SoK: The MITRE ATT&CK Framework in Research and Practice

Shanto Roy, Emmanouil Panaousis, Cameron Noakes, Aron Laszka, Sakshyam Panda, and George Loukas

Abstract—**The MITRE ATT&CK framework, a comprehensive knowledge base of adversary tactics and techniques, has been widely adopted by the cybersecurity industry as well as by academic researchers. Its broad range of industry applications include threat intelligence, threat detection, and incident response, some of which go beyond what it was originally designed for. Despite its popularity, there is a lack of a systematic review of the applications and the research on ATT&CK. This systematization of work aims to fill this gap. To this end, it introduces the first taxonomic systematization of the research literature on ATT&CK, studies its degree of usefulness in different applications, and identifies important gaps and discrepancies in the literature to identify key directions for future work. The results of this work provide valuable insights for academics and practitioners alike, highlighting the need for more research on the practical implementation and evaluation of ATT&CK.**

I. INTRODUCTION

ATT&CK presents a curated and actionable repository of adversarial Tactics, Techniques and Procedures (TTPs) [1] and details the characterization of adversary behavior after a successful system exploitation [2]. The cybersecurity industry uses ATT&CK for various applications including threat detection, adversary emulation, red teaming, behavioral analytics, defensive gap assessment, cyber threat intelligence (CTI) and threat modeling [3], [4], [5], [6], [7].

At the same time, ATT&CK is embraced in various domains, including ICS [8] and Enterprise [9]. Many vendors, including Cisco, Fortinet and Claroty have stated the importance of ATT&CK in CTI and how security experts can align their research with ATT&CK [10], [11], [8]. Cloud platforms such as Microsoft Azure Security have also been mapped to ATT&CK using TTPs [12]. Even organizations like the North Atlantic Treaty Organization and the U.S. Department of Homeland Security have been using ATT&CK for CTI and modeling [13], [14].

There is a number of academic [15], [16], [17], [18], [19], [20], [21], [22], [23] and industrial [24], [25], [26] surveys that present the state-of-the-art approaches in CTI and discuss the necessity and impact of ATT&CK in CTI [16], [22], [23]. There are also works that survey threat modeling approaches. For example, Tayouri et al. [27] surveyed attack graph-based

S. Roy is with the University of Houston, Houston, TX, USA. E-mail: shantoroy@ieee.org. E. Panaousis, C. Noakes, S. Panda, and G. Loukas are with the Internet of Things and Security Centre, University of Greenwich, London SE10 9LS, UK. E-mail: {e.panaousis, c.noakes, s.panda, g.loukas}@greenwich.ac.uk. A. Laszka is with the Pennsylvania State University, University Park, PA, USA. E-mail: aql5923@psu.edu.

models that utilize or extend the MulVal method and mapped these MulVAL interaction rules to ATT&CK techniques for evaluation in attack scenarios. Sadlek et al. [28] explored the current challenges of threat identification using public enumerations. The authors studied the usability of ATT&CK for threat modeling. Bodeau et al. [2] discussed various security frameworks, including NIST $800 - 154$, STRIDE, DREAD, OCTAVE, TARA, TAL, STIX, CAPEC, alongside ATT&CK for threat modeling and cybersecurity risk assessment purposes. These works are not systematizations highlighting a dearth of systematic research that addresses ATT&CK use cases, application domains, and research methodologies. Our paper fills this gap by addressing the following research questions.

RQ1: *How does the use of ATT&CK contribute to cybersecurity research, and in what application domains and use cases has ATT&CK been employed in the literature?*
The aim of RQ1 is to determine the effectiveness of using ATT&CK in creating novel and impactful research. Additionally, this inquiry may serve as a foundation for future studies exploring the application domains and use cases for which ATT&CK has been investigated, thus expediting the learning curve and enhancing the framework's practicality. Our analysis reveals that ATT&CK plays a critical role in cyber threat intelligence, intrusion detection and prevention, risk assessment and mitigation, red/purple team exercises and professional training. We also highlight the diverse application domains of ATT&CK, which include enterprise networks, industrial control systems, IoT and mobile communication systems.

RQ2. *How is ATT&CK correlated, mapped, or integrated with other security frameworks in practice?*
Understanding this correlation will illuminate the value of the framework for industrial applications, which frequently need to comply with various frameworks to meet cybersecurity requirements. This insight can clarify the possibility of integrating ATT&CK and these frameworks into a unified global framework. Our investigation reveals that several studies have attempted to combine ATT&CK with other security frameworks such as the cyber kill chain, NIST CSF, ISMS, CAPEC, D3FEND and Diamond models. The integration of these frameworks results in more comprehensive solutions enabling us, for example, to identify more effective sets of security controls.

