risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Iberian Journal of Information Systems and Technologies

Recebido/Submission: 16/02/2025
Aceitação/Acceptance: 22/06/2025

Revisão Sistemática sobre Frameworks de Modelagem de Ameaças em Segurança Cibernética

Edvan Gomes da Silva[1], Fernando Rocha Moreira[1], Georges Daniel Anvame Nze[1], João José Costa Gondim[1], Rafael Rabelo Nunes[1,2].

edvan402@gmail.com; frochamoreira@gmail.com; georges@unb.br; gondim@unb.br; rafaelrabelo@unb.br

[1] Programa de Pós-Graduação Profissional em Engenharia Elétrica – PPEE - Universidade de Brasília, Faculdade de Tecnologia, Departamento de Engenharia Elétrica, Brasília, Brasil - Zipcode 70910-900.

[2] Centro Universitário UniAtenas, Paracatu-MG, Brasil – Zipcode 38602-108 .

Pages: 74-87

Resumo: A modelagem de ameaças é reconhecida como ferramenta essencial para categorizar e avaliar sistematicamente a segurança de sistemas, produtos e serviços. Compreender *frameworks* que organizam a modelagem de ameaças torna-se essencial para fortalecer a segurança cibernética das organizações. Nesse sentido, o objetivo deste estudo foi avaliar o uso dessas ferramentas na comunidade científica. A metodologia adotada consistiu em uma revisão bibliográfica sistemática que avaliou 35 artigos relacionados à segurança cibernética que utilizaram algum desses *frameworks* . Os resultados destacam o *framework* MITRE ATT&CK como predominante. Esses resultados contribuem para um panorama abrangente sobre métodos de modelagem de ameaças, auxiliando gestores na tomada de decisões em segurança cibernética. O estudo também relaciona os *frameworks* mais citados e suas tendências atuais. O estudo também reforça uma visão abrangente sobre o uso de *frameworks* de modelagem de ameaças e fornece diretrizes para futuras pesquisas e aplicações práticas neste campo.

Palavras-chave: Modelagem de ameaças; segurança cibernética; *frameworks*; Mitre Att&ck.

Systematic Review of Threat Modeling Frameworks in Cybersecurity

Abstract: Threat modeling is recognized as an essential tool for systematically categorizing and evaluating the security of systems, products, and services. Understanding frameworks that organize threat modeling becomes crucial for enhancing the cybersecurity of organizations. In this context, the aim of this study was to assess the use of these tools within the scientific community. The adopted methodology involved a systematic literature review that evaluated 35 articles related to cybersecurity that utilized one of these frameworks. The results highlight the MITRE ATT&CK framework as predominant. These findings contribute to a comprehensive overview of threat modeling methods, assisting decision-makers in cybersecurity. The study also identifies the most cited frameworks and their current

trends. Furthermore, the study reinforces a comprehensive view of the use of threat modeling frameworks and provides guidelines for future research and practical applications in this field.

Keywords: Threat modeling; cybersecurity; frameworks; Mitre Att&ck.

1. Introdução

A crescente dependência de sistemas para processamento e transmissão de informações sensíveis torna a sociedade vulnerável a ameaças que afetam setores críticos, como energia, justiça, saúde e transporte (Lima et al., 2022; Alves et al., 2023; Silva, 2019; Rohde & Schwarz, 2025). Muitas organizações ainda não estão preparadas para lidar com ataques ou falhas nesses ambientes (Juuso, 2019). O custo global do cibercrime deve alcançar US$ 10,5 trilhões em 2025, enquanto a sofisticação dos ataques desafia abordagens tradicionais de defesa e impulsiona a adoção de novos paradigmas, como o Zero Trust (Secureworks, 2024; Mavroeidis & Bromander, 2017; de Arruda et al., 2023).

Nesse contexto, a modelagem de ameaças é fundamental para identificar riscos e selecionar contramedidas, fortalecendo a confiança e a segurança dos sistemas (Potteiger, Martins & Koutsoukos, 2016; Rodrigues, 2023; Georgiadou, Mouzakitis & Askounis, 2021). Este estudo busca avaliar o uso dessas ferramentas na pesquisa científica e propor diretrizes para futuras investigações.

A presente artigo adota a seguinte organização estrutural: além da introdução, a seção 2 dedica-se ao aprofundamento dos conceitos sobre modelagem de ameaças, e dos principais *frameworks*. A seção 3 contempla a exposição pormenorizada da metodologia empregada no estudo. A seção 4 apresenta de maneira sistemática os resultados obtidos, seguidos de sua devida análise. Por fim, a seção 5 consolida a apresentação conclusiva dos achados, e apresenta as limitações deste estudo.

2. Referencial Teórico

Esta seção apresenta os principais conceitos, métodos e frameworks de modelagem de ameaças em segurança cibernética, que fundamentam as análises desenvolvidas na pesquisa.

