., political, economic, ideological, military objectives).

Attacker groups are organizations or individuals that carry out regular or targeted cyber attacks to achieve various goals. These groups may have different backgrounds and may have different motivations and resources. We can distinguish four major groups based on their motivations and goals. Political, economic, or military goals mostly drive state-sponsored cyber actors or APT groups. In general, they are well-funded and possess a high level of technical expertise, to gain long-term, covert access and collect information valuable to the nation behind them. Cybercriminal groups conduct their activities primarily for financial gain, often involving phishing, ransomware attacks, the sale of malicious services, or other illicit cyber activities. Hacktivists carry out their activities for ideological or social purposes, actively spreading their views through

web defacement or denial-of-service attacks. In addition to the above, in the context of motivations and goals, we can also discuss individual attackers who carry out attacks for personal gain, most often acting independently. The activities of attacker groups can range from carefully planned, step-by-step attacks to improvised attacks. State-sponsored groups are best characterized by precision, deliberation, and persistence, while hacktivist groups most often launch quick, attention-grabbing attacks. The key elements of defense include a detailed analysis of activities, identification of indicators, exploitation of vulnerabilities, and other methods used by perpetrators. Threat models help to systematize the characteristics and attributes of activities.

4 Criteria to be applied in order to facilitate a comparison of threat models

Although publications have already appeared on the examination of threat models, they primarily examine the role of certain models in supporting the incident management process. [5] This study focuses specifically on the technical support options for attribution activities, therefore it was necessary to develop a unique set of criteria for the comparative analysis. The effectiveness of a threat model can be measured in a number of ways. To support attribution, the threat model must be sufficiently complex and capable of providing a detailed and comprehensive analysis of attacker activity. [6] The following factors, among others, may play a key role in the evaluation of a threat model:

- Applicability;
- Familiarity and prevalence of the model;
- Coverage of the entire attack lifecycle;
- Role of technical and non-technical indicators;
- Behavioral and tactical characteristics and details of TTPs (Tactics, Techniques, and Procedures) [7]
- Display of malicious codes and infrastructure used;
- Motivation, presumed purpose of the attack (financial gain, political interest, etc.);
- Direct and indirect effects of the attack;
- Integration and display of all actors involved in the attack in the model (attacker and victim).

The above criteria provide an opportunity to compare different threat models not only on a theoretical basis, but also as practical tools that can be applied in real-world scenarios. Each of the factors listed represents a detail or perspective that is essential in attribution and defense. Applying this set of criteria can contribute to selecting the appropriate model when handling a specific incident, and it also helps to reduce attribution uncertainties and provide a basis for decision-making processes. In order to support the legal process of attribution, it is essential that the model be able to handle factors and contradictions that cause uncertainty, as the steps leading to attribution must be legally sound, unobjectionable, and valid in the field of international law, since a wrongly attributed cyberattack could even lead to serious international conflict. [8]

5 Selection process of threat models

The primary objective of the study was to compare known threat models based on the criteria described in the previous chapter and, as a result, to determine which of the frameworks used in the analysis is capable of fully supporting the attribution process.

5.1 Criteria for selecting threat models

During the research, cyber threat models were selected that are relevant from the perspective of attribution analysis and represent different approaches to understanding and identifying attacks. The selection took into account the prevalence of the models, their areas of application, and the extent to which they support the identification of attackers and the prevention of attacks. The eight models selected are: Cyber Kill Chain, Unified Kill Chain, MITRE ATT&CK, Diamond Model of Intrusion Analysis, CAPEC, Pyramid of Pain, Triangle Model, and Bayesian Attack Model. Although all of these models can be used to analyze cyber threats, they highlight different aspects, such as the phases of the attack chain, the tactics and techniques used by attackers, and the possibilities for attributing attacks.

5.2 Cyber Kill Chain

The Cyber Kill Chain model, developed in 2011 by Lockheed Martin, a company specializing in defense technologies, provides a structured representation of the steps involved in executing cyber attacks. The model distinguishes seven phases as part of the attack process: Reconnaissance, Weaponization, Delivery, Exploitation, Installation, Command and Control, Actions on Objectives. [9] This is one of the oldest models used in research, which remains a reliable reference point for investigating cybersecurity incidents. However, several shortcomings have been identified in the model in the area of attribution.