RQ3.*What are some examples of how industry utilizes ATT&CK, and what research trends, as mentioned in **RQ1**, have not yet been observed in the industrial applications of ATT&CK?*

Understanding the gap between the use of ATT&CK in industry and academia can motivate the adoption of research methods that are better suited to realistic environments, thereby enabling the development of solutions to emerging societal and industrial problems. Our findings show that academic researchers tend to use ATT&CK to develop models for attack scenarios, analyze threat intelligence datasets and investigate system vulnerabilities using mathematical and statistical models. The utilization of ATT&CK enables them to demonstrate the applicability of their work to real-world scenarios, providing a stronger basis for their proposals and facilitating the assessment of their research. In contrast, the industry focuses more on developing CTI tools and frameworks, evaluating products against ATT&CK tactics and techniques, improving red or purple team exercises and providing offensive security training.

RQ4. *What scientific methods have academic researchers employed to construct attack scenarios, models, or methods using ATT&CK matrices?*
By examining these methods, we enable researchers to identify areas where these scientific methods are not being utilized to their full potential and determine the shortage of research that employs equally appropriate methods. These scientific methods include machine learning (ML), natural language processing (as subfield of ML), probability theory, graph theory and game theory. We examine how the ATT&CK framework has been implemented in different projects. Specifically, we analyze the testbed environments and tools that researchers have used to evaluate their work based on ATT&CK and how they have applied these tools to achieve their objectives. Finally, we investigate the methods used to evaluate research that utilizes ATT&CK. These methods include numerical or statistical, human-based and model-based evaluations.

The rest of this paper is structured as follows: Section II proposes a novel taxonomy of concepts used to answer the research questions. Section III outlines the application domains and use cases in which ATT&CK has been used to address significant cybersecurity challenges and how ATT&CK has been combined with other security frameworks (answering **RQ1-RQ3**). Section IV describes the research approaches used in conjunction with ATT&CK in the literature (answering **RQ4**). Finally, Section V summarizes the key points of this systematization work, including the significance and limitations of ATT&CK and offers suggestions for future work.

II. Proposed Taxonomy

To answer the research questions, we have defined a taxonomy (shown in Figure 1) that categorizes ATT&CK-oriented applications, use cases and research approaches from the literature. By utilizing this taxonomy, researchers can classify the literature and gain insights into the usefulness of ATT&CK and identify any gaps in research to date. Table I classifies all surveyed papers using our taxonomy.

The first level classification in our taxonomy considers ATT&CK-based Applications (A) and Research Approaches (RA) found in the literature. We divide ATT&CK applications into three primary categories: Use Cases (UC), Application Domains (AD) and Related Frameworks (RF), with subcategories for each application. UC defines the specific applications where ATT&CK has been utilized and is further categorized into Cyber Threat Intelligence (CTI), Intrusion Detection (ID), Offensive Security (OS), Cyber Risk Assessment (CRA), Professional Training (PT), Threat-driven Approaches (TA) and Product Evaluation (PE). AD defines the specific domains where ATT&CK has been applied and we identify three application domains: Enterprise Networks (EN), Mobile Communication Systems (MCS) and Industrial Control Systems (ICS). We categorize RF into Cyber Kill Chain (CKC), CAPEC (CA), STRIDE (ST), Security Controls (SC) and the Miscellaneous (MI) subcategory for the rest of security frameworks.

We classify the research approaches in our study into three categories: Scientific Method (SM), Implementation (I) and Evaluation (E). SM identifies the research fields that used ATT&CK in any capacity and we further categorize it into five subcategories: Machine Learning (ML), Natural Language Processing (NLP), Probability Theory (PT), Graph Modeling (GM) and Game Theory (GT). Implementation (I) defines how researchers utilized ATT&CK in implementing the proposed works and we define two subcategories: Testbed (TE) and Tools (TO), developed to implement certain attack scenarios or models. Finally, we categorize Evaluation (E) into three subcategories: Numeric Evaluation (NE), Human Evaluation (HE) and Model Evaluation (ME). This category shows how researchers evaluated their testbeds, tools and models.

III. Applications (A) of ATT&CK

In this section, we explore ATT&CK's application domains and use cases, examine how other security frameworks are mapped to or combined with ATT&CK and finally delve into the different ways in which ATT&CK is utilized by academia and industry.

A. A-UC: Use Cases

1) A-UC-CTI: Cyber Threat Intelligence: According to Legoy et al. [45], Cyber Threat Intelligence (CTI) is a continuous process that necessitates the use of text classification techniques for retrieving TTP-oriented information. Mundt et al. [74] combined CTI with Information Security Management Systems (ISMS) and automate CTI by utilizing ATT&CK. Al et al. [5] examined the connections between ATT&CK techniques enabling the prediction of previously unobserved ones. Kriaa et al. [42] used ATT&CK to create their detection and prediction module by constructing a knowledge graph of TTPs. Zhang et al. [107] proposed a model that uses ATT&CK to assess CTI reports automatically to extract Indicators of Compromise (IoC) timely. Here, the authors used ATT&CK to identify attack techniques related to IoC.