2.1. Métodos de Modelagem de ameaças

A modelagem de ameaças é fundamental para estruturar o conhecimento, criar uma linguagem comum e permitir análises detalhadas de riscos em diferentes domínios (Bodeau et al., 2018). Seu objetivo principal é avaliar cenários de ataques e vulnerabilidades, identificando riscos e impactos em ambientes de aplicação (UcedaVelez & Morana, 2015). Exemplos práticos incluem a proteção de ativos e o suporte à colaboração entre equipes desde as fases iniciais do desenvolvimento (Mantha et al., 2020; Rodrigues, 2023).

Diversos métodos, como PASTA, TARA, STRIDE e MITRE ATT&CK, abordam diferentes aspectos dos ataques e ajudam a criar listas de ameaças relevantes (Lohmann, Albuquerque & Machado, 2023). Esses frameworks são classificados em

comportamentais, arquiteturais e táticos, cada um com foco específico na análise e definição de contramedidas (Bodeau, McCollum & Fox, 2018; SAFECode, 2017; Legit Security, 2025).

2.2. Process for Attack Simulation & Threat Analysis – PASTA

O Processo de Simulação de Ataque e Análise de Ameaças (PASTA), criado por UcedaVelez, é uma metodologia centrada em riscos, composta por sete estágios que vão da definição de objetivos à análise de riscos e impacto (Dupont, 2022; UcedaVelez & Morana, 2015). O método utiliza ferramentas como diagramas arquitetônicos e árvores de ataque, adotando uma abordagem centrada no atacante (Puder, Henle & Sax, 2023).

2.3. Threat Analysis and Risk Assessment – TARA

A metodologia TARA, desenvolvida pela Intel IT, busca reduzir o número de ataques focando nas exposições mais prováveis e em agentes de ameaça com objetivos alcançáveis (Rosenquist & Casey, 2009). Para isso, utiliza três bibliotecas: agentes de ameaça, métodos e exposições, o que permite priorizar riscos e orientar medidas de segurança (Karahasanovic et al., 2017).

2.4. Cyber Kill Chain

O Cyber Kill Chain, desenvolvido pela Lockheed Martin, detalha sete fases de ataques cibernéticos, ampliando a visibilidade e o entendimento sobre táticas e procedimentos dos invasores (Martin, 2023; Hutchins, Cloppert & Amin, 2011). O modelo permite antecipar ou interromper ações dos atacantes, prevenindo ou mitigando danos (SentinelOne, 2022).

2.5. STRIDE

O STRIDE, criado na Microsoft, categoriza ameaças em seis tipos, ajudando desenvolvedores a identificar riscos desde o design do software (Shostack, 2014; Hernan et al., 2006). Utiliza diagramas de fluxo de dados para decompor aplicações e avaliar medidas de mitigação (Khan et al., 2024; AbuEmera et al., 2022).

2.6. ATTACK TREE

As árvores de ataque representam ataques de forma hierárquica, facilitando a análise de segurança e a identificação de vulnerabilidades (Schneier, 1999; Saini, Duan & Paruchuri, 2008; Salter, 1998). Elas permitem listar e reutilizar conhecimento sobre ataques, adaptando-se a mudanças e contramedidas (Shostack, 2014; Salter, 1998).

2.7. MITRE ATT&CK

O framework ATT&CK, desenvolvido pelo MITRE, reúne táticas, técnicas, procedimentos e medidas de mitigação para ataques em diferentes ambientes (Strom, 2018; Oruc, Amro & Gkioulos, 2022). Oferece informações sobre grupos adversários, técnicas e softwares, sendo utilizado em iniciativas como o OpenCTI (El Rob et al., 2024; Tavolato, Mohamed & Williams, 2024; Netwerk_LABS, 2023).

Framework	Vantagens Principais	Desvantagens	Referências
PASTA	Abordagem centrada em riscos, estruturada em 7 etapas, foca em falhas de design.	Processo complexo e demorado; exige alto grau de especialização; pode ser difícil de escalar em grandes organizações.	UcedaVelez & Morana, 2015; Puder et al., 2023
TARA	Priorização de ameaças baseada em agentes, uso de bibliotecas para análise detalhada.	Foco restrito a ameaças mais prováveis, podendo negligenciar ameaças emergentes ou de baixa probabilidade.	Karahasanovic et al., 2017; Rosenquist & Casey, 2009
Cyber Kill Chain	Visualização clara das etapas do ataque, útil para resposta e detecção.	Não cobre ameaças internas, ataques pós-exploração ou ameaças modernas como APTs; foco excessivo em ataques externos.	Martin, 2023; SentinelOne, 2022
STRIDE	Fácil de aplicar, cobre seis categorias de ameaças, boa para aplicações de software.	Pode ser simplista, não prioriza ameaças, depende do contexto e experiência do analista; não cobre ameaças humanas.	Shostack, 2014; Hernan et al., 2006
Attack Tree	Estrutura visual e formal, facilita análise de caminhos de ataque e mitigação.	Falta de padronização, cobertura limitada (foco em ataques maliciosos), pode ignorar ameaças acidentais ou internas.	Schneier, 1999; Saini et al., 2008
MITRE ATT&CK	Base de dados ampla, cobre táticas, técnicas, procedimentos e mitigação.	Curva de aprendizado elevada, pode ser difícil de adaptar a contextos específicos, dependência de atualização constante.	Oruc et al., 2022; Strom, 2018

Tabela 1 – Resumo dos Principais *Frameworks* de Modelagem de Ameaças

3. Metodologia

Trata-se de uma pesquisa aplicada, com abordagem quantitativa e objetivos exploratórios. Emprega-se a Teoria do Enfoque Meta Analítico Consolidado (TEMAC), conforme proposta por Mariano e Rocha (2017) para se realizar uma revisão sistemática. Essa metodologia compreende três fases distintas: (i) preparação da pesquisa, (ii) apresentação e análise inter-relacionada dos dados e (iii) detalhamento, criação de um modelo integrador e validação por meio de evidências.