5.3 MITRE ATT&CK

The MITRE ATT&CK -, which stands for Adversarial Tactics, Techniques, and Common Knowledge - framework was created by MITRE Corporation in 2013. The purpose of the framework is to document and categorize attacker tactics and techniques, as well as to support threat detection and preventive measures. [10] MITRE ATT&CK is the most commonly used threat model in cybersecurity, providing technical guidance for describing and evaluating the activities of cyber actors. This knowledge base, which contains detailed descriptions of the tactics, techniques, and procedures used by attacker groups, as well as recommendations for potential defensive measures, is continually updated to reflect both the various phases of attack lifecycles and the methods employed. The MITRE ATT&CK framework is widely regarded as the de facto standard for security threat modeling. [11]

5.4 Unified Kill Chain

The Unified Kill Chain model was developed by Paul Pols in 2017. The model was essentially created by integrating the Cyber Kill Chain and MITRE ATT&CK frameworks. [12] It compensates for the shortcomings of the underlying Cyber Kill Chain, which focuses mainly on attackers and malware, by implementing the tactics known from the MITRE ATT&CK framework, thus covering the entire attack lifecycle in detail. The model defines a total of 18 steps across three phases, covering the entire spectrum of attacks, including initial access, maintaining a persistent presence, and achieving the objective. This allows for the fine-tuning of defense strategies and a better understanding of attacks. [13]

5.5 Diamond Model of Intrusion Analysis

Sergio Caltagirone and his co-authors published their research on the creation of the Diamond Model of Intrusion Analysis framework in 2013. The model identifies four main elements: attacker, capability, infrastructure, and victim, which appear as the vertices of a diamond shape. This model enables a detailed analysis of attacks and the mapping of relationships and correlations behind them, which is particularly useful in attribution analysis. Applying the model fosters a deeper understanding of threats and enables more effective planning of defensive measures. [14]

5.6 CAPEC

CAPEC (Common Attack Pattern Enumeration and Classification) is an open-source database associated with the MITRE Corporation. It is primarily used to document and classify attack patterns, thereby helping organizations identify vulnerabilities in their systems and develop defense strategies. CAPEC can be particularly useful for developers and security analysts, as it provides detailed information on attack techniques and how to prevent them. [15] Unfortunately, however, beyond technical indicators and TTPs, it is unable to handle other parameters necessary for attribution support, or can only partially hold them. [16]

5.7 Pyramid of Pain

The Pyramid of Pain model was published by David Bianco in 2013 with the aim of illustrating the role of technical indicators defined by the model in the activities of attackers. At the bottom of the pyramid are easily changeable indicators (e.g., hashes), while at the top are elements that are difficult for attackers to change (e.g., TTPs). [17] This model primarily provides guidance in determining task priorities when developing detection capabilities and highlights the effectiveness of individual defense mechanisms.

5.8 Triangle Model

The Triangle Model threat model was created and presented by Arun Warikoo in 2021. The model rests on three main pillars: sector, tools, and tactics, techniques, and procedures (TTPs). [2] The model focuses specifically on the attribution of APT group activities, which sets it apart somewhat from threat frameworks used primarily for incident management purposes. However, the three pillars defined do not cover the full spectrum of factors that can be taken into account during attribution.

5.9 Bayesian Attack Model

The Bayesian Attack Model is a graph-based threat model that employs a probabilistic approach, considering the relationships between various events and their corresponding probabilities of occurrence. This model is particularly useful for dealing with complex attacks and uncertainties. Although the model is significantly more complex to apply than the frameworks described above, its advantage is that it can handle incomplete

or uncertain information, which often occurs during the investigation of a cybersecurity incident. [18]

6 Results

Attributing cyber threats is a complex problem that requires the combined interpretation of various types of indicators and other factors. The aim of this research is to explore the extent to which each model can support the various processes of attribution, based on an evaluation criteria system that serves as the basis for a comparative analysis of carefully selected threat models. A qualitative analysis method was used in the study, with a structured criteria system providing the framework for the evaluation. Following the preliminary assessment and selection of threat models based on primary and secondary sources, the existence of factors necessary to support the attribution process and their role in the given model provided the basis for comparison, enabling the identification of the strengths and weaknesses of each model. A four-point rating scale was used for each model and criterion:

- Not applicable;
- Low (minimal support for the criterion);
- Medium (partially or indirectly applicable);
- High (clear and explicit support).

During the evaluations, the publicly available documentation of the threat model was taken into account, as well as known examples of its application. The purpose of the comparative analysis was not to rank the models, but to identify their applicability in the attribution process.