The increasing number of connected IoT devices, which bear security vulnerabilities, is contributing to the constantly evolving operational technology (OT) cyber threat landscape. To address this issue, Kwon et al. [43] developed a Cyber Threat Dictionary utilizing the ATT&CK ICS matrix and mapped security controls to the ATT&CK ICS matrix. Odemis et al. [108] utilized ATT&CK to create a cyber expertise test

Fig. 1: Taxonomy of papers that use ATT&CK.

to detect and categorize adversarial behavior for their CTI research. Similarly, ATT&CK was also used for further threat analysis and adversarial TTP classification in the works of Lee et al. [50], Mendsaikhan et al. [51] and Jo et al. [109]. Hemberg et al. [37] and Kurniawan et al. [48] utilized the framework for linking ATT&CK techniques to vulnerabilities. Additionally, Bromander et al. [44] developed a CTI data model that identifies threats with ATT&CK being used as a source for tactics, techniques, tools, and threat actors.

Insight 1. ATT&CK is valuable for security teams seeking to keep up with the latest threats and enhance their CTI capabilities. Many studies link CTI reports with ATT&CK matrices to create effective mitigation strategies. It has been observed that the majority of research papers in this field utilize ATT&CK to improve CTI. However, there is a lack of investigation into how insights gained from CTI research can be used to enhance ATT&CK itself.

2) A-UC-ID: Intrusion Detection: ATT&CK techniques can be used to categorize adversary behavior and detect advanced intrusions [32]. Common Vulnerabilities and Exposures (CVEs) can be linked to specific exploitation strategies and then mapped to ATT&CK techniques.

Golushko et al. [41] applied ATT&CK to identify effective techniques under the *Command and Control* and *Defense Evasion* tactics and provided recommendations for detection and prevention. Kriaa et al. [42] proposed a novel approach for building knowledge graphs using ATT&CK and utilizing prediction techniques on event logs to identify and prevent 5G radio access network attacks. Additionally, Kwon et al. [43] extended the ATT&CK ICS matrix leading to the creation of new categories for threat detection and mitigation.

The DeTT&CT (Detect Tactics, Techniques & Combat Threats) framework [110], [111] was introduced by the industry [112] to enhance intrusion detection. DeTT&CT helps blue teams evaluate and analyze the quality and visibility of data log