Durante a catalogação dos artigos, utilizou-se o Microsoft Excel para registrar dados bibliográficos, categorizar frameworks e acompanhar critérios de inclusão e exclusão, promovendo controle e transparência no processo, conforme metodologias que empregam planilhas eletrônicas em revisões científicas (Borges et al., 2023). Diferente de revisões sistemáticas que focam em análises quantitativas, este estudo adotou análise qualitativa de conteúdo. Para garantir rigor metodológico, o processo seguiu os princípios do *checklist* PRISMA, considerando suas etapas para identificação, triagem, elegibilidade e inclusão dos estudos.

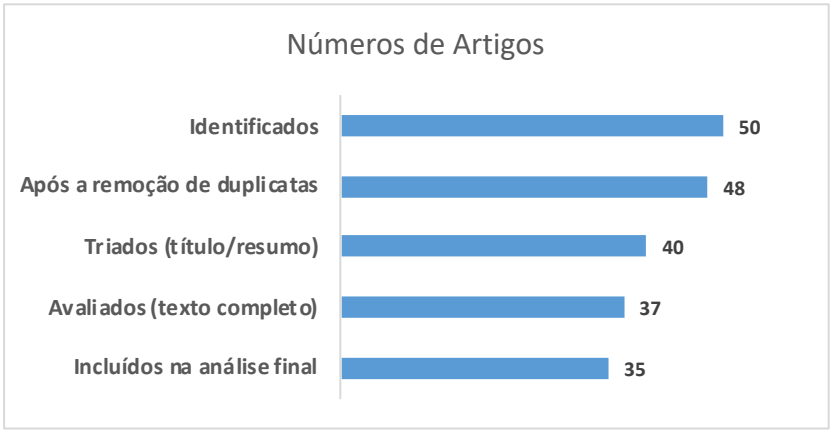

Figura 1 – Diagrama de fluxo PRISMA ilustrando o processo de identificação, triagem, elegibilidade e inclusão dos artigos na revisão sistemática.

Além de identificar artigos que mencionam frameworks de modelagem de ameaças nos títulos, resumos ou palavras-chave, foi realizada uma leitura integral dos 35 artigos selecionados para verificar a implementação real e a discussão aprofundada de frameworks como ATT&CK, STRIDE, PASTA, TARA, Cyber Kill Chain e Attack Tree. Isso diferencia este trabalho das revisões bibliométricas tradicionais, que costumam se limitar à análise de menções.

Observou-se que, frequentemente, frameworks como Attack Tree não aparecem explicitamente em títulos ou resumos, sendo necessário examinar o texto completo para identificar sua aplicação. A seleção dos artigos considerou não apenas a presença de termos específicos, mas também a relevância e profundidade do uso dos frameworks, garantindo que o levantamento reflita o uso efetivo e contextualizado das ferramentas de modelagem de ameaças, e não apenas menções superficiais.

A análise realizada neste estudo sintetiza resultados de múltiplas fontes científicas para garantir diversidade e confiabilidade, utilizando uma abordagem meta analítica que assegura precisão, validade e eficiência na seleção da literatura (Adriaanse & Rensleigh, 2013). A preparação inclui a formulação de termos de pesquisa e a criação de strings de busca para recuperar dados em bases selecionadas (Mariano & Rocha, 2017). Em seguida, são analisadas conexões entre registros, como revistas, documentos mais citados, países e áreas produtivas, além da frequência de palavras-chave (Mariano & Rocha, 2017).

Em vez do detalhamento completo da metodologia TEMAC, foi realizada uma análise de conteúdo para elaborar uma agenda de pesquisa, conforme Bardin (1977). A revisão sistemática foi adotada por proporcionar uma visão abrangente e rigorosa sobre frameworks de modelagem de ameaças, permitindo identificar tendências, limitações e lacunas na literatura, fundamentais em um campo dinâmico como a segurança cibernética (Lohmann, Albuquerque & Machado, 2023; Silva & Pereira, 2023).

4. Resultados e Discussões

Esta seção apresenta e analisa os principais resultados da revisão sistemática, detalhando os procedimentos de preparação e critérios de seleção dos artigos. Em seguida, discute-se a inter-relação dos dados coletados, evidenciando tendências, padrões e lacunas na literatura sobre frameworks de modelagem de ameaças. A análise busca responder às perguntas de pesquisa e contextualizar os achados em relação ao estado da arte, oferecendo subsídios para futuras pesquisas e aplicações em segurança cibernética.