The summarized assessments given for each aspect as shown in Table 1 can be supported by the following qualitative textual explanations. The Cyber Kill Chain breaks down attacks into seven linear steps, according to the tasks required to prepare and execute the attack. This structured approach effectively supports the identification of technical indicators. The model is not sufficiently detailed to recognize and comprehensively analyze the TTPs of an attack, and it does not examine the individual phases of the attack lifecycle, such as the operations following initial access, in depth; therefore, it is only partially applicable in this area. The model has limited ability to handle non-technical indicators, such as timestamps or character encoding, which are better covered by other, more detailed attribution models, such as the Diamond Model. The infrastructure used for the attack (e.g., C2 systems, exploits) is included in the model, but even in this case, there is a lack of detail regarding this factor. The model does not emphasize the motivations of the attackers or their geopolitical context, nor do these aspects fit into the model retrospectively, so they cannot be interpreted in relation to it. It also lacks an assessment of the potential impact of attacks and an evaluation of attribution uncertainty or reliability, which is not negligible in the attribution process. The Cyber Kill Chain can therefore be interpreted primarily as a general technical and tactical framework; however, it is insufficient on its own for broader and deeper technical analyses. MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) is one of the best-known and most widely used frameworks, created primarily to catalog technical and tactical patterns of attacker behavior. The system, which is used to analyze the activities of cyber actors, contains extremely detailed technical indicators, including the techniques, tools, and C2 infrastructure used in attacks. The matrix-structured indicator system allows cybersecurity researchers and experts to compare events detected in their own environment with known attack methods, thereby effectively supporting the incident management and preparedness process. [19] MITRE ATT&CK is primarily technically focused, and although it can indirectly handle certain non-technical indicators, these are not part of the applied assessment criteria. It only partially displays operational and infrastructure indicators, and in many cases, these are not identified in sufficient detail. The primary strength of the MITRE ATT&CK model lies in its integration and processing of behavioral and tactical characteristics, specifically TTPs. This aspect is extremely important in mapping the attack capabilities of a given cyber actor and in identifying opportunities for defense or detection against attacks. [20] Although the model does not directly analyze the objectives and effects of the attack, the analysis of the techniques used often allows conclusions to be drawn about the victim's profile and the nature of the attack. The framework does not examine the attackers' motivations or the geopolitical context of cyber activities, as these fall outside the scope of its defined criteria. The comparability of the techniques used by attackers makes the model partially suitable for addressing attribution uncertainty; however, it does not encompass all factors that influence the reliability of attribution. The MITRE ATT&CK framework is therefore excellent for technical-level analysis, particularly for creating detection patterns. However, for higher-level strategic interpretation or geopolitical assessment, it needs to be combined with other models, which limits its effectiveness to supporting only a narrower part of the entire attribution process. The Unified Kill Chain model is a combined, enhanced version of the previous two models. It focuses on the entire lifecycle of attacks, sup-

Model	Technical indicators	Non-technical indicators	Operational and infrastructure indicators	Tactical and behavioral characteristics (TTP)	Impact and purpose	Motivation	Geopolitical context	Attribution uncertainty
Cyber Kill Chain (CKC)	High	Low	Low	Medium	Low	Not applicable	Not applicable	Not applicable
Unified Kill Chain (UKC)	High	Medium	High	High	Low	Not applicable	Not applicable	Not applicable
Diamond Model	Low	High	Medium	Medium	Medium	Medium	Not applicable	Medium
MITRE ATT&CK	High	Low	High	High	Low	Not applicable	Not applicable	Not applicable
CAPEC	Low	Not applicable	High	Low	Not applicable	Not applicable	Not applicable	Not applicable
Pyramid of Pain	Medium	Not applicable	Low	Medium	Low	Not applicable	Not applicable	Not applicable
Triangle Model	Low	Not applicable	Low	Low	Not applicable	Not applicable	Not applicable	Not applicable
Bayesian Attack Model	High	High	High	Low	Low	Medium	Medium	Medium