TABLE I: Taxonomy classification of papers using ATT&CK

Description / Literature	Application			Research Approach		
	Use-cases	Application Domain	Related Frameworks	Scientific Methods	Implementation	Evaluation
Ahn et al. (2020) [29]	PT	EN	✗	GM	TE	NE
Ampel et al. (2021) [30]	OS	EN	✗	ML	TE	NE,ME
Choi et al. (2020) [4]	CTI	ICS	✗	✗	TE, TO	✗
Georgiadou et al. (2021) [1]	PT, OS, CRA	EN	✗	✗	✗	✗
Hong et al. (2019) [31]	PT, OS	EN	✗	ML	TE	✗
Kuppa et al. (2021) [32]	OS	EN	✗	NLP	✗	ME, NE
Munaiah et al. (2019) [33]	OS	EN	✗	GM	✗	NE
Outkin et al. (2021) [34]	TA, PE	EN	✗	GM	✗	ME
Pell et al. (2021) [35]	TA	MCS	✗	✗	✗	✗
Xiong et al. (2021) [36]	TA	EN	MI	GM	TE	ME
Hemberg et al. (2020) [37]	CTI	EN	CA	GM	TE	NE
Kim et al. (2021) [38]	PT, OS, PE	EN	CKC	GM	✗	NE
Choi et al. (2021) [39]	OS, PT	ICS	✗	GM	TO	ME
Al et al. (2020) [5]	CTI, OS	EN	✗	ML,GM	TO	NE, HE
Amro et al. (2021) [?]	CRA	ICS	CA	GM	✗	NE
Arshad et al. (2021) [40]	OS, PT	EN	✗	GT	TO	ME
Golushko et al. (2020) [41]	IDS, OS	EN, ICS, MCS	✗	✗	TO	✗
Kriaa et al. (2021) [42]	CTI	EN, ICS, MCS	CA	GM	TO	ME
Kwon et al. (2020) [43]	CTI, TA	ICS	MI, CKC	✗	TO	✗
Bromander et al. (2020) [44]	CTI	ICS	CA	GM	TO	ME
Legoy et al. (2020) [45]	CTI	EN, MCS, ICS	✗	ML	TO	ME
Fairbanks et al. (2021) [46]	CTI	MCS	✗	GM, ML	✗	NE
Huang et al. (2021) [47]	CTI, TA	EN, MCS, ICS	MI	ML	TO	NE, ME
Kurniawan et al. (2021) [48]	CTI	EN, MCS, ICS	MI	GM	TO	ME
Lakhdhar et al. (2021) [49]	CTI, TA	EN, MCS, ICS	CA, MI	ML	TO	NE, ME
Lee et al. (2021) [50]	CTI	EN, MCS, ICS	✗	GM, ML	TO	NE, ME
Mendsaikhan et al. (2020) [51]	CTI, TA	EN, MCS, ICS	CA	ML	TO	NE, ME
Parmar et al. (2019) [13]	CTI	EN, MCS, ICS	✗	GM	TE, TO	NE
Purba et al. (2020) [52]	CTI	EN, MCS, ICS	✗	NLP	TO	NE, ME
Aghaei et al. (2019) [53]	CTI, TA	EN, MCS, ICS	CA, MI	✗	✗	✗
Ajmal et al. (2021) [54]	CTI, OS, PT	EN	✗	PT	TE, TO	NE, ME
Brazhuk et al. (2021) [55]	CTI, TA	EN, MCS, ICS	CA, ST, SC, MI	GM, PT	TO	NE
Elitzur et al. (2019) [56]	CTI, TA	EN, MCS, ICS	SC	GM, PT	TO	NE, ME
Fairbanks et al. (2021) [57]	CTI	EN, MCS, ICS	✗	GM, ML	✗	NE, ME
Franklin et al. (2017) [58]	TA	EN, MCS, ICS	✗	ML	TO	✗
Gourisetti et al. (2019) [59]	CTI, TA, CRA	ICS	SC, MI	✗	TE, TO	NE
Gylling et al. (2021) [60]	CTI, TA	EN, MCS, ICS	✗	GM	TO	NE
Hacks et al. (2021,2022) [61], [62]	CTI, TA	EN, MCS, ICS	SC	✗	TO	NE, ME, HE
Hassanzadeh et al. (2020) [63]	CTI, TA	ICS	SC	ML	TE, TO	NE, ME
Ahmed et al. (2022) [64]	CRA, TA	EN, MCS, ICS	SC	PT, GM	✗	ME
Bolbot et al. (2022) [65]	CRA, TA	EN, MCS, ICS	ST, MI	✗	TO	NE
Oruc et al. (2022) [66]	CRA	ICS	SC	PT	TO	NE
TJ OConnor (2022) [67]	PT	EN	✗	✗	TE, TO	NE, HE
Kim et al. (2020) [68]	PT, PE	EN	CKC	GM	TE, TO	ME
Sadlek et al. (2022) [28]	CTI, TA	EN	CA, MI	✗	✗	NE
Rao et al. (2023) [69]	TA	MCS	MI	GM	✗	ME
Chen et al. (2022) [70]	TA, PE	EN	MI	NLP, GM	TO	NE
Adam et al. (2022) [71]	CTI	EN	CA, MI	NLP, ML	✗	NE,ME
Sadlek et al. (2022) [72]	CTI, TA	EN, MCS, ICS	ST, CKC, SC	GM	TE, TO	ME
Jadidi et al. (2021) [73]	CTI, TA	ICS	SC	GM	TO	ME
Mundt et al. (2022) [74]	CTI	EN	MI	GM	TO	ME
Niakanlahiji et al. (2018) [75]	CTI	EN	MI	NLP	TO	NE, ME
Ayoade et al. (2018) [76]	CTI	EN	CKC, MI	NLP, PT, ML	TO	NE, ME
Karuna et al. (2021) [77]	CTI	EN, MCS, ICS	✗	NLP	✗	✗
Shin et al. (2021) [78]	CTI	EN, MCS, ICS	✗	PT, ML	TO	NE
He et al. (2021) [79]	CTI, CRA	EN, MCS, ICS	MI	PT, GM	✗	NE
Johnson et al. (2018) [80]	TA, OS	EN, MCS, ICS	SC, MI	PT, GM	TO	NE
Tayouri et al. (2023) [27]	TA, CTI	EN	MI	GM	TO	NE
Bodeau et al. (2018) [2]	CTI, TA, CRA	EN, MCS, ICS	CA, CKC, ST, SC, MI	✗	✗	✗
Manocha et al. (2021) [81]	CRA, OS	EN, MCS, ICS	MI	PT	✗	NE
Mashima et al. (2022) [82]	CTI, PE	ICS	SC, MI	✗	TE, TO	ME
Dhirani et al. (2021) [83]	TA, PE, CRA	ICS	SC, MI	✗	✗	✗
Luh et al. (2022) [84]	TA, OS	EN, ICS	CA, SC, MI	GT	TE, TO	HE, NE
Husari et al. (2019) [85]	CTI	EN, MCS, ICS	CKC, MI	NLP	TO	✗
Nisioti et al. (2021) [86]	TA, OS	EN, MCS, ICS	CKC, MI	GT, GM	TO	NE, ME
Halvorsen et al. (2019) [87]	CTI, TA, ID	EN	SC, MI	PT	TE, TO	NE

TABLE I: Taxonomy classification of papers using ATT&CK (continued)