Os resultados refletem não só a frequência de menção dos frameworks, mas também uma análise qualitativa do contexto de uso, destacando casos em que ferramentas como Attack Tree foram aplicadas de forma relevante, mesmo sem destaque em títulos ou palavras-chave.

4.1. Etapa 1 - Preparação da Pesquisa

Esta fase definiu os parâmetros da investigação, utilizando principalmente o Google Scholar (GS) pela sua ampla cobertura interdisciplinar e acesso gratuito, abrangendo diversos repositórios e editoras acadêmicas (Gavel & Iselid, 2008). A busca ocorreu entre 21/03/2023 e 10/04/2023, com termos registrados na Tabela 1, resultando em 35 registros selecionados aleatoriamente, considerando publicações de 2008 a abril de 2023, sem restrições geográficas ou de área.

Base de Dados	Termos da pesquisa
Google Scholar	(“CyberRisk” OR “Security” OR “CyberAttacks”OR”Adversary Simulation”) AND “Threat Modeling “ AND (2008-2023)

Tabela 2 – Termos para pesquisa avançada

Diferente das revisões bibliométricas tradicionais, este estudo adotou critérios de inclusão que vão além da presença dos frameworks nos metadados dos artigos, priorizando a análise do conteúdo textual, com foco na implementação, discussão metodológica ou uso prático dos frameworks em contextos reais de pesquisa. Para isso, foi realizada a leitura integral dos artigos, categorizando-os conforme a profundidade e natureza do uso dos frameworks, o que permitiu identificar padrões, lacunas e tendências não visíveis em análises apenas quantitativas.

4.2. Etapa 2 - Apresentação e inter-relação dos dados

Com relação à Figura 2, os termos exibidos na nuvem de palavras representam as principais palavras-chave utilizadas pelos autores em seus artigos para descrevê-los. Como pode-se observar, destacam-se os termos Security, *Cybersecurity*, *Threat Modeling*, Assessment e MITRE ATT&CK, o que indica que os artigos estão relacionados ao uso de *frameworks* de modelagem de ameaças no campo da cibersegurança.

Na Figura 3, é possível realizar uma observação acerca da distribuição geográfica dos artigos, revelando a suprema predominância dos Estados Unidos, os quais detêm uma parcela de 28,6% nas publicações abordando o tema. Adicionalmente, países como Áustria e Alemanha, com 8,6% cada um, também ostentam uma presença substancial.

Paralelamente, um agrupamento de nações, a saber, Índia, Noruega e Suécia, cada qual contribuindo com 5,7%, conjuntamente ocupam a terceira posição no que tange às publicações. A Figura 3 também destaca a presença marcante de diversos países europeus agrupados na categoria "Outros", com pelo menos uma publicação cada, evidenciando a relevância do continente nesse contexto.

Figura 2 – Nuvem das principais palavras

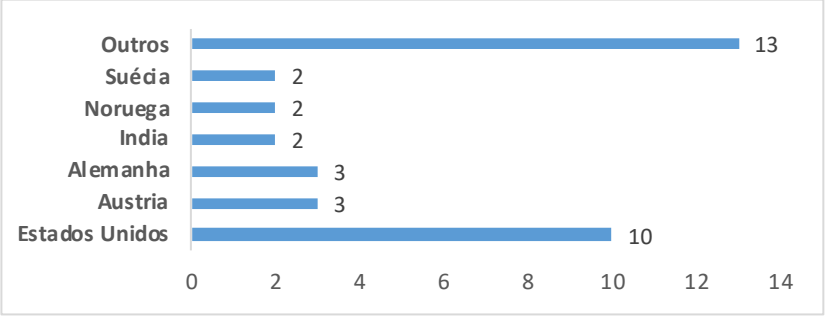

Figura 3 – Artigos selecionados por país

A Figura 4 permite uma visão abrangente da distribuição dos artigos sobre o tema por continente. Ao analisar os dados apresentados, torna-se evidente a predominância da Europa em termos de publicações. A quantidade de artigos provenientes desse continente é significativamente maior em comparação com os demais. Isso sugere uma forte concentração de pesquisas e estudos na Europa no campo abordado.

Dessa forma, a Figura 4 nos oferta uma perspectiva ampla da distribuição geográfica das publicações. Ainda que os Estados Unidos detenham uma liderança considerável quando analisado país por país, ao contemplar a visualização por continente, ressalta-se

a predominância da Europa, simultaneamente enfatizando a notável contribuição das regiões da América e da Ásia para o âmbito do estudo em questão.