Table 1 Comparison of Selected Threat Models

plementing the Cyber Kill Chain structure with additional attack vectors, phases, and the ability to recognize recurring attack patterns. At the technical indicator level, the model offers significant progress, as it covers the various technical aspects of an attack in detail—including various exploits, malware, and network activities—thereby supporting more accurate detection and response. The model does not focus on the analysis of metadata, timestamps, and other non-technical indicators; however, these can be taken into account in specific phases. The model essentially handles TTPs based on the MITRE ATT&CK framework, making it well-suited to support the attribution process in relation to the aspects mentioned above, along with high-level handling of operational and infrastructure indicators. It can only analyze the effects and objectives of attacks retrospectively and, similar to the underlying frameworks, completely ignores geopolitical contexts and motivations. These shortcomings also limit the model's ability to handle attribution uncertainty. The Unified Kill Chain is a highly applicable, technically focused threat model that can be particularly advantageous when setting up a structured and cyclically updatable attack model. Compared to the models already described, the Diamond Model for Intrusion Analysis takes a more complex and structured approach to analyzing cyber threats, based on four fundamental factors—adversary, capability, infrastructure, and victim—and their interrelationships. The Diamond model facilitates the structuring of cyber attack scenarios, reduces dependency on individual analysts, and provides a systematic approach to threat modeling. [21] The model can handle both technical and non-technical indicators—although it only partially takes the latter into account—thus providing a comprehensive solution for analyzing the details of an attack. Compared to previous frameworks, the Diamond Model emphasizes non-technical metadata such as timestamps, behavior patterns, typos, and linguistic characteristics, in addition to IP addresses, domain names, hash values, exploits, and other technical indicators. This approach makes the model particularly suitable for use in early threat detection and attribution support. The model is suitable for analyzing infrastructure, including its role and the connection between attackers and victims. Documenting attack tactics and techniques (TTPs) is also a key element that contributes to understanding attacker behavior. A unique feature of the Diamond Model is that it also allows for a detailed examination of the target (victim), thus indirectly addressing the purpose of the attack and its potential effects. The motivation of the attackers is also an indirect element in the application of the model, mainly taken into account during the analysis of the targets. The model does not thoroughly examine the geopolitical context, which is a notable shortcoming in terms of attribution activities. The model supports the substantiation of attribution conclusions, thus helping to reduce uncertainty in identifying attackers in cyberspace by revealing connections. In practice, the Diamond Model is often used in conjunction with other frameworks, such as the Cyber Kill Chain, to support technical analysis more effectively. However, this common set of criteria eliminates the possibility of flexible application of the four fundamental factors, thereby