Description / Literature	Application			Research Approach		
	Use-cases	Application Domain	Related Frameworks	Scientific Methods	Implementation	Evaluation
Wong et al. (2021) [88]	TA, OS	EN	ST	✗	✗	✗
Dhir et al. (2021) [89]	TA, OS	EN	✗	PT	✗	ME
Holder et al. (2021) [90]	TA, CRA	EN	✗	PT	TE	NE
Ahn et al. (2022) [91]	ID, CTI, TA	EN	✗	PT, GM, NLP	TE, TO	NE
Stoleriu et al. (2021) [92]	ID	EN	SC, MI	ML	TE, TO	NE
Bagui et al. (2022) [93]	ID	EN	✗	ML	✗	NE, ME
Zurowski et al. (2018) [94]	TA, OS	EN	SC	ML	TO	NE
Alnafrani et al. (2022) [95]	TA	EN	✗	PT, ML	TE, TO	ME
Samtani et al. (2022) [96]	CTI, TA	EN	✗	ML	✗	✗
Grigorescu et al. (2022) [97]	CTI	EN	CA, MI	NLP, ML, GM	TO	NE, ME
Hasan et al. (2019) [98]	ID	EN, ICS	CA, CKC, MI	ML, GM	TO	NE, ME
Maymí et al. (2017) [99]	CTI	EN, MCS, ICS	CKC, MI	ML, GM	✗	✗
Drašar et al. (2020) [100]	TA, OS	EN, MCS, ICS	MI	GT, GM	TE, TO	NE, ME
Kim et al. (2022) [101]	CTI, TA	EN	ST, CKC	ML	TO	NE, ME
Kim et al. (2021) [102]	CTI, TA	MCS	✗	ML	✗	ME, NE
Sahu et al. (2021) [103]	TA	EN	MI	✗	✗	ME
Zhao et al. (2021,2022) [104], [105]	PT	EN	MI	✗	✗	✗
Van et al. (2022) [106]	TA	EN	MI, SC	PT, GM	TO	ME

sources and detection coverage using ATT&CK. In addition to DeTT&CT, the industry is continuously creating frameworks and tools for detecting and responding to security incidents. These frameworks and tools are exemplified by ATT&CK. For instance, Security Information and Event Management (SIEM) tools are adopting ATT&CK for better detection and alert management [63], [113], [114], [6].

Insight 2. ATT&CK assists researchers identify behavior patterns of known threats and recognize the use of particular techniques and tools, which can aid in intrusion detection. There is a lack of studies that evaluate the effectiveness of ATT&CK in supporting intrusion detection frameworks in real-world settings as well as research on how to adapt ATT&CK to detect new threats.

3) A-UC-OS: Offensive Security: ATT&CK is a valuable resource to conduct effective adversary emulation as it contains comprehensive information on techniques employed by various threat actors. By utilizing the ATT&CK knowledge base, organizations can simulate realistic attack scenarios and proactively identify potential security gaps thus enhancing their overall security posture.

Kuppa et al. [32] leveraged a CVE regular expression dataset to identify frequently exploited CVEs created by collecting different APT reports[1] from 2008 to 2019, zero-day exploits[2] from Google project zero, 63720 vulnerability reports and 37000 threat reports[3]. The researchers obtained a sample of 200 CVEs from publicly available threat reports along with their corresponding ATT&CK techniques to extract the relevant context phrases. Munaiah et al. [33] used data from the 2018 National Collegiate Penetration Testing Competition and codified their approach in terms of ATT&CK tactics and techniques that it is possible to characterize attacker campaigns as a chronological series of them.

Kim et al. [38] developed an offensive security taxonomy and provided a systematic cyber attack scoring model. They employed artifacts from attacks to identify the techniques used. They constructed the technology and stages used by malware based on ATT&CK and grouped the identified attack techniques used in a few real cyber-attack incidents. Other studies such as [30], [5], [40], [54] have also utilized ATT&CK for offensive security practices, red teaming exercises, and penetration testing.

Insight 3. ATT&CK is a valuable tool for offensive security teams to plan and execute simulated attacks in order to test an organization's security measures. By utilizing ATT&CK, organizations can identify weaknesses in their defenses and improve their overall security posture. This proactive security approach can help organizations better protect themselves from real-world attacks. A potential research gap in the application of ATT&CK to offensive security is the development of metrics for evaluating the effectiveness of defensive measures against specific TTPs, as well as standardized methods for mapping defensive measures to specific TTPs.

4) A-UC-CRA: Cyber Risk Assessment: ISO 27005, CO-BIT 5, NIST SP 800-30 and other frameworks are widely used for cyber risk assessment. Researchers have recently combined these frameworks with ATT&CK for more effective risk assessment. For example, Ahmed et al. [64] proposed a methodology that uses ATT&CK, NIST SP 800-30 Rev.1, and attack graphs to assess and characterize cyber risk. Sadrazamis [115] proposed a hierarchical risk assessment system based on ATT&CK knowledge graph. Amro et al. [116] employed semantics and components of ATT&CK to quantify risks associated with cyber-physical systems. Ahmed et al. [64] analyzed and characterized TTPs used by different threat actors for informed cyber risk assessment. In their study, Kure et al. [117] presented an integrated cyber risk management framework that utilizes an ATT&CK-driven threat modeling approach. Oruc et al. [66] used ATT&CK to assess risks associated with cyber threats and vulnerabilities for integrated

---

[1]https://github.com/CyberMonitor/APT_CyberCriminal_Campaign_Collections

[2]https://googleprojectzero.blogspot.com/p/0day.html

[3]https://www.broadcom.com/support/security-center/a-z

navigation systems on board shipping vessels.