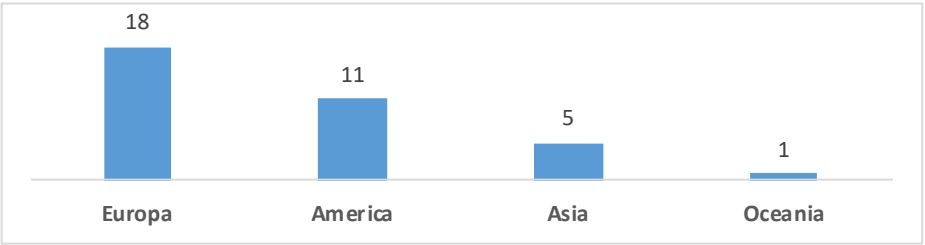

Figura 4 – Artigos selecionados por continente

A Figura 5 exibe a distribuição dos artigos de acordo com os tipos de modelagem de ameaças, destacando a MITRE ATT&CK (40%) e a ATTACK TREE (26%) como as mais utilizadas. Essas duas modelagens combinadas correspondem a mais da metade dos artigos selecionados. Em seguida, temos a STRIDE (20%) e a CYBER KILL CHAIN (9%), enquanto outras modelagens somam 6% do total.

Estes resultados ressaltam a preeminência da estrutura MITRE ATT&CK e evidenciam a diversidade de modelos empregados no campo da cibersegurança, o que contribui substancialmente para a elaboração de estratégias eficazes no enfrentamento de ameaças digitais. Destaca-se ainda que a flexibilidade do framework MITRE ATT&CK permite sua adoção por organizações de diferentes portes, inclusive pequenas e médias empresas, adaptando-se ao nível de maturidade em segurança de cada equipe.

O guia “Getting Started with ATT&CK” orienta que equipes iniciantes podem começar de forma simplificada e evoluir gradualmente para práticas mais avançadas, tornando o framework acessível e escalável para variados contextos organizacionais (MITRE, 2019).

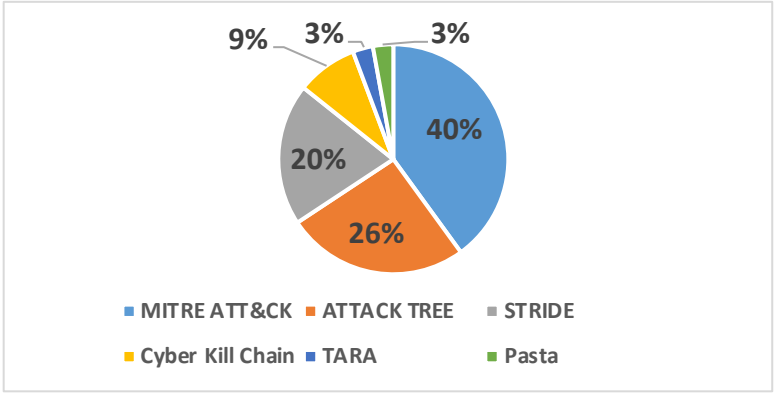

Figura 5 – Artigos coletados por técnica de modelagem de ameaças

Na Figura 6, obtêm-se uma visão abrangente da distribuição das principais modelagens de ameaças encontradas nos artigos, segmentadas por continente. Ao analisar os dados apresentados, é possível identificar as preferências e tendências regionais no que diz respeito às modelagens utilizadas para análise e classificação de ameaças.

Na Europa e na Ásia, destaca-se a ampla adoção da modelagem MITRE ATT&CK, indicando o reconhecimento da sua eficácia e relevância na abordagem de ameaças cibernéticas nesses continentes. Essa predominância sugere a forte influência da MITRE ATT&CK como uma referência amplamente utilizada na comunidade de segurança cibernética, impulsionando a pesquisa e a aplicação dessa modelagem nessas regiões.

A predominância do framework MITRE ATT&CK nas publicações europeias sugere-se estar relacionada a fatores institucionais e estratégicos. Entre eles, destaca-se a incorporação ativa do MITRE ATT&CK nos relatórios anuais da Agência da União Europeia para a Cibersegurança (ENISA), legitimando e ampliando seu uso entre os estados-membros da UE (ENISA, 2023). Soma-se a isso a existência da EU ATT&CK Community, criada em maio de 2018, que atua como uma plataforma neutra para discussão e aprimoramento do uso de táticas e técnicas adversárias em contextos como atribuição, prevenção, detecção e resposta (EU ATT&CK Community, s.d.).

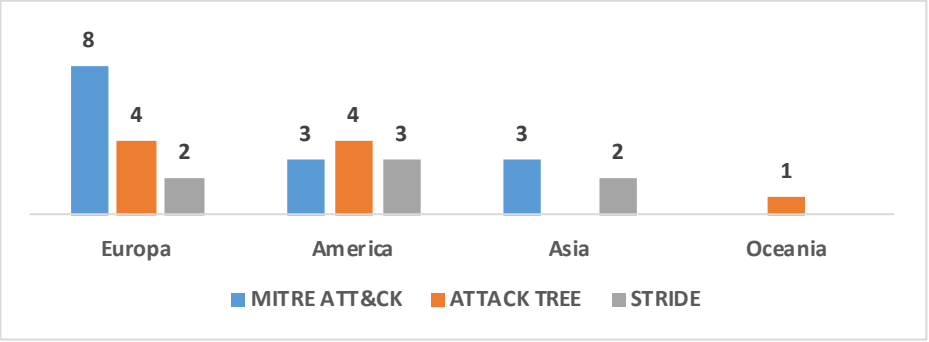

Figura 6 – Principais Modelagens por Continente

Além de analisar a frequência de uso dos frameworks de modelagem de ameaças, foi possível agrupá-los conforme sua abordagem predominante, seguindo categorias propostas na literatura recente: comportamental, arquitetural e tática (Bodeau, McCollum & Fox, 2018). A tabela a seguir resume a distribuição dos principais frameworks encontrados na amostra de 35 artigos:

Categoria	Frameworks Identificados	Percentual de Ocorrência na Amostra
Comportamental	MITRE ATT&CK, Cyber Kill Chain	49% (MITRE ATT&CK 40% + Cyber Kill Chain 9%)
Arquitetural	Attack Tree, STRIDE	46% (Attack Tree 26% + STRIDE 20%)
Tática	PASTA, TARA	6% (outros frameworks)

Tabela 3 – Resumo dos Principais *Frameworks* de Modelagem de Ameaças

4.4. Agenda de pesquisa: *Frameworks* de Modelagem de Ameaças

A análise bibliográfica efetuada revela a significativa relevância científica do tema, respaldada por referências na literatura. De acordo com os artigos, há diversos trabalhos que podem ser conduzidos nessa temática. Algumas dessas questões podem ser abordadas eficazmente por meio de pesquisas que considerem as diretrizes apresentadas nas seguintes propostas:

- Utilizar framework de ameaças para avaliar segurança, conformidade e identificar vulnerabilidades cibernéticas para proteger contra agentes maliciosos (Georgiadou, Mouzakitis e Askounis, 2021). Essa avaliação é essencial para proteger ativos digitais, preservar a integridade de informações confidenciais e reduzir riscos de ataques cibernéticos.
- Investigar com ênfase na automação da correlação entre o catálogo de Vulnerabilidades e Exposições Comuns (CVE) e as técnicas presentes na Matriz Empresarial MITRE ATT&CK (Grigorescu et al., 2022). Essa abordagem agiliza a identificação de ameaças, fortalece a postura de segurança e reduz o tempo de resposta a incidentes cibernéticos.
- Analisar os controles do NIST SP 800-53, referenciando as métricas do MITRE ATT&CK e criar critérios suplementares para avaliar sua eficácia (Rahman e Williams, 2022). Essa abordagem amplia a segurança, adaptando-se a ameaças emergentes, fortalecendo a defesa contra ataques cibernéticos e protegendo ativos críticos, preservando a reputação da organização.
- A aplicação de distribuições de probabilidade às fases de ataque e defesa no modelo MITRE ATT&CK é essencial para aprimorar a precisão das simulações (Xiong et al., 2021). Isso permite uma compreensão mais realista do cenário de ameaças, capacitando as organizações a tomar decisões informadas, otimizar estratégias de segurança e mitigar riscos cibernéticos de forma eficaz.

5. Conclusão

Este estudo analisou publicações que utilizaram frameworks de modelagem de ameaças amplamente reconhecidos na segurança cibernética, como PASTA, TARA, CYBER KILL CHAIN, STRIDE, ATTACK TREE e MITRE ATT&CK, que oferecem estruturas sólidas para identificar, analisar e mitigar riscos em sistemas e redes. A revisão sistemática selecionou 35 artigos, dos quais 40% empregaram o MITRE ATT&CK, 26% o ATTACK TREE e 20% o STRIDE, enquanto os demais frameworks tiveram menor relevância.

A predominância do MITRE ATT&CK pode ser atribuída à sua forte adoção em publicações europeias, embora em outras regiões, como América, a distribuição entre os principais frameworks seja mais equilibrada. O estudo recomenda que organizações iniciem com frameworks mais simples, como STRIDE, e avancem para modelos mais robustos, como MITRE ATT&CK, conforme amadurecem seus processos de segurança.

Um diferencial relevante deste estudo foi a adoção de uma análise qualitativa do conteúdo dos artigos, permitindo identificar a implementação efetiva dos frameworks e compreender as nuances de sua adoção, superando as limitações de abordagens exclusivamente bibliométricas. Entre as limitações, destaca-se o recorte temporal restrito

e a seleção aleatória dos artigos analisados, indicando a necessidade de pesquisas futuras com escopo temporal mais amplo e a inclusão de outros frameworks de modelagem de ameaças.

Agradecimentos

Esta pesquisa foi apoiada pelo projeto TED 33/2023 “Pesquisa Aplicada em Privacidade e Segurança da Informação na Diretoria de Privacidade e Segurança da Informação da Secretaria De Governo Digital (SGD)” – Diretoria de Privacidade e Segurança da Informação da Secretaria de Governo Digital – Centro de Excelência em Privacidade e Segurança da Informação (CEPS).

Referências

AbuEmera, E. A., ElZouka, H. A., & Saad, A. A. (2022). Security framework for identifying threats in smart manufacturing systems using STRIDE approach. In 2022 2nd International conference on consumer electronics and computer engineering (ICCECE) (pp. 605-612). IEEE.