limiting the potential for utilizing this fundamentally strategic model. Overall, the Diamond Model is a holistic, multidimensional solution that provides a comprehensive picture of the characteristics of an attack and can effectively support the attribution process. However, the strategic approach underlying the model can also lead to a simplification of the characteristics of the attack, as the four predefined categories are not capable of handling all attribution factors. CAPEC (Common Attack Pattern Enumeration and Classification) is an open, systematic knowledge base designed to categorize different attack patterns from a technical perspective. The model is primarily used in application security testing, so unlike the ATT&CK framework, also developed by MITRE, it is not intended to support comprehensive protection of IT systems and cover the entire attack process from initial access to data exfiltration. CAPEC is used to identify and define exploit types, vulnerabilities that can be exploited during attacks, and the tactics, techniques, and procedures used by attackers. The model itself has a very narrow scope of interpretation in terms of attribution. It can only handle technical indicators indirectly and does not consider non-technical indicators at all. It has limited applicability to the analysis of the infrastructure used by attackers, such as command-and-control systems, VPS providers, or network geolocation. The CAPEC framework does not address the attacker's motivation, geopolitical background, or uncertainty regarding attribution. About the aforementioned results, it should be emphasised that although the CAPEC framework is not suitable for use in the attribution or even detection process on its own – as it is primarily intended to support application security – it can be effectively integrated into other frameworks to facilitate understanding of the technical aspects of attacks. David J. Bianco created the Pyramid of Pain. [17] The model encompasses a broad range of technical indicators, including IP addresses and hash identifiers, as well as characteristics based on attackers' tactics, techniques, and procedures, which are considered the highest level of interpretation in the model. The model also illustrates the extent to which the use of different types of indicators in defense can make the attackers' job more difficult. The Pyramid of Pain was primarily created to examine the technical aspects of a cyberattack and thus support the defense process. It can confidently handle technical indicators, which is clearly one of the model's strengths. Elements related to the attacker's infrastructure, such as C2 servers or domain names, also appear at certain levels of the model, but no additional context is assigned to them; these aspects are only considered to enhance the effectiveness of the detection process. The model is unable to handle non-technical indicators, nor does it account for aspects related to the purpose of the attacks, their potential effects, the geopolitical context, or the motivations of the attackers. Due to these shortcomings, it lacks a dedicated mechanism for handling attribution uncertainty. Overall, Pyramid of Pain is well-suited for detection tasks [22], but it is a one-dimensional threat model that cannot be used on its own to support attribution activities. The Triangle Model for Cyber Threat Attribution is a relatively uncommon model for analyzing cyber threats, focusing on the attacker's target, tools, and behavior-based patterns. In terms of applicability, the model can be interpreted as a simplified TTP-oriented solution, which has been supplemented by examining the target selection method. When examining TTPs, it may be helpful to use this model in conjunction with other frameworks, such as MITRE ATT&CK, to compare behavioral patterns, as the Triangle Model contains less detailed instructions. Technical indicators, such as hashes, IP addresses, or domain names, are challenging to integrate into the analysis process of the three pillars of the Triangle Model, as the model can only handle them indirectly. Specific technical characteristics, such as the infrastructure used by the devices, also appear, but they are not analyzed in detail. In the absence of sufficiently defined steps, these indirectly appearing aspects are not necessarily available when comparing two attack methods for attribution purposes. In a narrow sense, non-technical indicators cannot be integrated into any of the three pillars of the model. The geopolitical context appears to a limited extent in the analysis of targets, as do the purpose and impact of the attack, as well as the motivation behind the activity. The framework is not suitable for addressing attribution uncertainty, mainly because most of the criteria defined to support the attribution process can only be addressed indirectly or tangentially by the Triangle Model. The Triangle Model is therefore a framework representing a unique approach, which, on its own, is not suitable or only appropriate to a limited extent, but in combination with other frameworks can be used effectively to support both detection and attribution processes. [2] The Bayesian Attack Model provides one of the most complex yet flexible approaches to threat modeling. Through the application of probabilistic graphs, a branch of graph theory, it is capable of handling multiple indicators and uncertainties simultaneously. The model is based on Bayes' theorem, which allows us to dynamically conclude the probability, purpose, or origin of an attack based on technical and non-technical data points, such as IP addresses, timestamps, linguistic characteristics, typos, TTPs, or even related geopolitical events. As a result, the integration of tech-

nical indicators and TTPs is not only possible but also a key element in the model's operation. At the same time, non-technical indicators can also play a significant role in weighting probabilities. The model is beneficial in dealing with attribution uncertainty, as it can handle uncertainty on a mathematical basis, which is a unique advantage over other, less mature approaches. However, this process can be significantly influenced by the degree to which all elements of the defined set of criteria are integrated into the model. The geopolitical context and the characteristics of the infrastructure used by the attackers can only be incorporated into the assessment to a limited extent, with the former in particular proving too complex a task to handle within a graph-based framework. The attacker's motivation, as well as the purpose and impact of the activity, are also challenging to fit into the mathematical framework provided by the model. Overall, the strength of the Bayesian Attack Model lies in its reliable interpretation of multidimensional threats, as the graph theory approach it offers can provide a high degree of flexibility and accuracy. In addition to the eight criteria identified as part of the evaluation, the applicability and prevalence of the selected threat models were also examined during the research. Applicability is a fundamentally subjective attribute, which was discussed using empirical methods, so the results described below are based on the author's frequent experience in this regard. Prevalence, on the other hand, can be measured objectively. The table below shows the number of search results for the eight selected threat models based on the results of three major search engines (Google, Bing, DuckDuckGo). The figures are provided for informational purposes only, as search engine algorithms and indexing practices are subject to change over time.

Model name	Google results	Bing results	DuckDuckGo results
Cyber Kill Chain	~1,200,000	~1,000,000	~950,000
Unified Kill Chain	~15,000	~12,000	~10,000
MITRE ATT&CK	~2,500,000	~2,300,000	~2,100,000
Diamond Model of Intrusion Analysis	~25,000	~22,000	~20,000
CAPEC	~35,000	~30,000	~28,000
Pyramid of Pain	~20,000	~18,000	~16,000
Triangle Model	~5,000	~4,500	~4,000
Bayesian Attack Model	~2,000	~1,800	~1,600

Table 2 Search Results for Individual Models Across Various Search Engines

The data summarized in Table 2 help to understand how well-known and widespread certain models are within the professional community. The results of the assessment of applicability and prevalence are illustrated in the diagram shown on Figure 1.