The use of cyber risk and vulnerability assessment data mapped to ATT&CK tactics and techniques has been explored by the industry to identify mitigation strategies [118], [119]. Grantek [120] has detailed an approach to utilizing ICS ATT&CK strategies for risk management, which involves system identification and characterization, vulnerability identification and threat modeling, and risk calculation and management. AttackIQ, a security research organization focused on prioritizing vulnerability management, published a whitepaper proposing the use of ATT&CK and CVE for better risk management [121]. MITRE presented cyber resiliency metrics and scoring for better risk management in a whitepaper by Bodeau et al. [2].

On the research front, Georgiadou et al. [1] associated individual and organizational culture dimensions with adversarial behavior and patterns documented in ATT&CK, using a cybersecurity culture framework. They developed a hybrid ATT&CK for Enterprise and ICS matrix to identify cyber risks to which an organization lacks resilience.

Insight 4. By mapping threat behaviors with vulnerabilities, researchers have been able to provide essential mitigation tactics for assessing cyber risk. ATT&CK provides a consistent and repeatable approach to evaluating security risks, enabling organizations to make more informed decisions about the threats they are facing. Investigating further the integration of ATT&CK with other risk assessment methodologies has the potential to enhance its utility and effectiveness. Additionally, conducting empirical studies in collaboration with practitioners to assess the impact of using ATT&CK on cyber risk quantification can contribute to advancing cyber risk management practice.

5) A-UC-PT: Professional Training: Georgiadou et al. [1] focused on cyber warfare simulations for training offense and defense from real-world cyber scenarios related to ATT&CK. Hong et al. [31] proposed an automated script to generate simulated threats for training professionals with practical methods for real-world defensive scenarios. O'Connor [67] shared experiences, lessons and materials from an undergraduate course that suggests using ATT&CK to combine theoretical learning and exploratory labs.

Kim et al. [68] analyzed real-world data from ATT&CK to propose CyTEA, a model that can generate simulated cyber threats for a cybersecurity training system. The simulation level was evaluated based on procedural, environmental and consequential similarities to determine if the model is suitable for real-world use and acceptable for industry usage. Arshad et al. [40] proposed an attack specific language (ASL) based on ATT&CK that is used to streamline and automate the functions of a cyber range, which is used for training. The authors used ATT&CK to specify procedure classification and map corresponding tactics and techniques. Other researchers have also utilized ATT&CK to improve or design professional training programs, including Ahn et al. [29] and Ajmal et al. [54].

Insight 5. ATT&CK enables professionals to enhance their knowledge of the threat landscape and improve their hands-on skills in responding to cyber attacks. By staying up-to-date with the latest threats and using ATT&CK to develop effective defensive strategies, security professionals can better protect their organizations against cyber threats. While there are studies proposing different ways to use ATT&CK in training, a research gap exists in the form of comprehensive evaluation studies that assess the effectiveness and efficiency of these programs. Therefore, there is a need for more empirical research to compare and measure the impact of different approaches on the development of cybersecurity skills and knowledge.

6) A-UC-TA: Threat-driven Approaches: Jadidi et al. [73] emphasized that threat hunting and modeling rely on various inputs, such as CTI, third-party notifications and data from security analysts, to identify threat actor behavior or vulnerabilities. In this way, security professionals can be empowered to stay ahead of emerging threats. To enhance mitigation strategies, Ampel et al. [30] developed a model that automates the mapping of CVEs to ATT&CK techniques within the matrix. They extracted data from 24,863 CVEs across various exploitation databases. Hacks et al. [61] proposed a solution that offers CTI capabilities by utilizing ATT&CK and mapping its components to attack graphs labeled with CTI. Rao et al. [69] introduced a threat modeling framework named *Bhadra*, designed specifically for MCS. Bhadra aligns with ATT&CK for enterprise networks and can be used with or without ATT&CK for threat modeling purposes. Since there was not any dedicated threat modeling framework for MCS, the authors looked into ATT&CK for Enterprise and reused the structure and terminology of ATT&CK.

Sadleck et al. [28] introduced an approach for managing and modeling threats by leveraging Common Platform Enumeration for asset management, CVEs and CWE for vulnerability management, and CAPEC and ATT&CK for threat management. By using ATT&CK and CAPEC together, the authors were able to provide a comprehensive description of adversarial tactics and techniques and attack patterns, leading to better threat management. Kim et al. [102] proposed an automated framework for attributing mobile threat actors by analyzing the mobile malware using automated ATT&CK-based TTP and Indicators of Compromise. Similarly, Fox et al. [14] developed an enhanced cyber threat model for the financial service sector that utilizes ATT&CK and CAPEC. In another study, Jadidi et al. [73] presented a threat-hunting framework to detect cyber threats against ICS devices during the early stages of the attack lifecycle. The authors leveraged ATT&CK to generate hunting hypotheses and predict the future behavior of potential adversaries.