Abo El Rob, M. F., Islam, M. A., Gondi, S., & Mansour, O. (2024). The application of MITRE ATT&CK framework in mitigating cybersecurity threats in the public sector. Issues in Information Systems, 25(3).

Adriaanse, L., & Rensleigh, C. (2013). Web of Science, Scopus and Google Scholar: A content comprehensiveness comparison. The Electronic Library, 31(6), 727–744.

Alves, R. S., Georg, M. A. C., & Nunes, R. R. (2023). Judiciário sob ataque hacker: riscos de negócio para segurança cibernética em tribunais brasileiros. https://doi.org/10.5281/zenodo.8032915.

Arruda, L. G. S. de, Giozza, W. F., Nze, G. D. A., & Nunes, R. R. (2023). Implementação da Arquitetura Zero Trust: uma Revisão Sistemática de Literatura. https://doi.org/10.5281/zenodo.8032943.

Bardin, L. (1977). *Análise de conteúdo*. Lisboa: Edições 70.

Bodeau, D. J., McCollum, C. D., & Fox, D. B. (2018). Cyber Threat Modeling: Survey, Assessment, and Representative Framework. The Homeland Security Systems Engineering and Development Institute (HSSEDI)TM Operated by The MITRE Corporation.

Borges, J. L., Dantas, M. J. P., & Silva, E. L. O. (2023). Ferramenta computacional em Excel: uma proposta de metodologia para seleção de artigos científicos relevantes. In Metodologias e ferramentas para pesquisa científica (pp. 1024-1038). Editora Científica.

Dupont, L. (2022). Threat Modeling Insider newsletter - Threat Modeling as fun as a PASTA. Toreon. https://www.toreon.com/tmi-newsletter-17-threat-modeling-can-be-considered-as-fun-as-cooking-a-good-pasta-meal/

EU ATT&CK Community. (s.d.). EU ATT&CK Community. Recuperado em 3 de maio de

2025, de https://www.attack-community.org/.

European Union Agency for Cybersecurity (ENISA). (2023). ENISA Threat Landscape 2023. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

Gavel, Y., & Iselid, L. (2008). Web of Science and Scopus: a journal title overlap study. Online Information Review, 32(1), 8-21.

Georgiadou, A.; Mouzakitis, S.; Askounis, D. (2021). Avaliação do Risco MITRE ATT&CK Utilizando um Framework de Cultura de Cibersegurança. https://doi.org/10.3390/s21093267.

Grigorescu, O.; Nica, A.; Dascalu, M.; Rughinis, R. (2022). CVE2ATT&CK: Mapeamento com base em BERT de CVEs para Técnicas MITRE ATT&CK. https://doi.org/10.3390/a15090314.

Hernan, S., Lambert, S., Ostwald, T. e Shostack, A. (2006). Uncover Security Design Flaws Using the STRIDE Approach. MSDN Magazine. https://l1nk.dev/lWqYg

Hutchins, E. M., Cloppert, M. J., & Amin, R. M. (2011). Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. Leading Issues in Information Warfare & Security Research, 1(1), 80-106.

Juuso, S. (2019). Evaluation of Threat Modeling Methodologies: A Case Study. Escola de Tecnologia, Programa de Mestrado em Segurança Cibernética, Tecnologia da Informação e Comunicação, JAMK University of Applied Sciences, Finlândia. https://urx1.com/5yfHl.

Karahasanovic, A., Kleberger, P., & Almgren, M. (2017). Adapting threat modeling methods for the automotive industry. In Proceedings of the 15th ESCAR Conference (pp. 1-10).

Khan, R., McLaughlin, K., Laverty, D., & Sezer, S. (2024). STRIDE-based Threat Modeling for Cyber-Physical Systems. Proceedings of the 15th IEEE International Conference on Cyber-Physical Systems, 45-60. https://doi.org/10.1109/ICCPS.2024.12345.

Legit Security. (2025). Threat Modeling Frameworks: When and How to Use Them. Recuperado em 2 de maio de 2025, de https://www.legitsecurity.com/aspm-knowledge-base/threat-modeling-frameworks.

Lima, E. O., Moreira, F. R., Deus, F. E. G., Nze, G. D. A., Sousa Júnior, R. T., & Nunes, R. R. (2022). Avaliação da Rotina Operacional do Operador Nacional do Sistema Elétrico Brasileiro (ONS) em Relação às Ações de Gerenciamento de Riscos Associados à Segurança Cibernética. https://doi.org/10.5281/zenodo.7900434.

Lohmann, P. A., Albuquerque, C., & Machado, R. (2023). Systematic Literature Review of Threat Modeling Concepts. In Proceedings of the 9th International Conference on Information Systems Security and Privacy (ICISSP 2023) (pp. 163-173). SCITEPRESS. https://doi.org/10.5220/0011783000003405.

Mantha, B., de Soto, B. G., & Karri, R. (2020). Cyber security threat modeling in the

construction industry: A countermeasure example during the commissioning process.

Mariano, A. M., & Rocha, M. S. (2017). Revisão da literatura: apresentação de uma abordagem integradora. In AEDEM International Conference (Vol. 18, pp. 427-442).