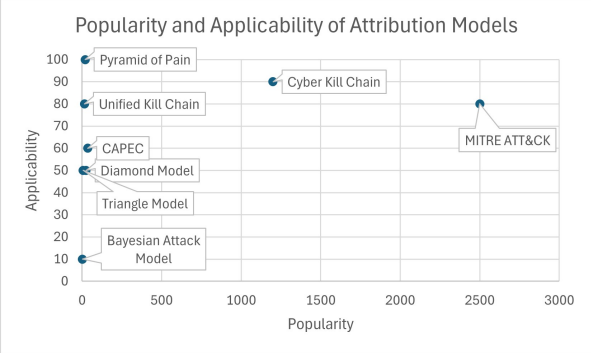

Fig. 1 Attribution models by prevalence and applicability

7 Reasoning behind the need for a new threat model and its structural characteristics – the HexAttribution Model

Attribution of cyber threats — that is, determining exactly who or what organization is behind an attack — is one of the most complex and challenging tasks in cybersecurity. [23] Based on the analysis results presented in the previous chapter, it can be concluded that there is no universal framework among the models examined that is capable of fully supporting the attribution process, as some of the options presented were unable to handle all the key aspects of attribution. In several cases, much greater emphasis was placed on examining a single aspect than would have been justified in terms of the reliability of attribution. A significant proportion of the threat models examined—Cyber Kill Chain, MITRE ATT&CK, Diamond Model, CAPEC, and Triangle Model—focus on a more detailed analysis of one or a few aspects; however, none of them provide a comprehensive, multidimensional framework specifically designed to increase the reliability of attribution. Several models perform exceptionally well in the area of analyzing aspects that form the basis of detection capabilities. Still, they are only able to integrate aspects that can be taken into account specifically in the case of attribution, such as the geopolitical context of the attack, the possible impact and purpose of the activity, the attacker's motivation, and the handling of attribution uncertainty, into the analysis process to a limited extent. The use of a framework that incorporates all of the above criteria can significantly increase the effectiveness and role of attack detection and information sharing in the attribution process. [24] Recognizing this shortcoming led to the development of the HexAttribution model, which aims to provide a coherent and systematic structure for the indicators needed for attribution.

7.1 The structure of the HexAttribution model

The HexAttribution model - as shown in Figure 2 - offers a six-dimensional framework that organizes the following main components:

1. Technical Indicators – IP addresses, hashes, domain names, exploit patterns, and other technical characteristics.
2. Non-Technical Indicators – timestamps, language usage characteristics, steps taken during each phase of the attack, sequence of commands issued, characteristics indicative of the attacker's unique methodology, and other metadata
3. Behavioral and Tactical Indicators – TTPs used and characteristics of the infrastructure operated by or indirectly used by the attacker throughout the entire attack lifecycle.
4. Motivation and Impact – examination of the attackers' motivations for obtaining information, financial gain, or destruction, their related goals, and the expected or actual effects of the attacks.
5. Geopolitical Context – consideration of regional conflicts, political events, and conflicting state interests that may be causally related to the attack.
6. Reliability of Attribution Factors – evaluation of the above factors based on reliability, credibility, and repeatability.