Numerous other research papers have used ATT&CK for threat modeling [70], [43], [47], [49], [51], [53], [55], [56], [59], [60], [61], [63], [122]. Among these, Elitzur et al. [56] utilized a CTI-based knowledge graph, based on ATT&CK, to demonstrate increased accuracy in detecting attack patterns on enterprise networks. They used information and knowledge about past, present, and future cyber attacks that help build a comprehensive understanding of the TTPs used by cyber attackers. Gourisetti et al. [59] developed a framework that provides functions for identifying, protecting, detecting, responding to, and recovering from cyber threats, aligning

recorded events or alerts with relevant attack vectors from ATT&CK. Gylling et al. [60] used ATT&CK as the basis for their CTI when creating their probabilistic attack graph. Xiong et al. [122] introduced a language to model and describe cyber threats and attacks against an enterprise security system using ATT&CK for the enterprise.

Insight 6. ATT&CK is used to model threat scenarios and assess their impact. This helps security teams prioritize their defenses and focus on the most critical cyber risks. We believe there is a need for further research on how to effectively integrate CTI sources beyond ATT&CK into existing security operations workflows and how to leverage the wealth of data generated by CTI for more proactive and effective threat hunting and mitigation.

7) A-UC-PE: Product Evaluation: Since ATT&CK is a well-maintained knowledge base, it can be used for evaluations of cybersecurity products and research tools. Researchers have utilized ATT&CK to evaluate security systems with scoring metrics. For example, Manocha et al. [81] developed a security assessment rating framework that enables precise security rating for security systems. They developed a prediction score that involves weighted exploitability and impact of different levels of an attack technique. In addition, academic research has started to analyze the data stemming from ATT&CK-based product evaluations. For example, Outkin et al. [123] developed a game-theoretic framework that utilizes data from MITRE's APT3 ATT&CK Evaluations. From this data, authors were able to generalize defender capabilities.m Mashima et al. [82] evaluated an in-network deception technology in a smart grid, named DecIED based on ATT&CK for ICS. The work tests the mitigation against a few APT groups including Stuxnet and CrashOverride. It appeared that DecIED was able to mitigate only around half of the total number of ATT&CK techniques.

Insight 7. ATT&CK is used to evaluate the capabilities of cybersecurity technologies such as assessing their ability to respond to ATT&CK tactics and techniques. In this way, organizations can make informed decisions when choosing cybersecurity solutions. There is a lack of standardization in how cybersecurity products implement ATT&CK and since the framework is flexible and customizable, organizations may use it differently or interpret it differently, making it challenging to compare the effectiveness of different cybersecurity products across organizations.

B. A-AD: Application Domains

1) A-AD-EN: Enterprise Networks: This section discusses works that study attacks and threats related to popular CVEs of enterprise systems (vulnerabilities commonly used for internal infrastructure exploitation) [29], [30], [54]. Ahn et al. [29] proposed a system configuration model (specific elements that define or prescribe what a system is composed of) based on the Cyber Kill Chain (CKC) and ATT&CK to produce analytical data on threat actors resulting in providing infrastructure protection mitigation strategies. The authors utilized ATT&CK for cyber warfare simulation and threat analysis. Xiong et al. [36] proposed a threat modeling language for enterprise network security based on ATT&CK. They analyzed

key features between ATT&CK and a Meta Attack Language framework, combining knowledge from both to define attack steps, defenses, and asset associations. Munaiah et al. [33] carried out a penetration testing competition for enterprise systems. The authors analyzed a dataset of over 500 million events generated by six teams of attackers during a penetration testing competition. The authors examined the competition data set to identify ATT&CK tactics and techniques and found that it is possible to describe attackers' campaigns in a chronological sequence by analyzing their behavior.

Previous research that uses ATT&CK has explored the connection between CVEs and ATT&CK tactics to develop effective mitigation strategies [32]. Additionally, Kim et al. [68], [38] gathered data to develop a training system for cybersecurity that focuses on threats to internal infrastructure and enterprise systems, which the simulation aims to address. The authors identified different ATT&CK techniques and obtained scoring results for some APT groups. Hemberg et al. [37] attempted to link ATT&CK, NIST CWEs, CVEs, and CAPEC. This paper takes five browsers and compares their severity ratings, in terms of CVEs, to determine the motives behind attacks and how they will be executed. In general, most threat modeling works that use ATT&CK, including [31], [34], [44], [107], [74] discuss internal infrastructure attacks and the simulated threats are related to the enterprise systems' internal infrastructure. Here, Outkin et al. [34] developed reliable criteria for allocating resources across such detection and response opportunities at different steps in the attack. To evaluate defender policy, the authors incorporated the results of ATT&CK Evaluation into attack success and defender response metrics.