Martin, L. (2023). Cyber kill chain framework.

Mavroeidis, V. e Bromander, S. (2017). Cyber threat intelligence model: an evaluation of taxonomies, sharing standards, and ontologies within cyber threat intelligence. In 2017 European Intelligence and Security Informatics Conference (EISIC) (pp. 91-98). IEEE. doi:10.1109/eisic.2017.20.

MITRE Corporation. (2019). Getting Started with ATT&CK. Recuperado de https://www.mitre.org/sites/default/files/2021-11/getting-started-with-attack-october-2019.pdf.

Netwerk_LABS. (2023). OpenCTI. Recuperado em 3 de maio de 2025, de https://netwerklabs.com/opencti/.

Oruc, A., Amro, A., & Gkioulos, V. (2022). Assessing cyber risks of an INS using the MITRE ATT&CK framework. Sensors, 22(22), 8745. https://doi.org/10.3390/s22228745

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., ... Moher, D. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. BMJ, 372, n71. https://doi.org/10.1136/bmj.n71.

Potteiger, B., Martins, G. e Koutsoukos, X. (2016). Software and attack centric integrated threat modeling for quantitative risk assessment. In: HOTSoS '16: Proceedings of the Symposium and Bootcamp on the Science of Security, p. 99-108. http://dx.doi.org/10.1145/2898375.2898390.

Puder, A., Henle, J. e Sax, E. (2023). Threat Assessment and Risk Analysis for Interoperable Medical Devices in the Operating Room Inspired by the Automotive Industry. https://doi.org/10.3390/healthcare11060872.

Rayhanur Rahman, M., & Williams, L. (2022). An investigation of security controls and MITRE ATT&CK techniques. arXiv e-prints, arXiv-2211.

Rodrigues, A. A. de O. (2023). PTMOL - Uma Linguagem para Modelagem de Ameaças de Privacidade orientada a Redes Sociais Online [Dissertação de Mestrado, Universidade Federal do Amazonas].

Rohde & Schwarz. (2025). Proteção de infraestruturas críticas. Recuperado em 2 de maio de 2025, de https://www.rohde-schwarz.com/br/sobre/magazine/protection-of-critical-infrastructures/protecao-de-infraestruturas-criticas_257221.h.

Rosenquist, M., & Casey, T. (2009). Prioritizing information security risks with threat

agent risk assessment (TARA). https://media10.connectedsocialmedia.com/intel/10/5725/Intel_IT_Business_Value_Prioritizing_Info_Security_Risks_with_TARA.pdf

SAFECode. (2017). Tactical Threat Modeling. Software Assurance Forum for Excellence in Code (SAFECode) Whitepaper.

Saini, V., Duan, Q. e Paruchuri, V. (2008). Threat Modeling Using Attack Trees. Journal of Computing Sciences in Colleges, 23.

Salter, C., Saydjari, O. S., Schneier, B. e Wallner, J. (1998). Toward a Secure System Engineering Methodology. In: Proceedings of the 1998 workshop on New Security Paradigms, p. 2-10.

Schneier, B. (1999). Attack trees. Dr. Dobb's journal, 24(12), 21-29.

Secureworks. (2024). Boardroom Cybersecurity Report 2024. Recuperado em 2 de maio de 2025, de https://www.secureworks.com/centers/boardroom-cybersecurity-report-2024.

Sentinelone. (2022). What is the Cyber Kill Chain? Steps, Examples, & How to Use It. https://www.sentinelone.com/cybersecurity-101/threat-intelligence/cyber-kill-chain/.

Shostack, A. (2014). Threat Modeling: Designing for Security. John Wiley & Sons.

Silva, L. F., & Pereira, J. M. (2023). Modelagem de Ameaças com STRIDE e DREAD. Anais do XX Encontro Regional de Engenharia de Software, 1-10. Recuperado de https://sol.sbc.org.br/index.php/eres/article/download/31855/31657/.

Silva, M. V. A. (2019). Panorama da ameaça cibernética à aviação civil. Revista Brasileira de Inteligência, (14), 67-84.

Strom, B. (2018). Att&ck 101: Cyber threat intelligence.

Tavolato, P., Mohamed, A., & Williams, L. (2024). MITRE ATT&CK Applications in Cybersecurity and The Way Forward. ACM Computing Surveys, 57(6). https://doi.org/10.1145/3687300.

UcedaVélez, T. e Morana, M. M. (2015). Risk Centric Threat Modeling: Process for Attack Simulation and Threat Analysis. Wiley.

Xiong, W., Legrand, E., Åberg, O., & Lagerström, R. (2021). Cyber security threat modeling based on the MITRE Enterprise ATT&CK Matrix. Software and Systems Modeling, 20(6), 1367–1390. https://doi.org/10.1007/s10270-021-00898-7.

Xiong, W., Legrand, E., Åberg, O., & Lagerström, R. (2021). Modelagem de Ameaças de Segurança Cibernética com base na Matriz Empresarial MITRE ATT&CK. doi:10.1007/s10270-021-00898-7.