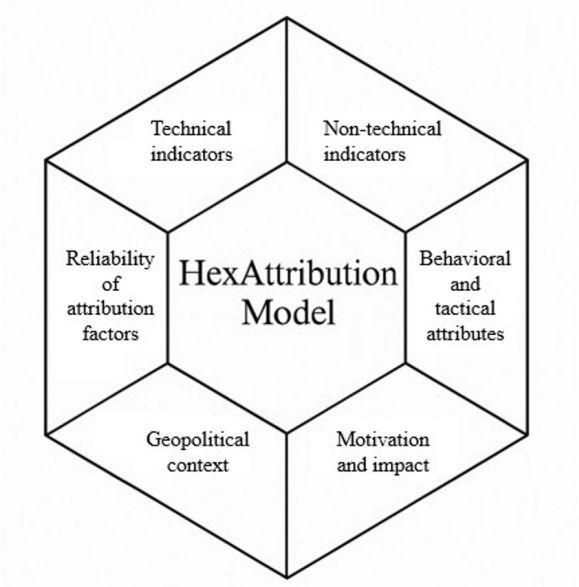

Fig. 2 Diagram of the HexAttribution Model

These six components together offer a structured but flexible framework in which various indicators can be evaluated according to both qualitative and quantitative criteria. The model can be used for both hypothesis based testing and real-time incident analysis. Due to its structured approach, the results of attacks evaluated using the HexAttribution model can be easily compared with each other, simplifying and streamlining the attribution process. Another significant advantage is that the HexAttribution model is specifically designed to address attribution uncertainty, a dimension that most previous models have ignored or treated tangentially. In addition, through strategic-level impact analysis, analysts can handle attacks not only at the technical level as incidents, but also at the management level, supplemented with contextualized strategic-level information. However, the main strength of the HexAttribution model lies in its ability to connect different levels of analysis: from technical details to strategic context. This is particularly useful in cases where it is necessary to provide a comprehensive picture of a cyber actor's activities or the identity of the possible perpetrator behind an attack on a government organization within a relatively short period, using partially reliable information from multiple sources. The structured nature of the model helps reduce the chance of attribution errors, as weighting criteria or reliability indicators can be assigned to each of its components. However, as with any complex framework, the HexAttribution model has limitations, and minor challenges may arise when applying it. The main limitation is the availability and quality of data: the model only works well if sufficient, structured data is available for all aspects under consideration. In addition, the implementation of the model requires a relatively high level of expertise, especially in the case of geopolitical and motivational contexts that can be assessed qualitatively, where subjective interpretations can distort the results.

8 Discussion

The previous chapters described the main aspects identified during the research that should be considered during the attribution process. Each of the specified characteristics can significantly influence the success of identifying threat actors. This article presents the most significant threat models and, based on the established set of criteria, evaluates their applicability in supporting the attribution process using a qualitative method. In this regard, the research highlighted the shortcomings and limitations of frameworks explicitly created to support incident management activities, as well as possible opportunities for improvement through the parallel or combined use of other frameworks that can be considered complementary in terms of the criteria covered by the given model. The results showed that there

is no universal, complex attribution framework among the models examined that meets all the specified criteria; therefore, it became necessary to create a new framework in light of these results. The HexAttribution model offers a novel and versatile approach to supporting the attribution of cyber threats. Thanks to its structure, it can combine information that can be interpreted in both technical and strategic contexts, while also addressing uncertainty in an integrated manner. Thus, it is not just another model in the incident management arsenal, but an attribution-centric, analyst-friendly framework that can be adapted to both current and future cybersecurity challenges. Further development opportunities include partial (focusing on technical aspects) or complete automation of the model's application, for example, through the use of machine learning methods capable of uncovering hidden relationships between different components. Additionally, enhancing the model's interoperability with widely used CTI frameworks, such as STIX (Structured Threat Information Expression) or MISP (Malware Information Sharing Platform), could promote its adoption within the cybersecurity community.

References

1. Lee, M.: "Attribution" in Cyber Threat Intelligence. Wiley. pp. 155-174. (2023) https://doi.org/10.1002/9781119861775.ch6.
2. Warikoo, A.: The Triangle Model for Cyber Threat Attribution. Journal of Cyber Security Technology, 5(3–4), 191–208. (2021) https://doi.org/10.1080/23742917.2021.1895532.
3. Odarchenko, R., Pinchuk, A., Polihenko, O., and Skurativskyi, A.: A comparative analysis of cyber threat intelligence models. CEUR Workshop Proceedings 2025 v3925. pp. 3-12. (2025)
4. Irfan, A. N., Chuprat, S., Mahrin, M. N. and Ariffin, A.: "Taxonomy of Cyber Threat Intelligence Framework". 2022 13th International Conference on Information and Communication Technology Convergence (ICTC). Jeju Island. Republic of Korea. pp. 1295-1300. (2022) https://doi.org/10.1109/ICTC55196.2022.9952616.
5. Mavroeidis, V. and Bromander, S.: "Cyber Threat Intelligence Model: An Evaluation of Taxonomies, Sharing Standards, and Ontologies within Cyber Threat Intelligence". 2017 European Intelligence and Security Informatics Conference (EISIC). Athens. Greece. pp. 91-98 (2017) https://doi.org/10.1109/EISIC.2017.20.
6. Prasad, N., Diro, A., Warren, M., and Fernando, M.: A survey of cyber threat attribution: Challenges, techniques, and future directions. Computers & Security. Volume 157. 104606. ISSN 0167-4048. (2025) https://doi.org/10.1016/j.cose.2025.104606.
7. Maymi, F., Bixler, R., Jones, R. and Lathrop, S. "Towards a definition of cyberspace tactics, techniques and procedures". 2017 IEEE International Conference on Big Data (Big Data). Boston, MA, USA. pp. 4674-4679. (2017) https://doi.org/10.1109/BigData.2017.8258514.
8. Banks, W. Cyber Attribution and State Responsibility. International Law Studies. vol. 97. pp. 1039–1072. (2021)
9. Bahrami, P., Dehghantanha, A., Dargahi, T., Parizi, R., Choo, K., and Javadi, H.: Cyber Kill Chain-Based Taxonomy of Advanced Persistent Threat Actors: Analogy of Tactics, Techniques, and Procedures. Journal of Information Processing Systems, 15(4), 865-889. (2019) https://doi.org/10.3745/JIPS.03.0126.
10. Strom, B., Applebaum, A., Miller, D., Nickels, K., Pennington, A. and Thomas, C.: MITRE ATT&CK®: Design and Philosophy. MITRE Corporation. McLean, VA, USA. Tech. Rep. MP180360R1. (2018)
11. Kim, H., Kim, H.: Comparative Experiment on TTP Classification with Class Imbalance Using Oversampling from CTI Dataset. Security and Communication Networks. 5021125. (2022) https://doi.org/10.1155/2022/5021125
12. Pols, P., Domínguez, F.: The Unified Kill Chain. https://www.unifiedkillchain.com/assets/The-Unified-Kill-Chain.pdf. Accessed on August 27, 2025 (2021)
13. Hutchins, E., Cloppert, M. and Amin, R.: "Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains". 6th International Conference on Information Warfare and Security, ICIW 2011. no. July 2005. pp. 113–125. (2011)
14. Caltagirone, S., Pendergast, A. and Betz, C.: The Diamond Model of Intrusion Analysis. (2013) https://doi.org/10.13140/RG.2.2.31143.56481.
15. Gilmore, J., Moore, U. V., Yuan, X., Headen, T., and Vanamala, M.: Visualization Dashboard for Recommending Attack Patterns Using Topic Modeling. In Proceedings of the 2023 12th International Conference on Software and Information Engineering. pp. 46-51. (2023)
16. Barnum, S.: Common attack pattern enumeration and classification (capec) schema description. Cigital Inc, 3. Department of Homeland Security. (2008)
17. Bianco, D.: Pyramid of Pain. Accessed on August 27, 2025. http://detect-respond.blogspot.gr/2013/03/the-pyramid-of-pain.html (2013)
18. Aguessy, F., Bettan, O., Blanc, G., Conan, V., and Debar, H.: Bayesian Attack Model for Dynamic Risk Assessment. (2016) https://doi.org/10.48550/arXiv.1606.09042
19. Al-Sada, B., Sadighian, A. and Oligeri, G.: "Analysis and Characterization of Cyber Threats Leveraging the MITRE ATT&CK Database" in IEEE Access. vol. 12. pp. 1217-1234. (2024) https://doi.org/10.1109/ACCESS.2023.3344680.
20. Abo-alian, A., Youssef, M. and Badr, N.L.: A data-driven approach to prioritize MITRE ATT&CK techniques for active directory adversary emulation. Sci Rep 15, 27776 (2025). https://doi.org/10.1038/s41598-025-12948-x
21. Fujita, J., Ogura, T., Okochi, K., Matsumoto, N., Sawada, K., and Kaneko, O.: The structured cyber attack scenario expression model based on diamond model and adversarial states. IEEJ Transactions on Electronics, Information and Systems, 142(3), pp. 328-338. (2022)
22. Tatam, M., Shanmugam, B., Azam, S., Kannoorpatti, K.: A review of threat modelling approaches for APT-style attacks. Heliyon, Volume 7, Issue 1. ISSN 2405-8440. (2021) https://doi.org/10.1016/j.heliyon.2021.e05969.
23. Chen, Z. -S. et al.: Clustering APT Groups Through Cyber Threat Intelligence by Weighted Similarity Measurement in IEEE Access. vol. 12. pp. 141851-141865. (2024) https://doi.org/10.1109/ACCESS.2024.3469552
24. Satvat, K., Gjomemo, R. and Venkatakrishnan, V. N.: "Extractor: Extracting Attack Behavior from Threat Reports" 2021 IEEE European Symposium on Security and Privacy (EuroS&P). Vienna, Austria. pp. 598-615. (2021) https://doi.org/10.1109/EuroSP51992.2021.00046