Additionally, ATT&CK is also being used for cloud security [103], [122], [104], [105], [106]. Sahu et al. [103] developed an Infrastructure-as-a-Service (IaaS) security model named MISP, where the authors considered the ATT&CK matrix for enterprises and a subset of it for cloud computing. The authors filtered the necessary TTPs related to the cloud for the evaluation of the adversary's behavior. Zhao et al. [104], [105] developed a board game to improve cloud security that includes an automated evaluator to check defense plans and attack plans built by invited players. The attack cards, defense cards, and the mapping between them are derived from ATT&CK and CSA cloud control matrix.

2) A-AD-MCS: Mobile Communication Systems: Mobile Communication Systems (MCS) are evolving and require standardized threat modeling frameworks [124]. Authors state that ATT&CK and Bhadra [69] are most useful for MCS-based threat modeling. Rao et al. [69] claimed that Bhadra aligns conveniently with ATT&CK. Nevertheless, within the MCS domain, most works utilize ATT&CK for threat modeling and threat detection. Early stage 5G networks have incorporated the use of ATT&CK to demonstrate the exploitation of network functions NFV and SDN. 5G threat assessments and industry reports offer studies on how the domain-specific techniques can be used by Advanced persistent threats in multi-step attacks for 5GCN networks. Pell et al. [35] discusses how to exploit front-facing network functions to compromise 5G networks. This work has contributed to the MITRE FiGHT,

which is a knowledge base of adversary Tactics and Techniques for 5G systems [125].

3) A-AD-ICS: Industrial Control Systems: Industrial Control Systems (ICS) are critical environments such as Gas, Oil, and nuclear industries. ATT&CK literature has studied ICS and its equipment, including evaluation testbeds for ICS systems [4], [39], [43], [59], [126]. Choi et al. [4] introduced a method to expand existing testbeds for ICS so that information can be collected during a cyber incident based on ATT&CK. This method is useful for creating attack simulations for ICS. In a later work, authors introduced a probabilistic attack sequence generator to leverage ICS datasets [39]. Here, the authors proposed a method for generating attack sequences based on the characteristics desired by the user using tactics and techniques from ATT&CK. They overcame difficulties in developing an ICS dataset by implementing a hidden Markov model-based attack sequence generation method that uses probabilities to produce the attack sequence. Dhirani et al. [83] utilized ATT&CK along with other standards (e.g. NIST 800 − 82, ISO 27001, IEC 62443, etc.) to build unified an Industrial IoT standards roadmap. They specifically used ATT&CK for identifying different aspects of ICS/SCADA security.

C. A-RF: Related Frameworks

As a well-documented knowledge base of adversarial behavior, ATT&CK has been widely adopted and combined with other cybersecurity frameworks by both academic and industrial researchers to achieve specific goals.

1) A-RF-CA: CAPEC: In addition to ATT&CK, various threat frameworks are utilized, including the Common Attack Pattern Enumeration and Classification (CAPEC) [127]. CAPEC is a threat modeling framework that focuses on application security and is primarily associated with Common Weakness Enumeration (CWE) [128]. On the other hand, ATT&CK concentrates on network defense. Although CAPEC describes common patterns frequently employed by specific techniques described in ATT&CK, the cross-reference helps to improve threat management by identifying potential vulnerabilities. For example, Adam et al. mapped CWEs to ATT&CK techniques via CAPEC [71], while Aghaei et al. [53] created a mapping between all CVEs, CAPEC and ATT&CK. Also, CAPEC can provide valuable insights into potential vulnerabilities within an application, while ATT&CK can provide information on how attackers might exploit those vulnerabilities to achieve their goals.

The integration of ATT&CK and CAPEC helps organizations to detect and mitigate a wide range of threats, including attacks against applications (which is the primary focus of CAPEC) and network infrastructure (which is the primary focus of ATT&CK). As a result, organizations can have a more comprehensive view of the threat landscape and develop a more effective response to cyber threats. Sadlek et al. [28] have combined CAPEC and ATT&CK for more effective threat management. Similarly, Fox et al. [14] have integrated ATT&CK and CAPEC to construct an extensive high-level threat modeling framework. Interestingly, some researchers have developed a formal knowledge base or model that unites all existing attack knowledge bases. For instance, Brazhuk et al. [55] established relationships between ATT&CK, CAPEC, CWE and CVE security enumerations to create a generic knowledge base that offers improved threat modeling over previous threat-based approaches.

2) A-RF-CKC: Cyber Kill Chain: ATT&CK consists of 14 tactics that can be mapped to the phases of Lockheed Martin's Cyber Kill Chain (CKC): Reconnaissance, Weaponization, Delivery, Exploitation, Installation, Command & Control and Actions on Objectives. Unlike the traditional CKC, ATT&CK is a globally accessible knowledge base, which makes it more comprehensive but is also regularly updated with new techniques based on real-world observations. By understanding the different stages of an attack and the specific TTPs used by attackers, organizations can detect and prevent attacks earlier in the CKC. By mapping known TTPs to the different stages of CKC, organizations can develop a more targeted and effective response to an attack. Naik et al. [129] have studied characteristics, advantages and disadvantages of ATT&CK and CKC and provide a comparative study to highlight the most suitable attack models for different applications.

3) A-RF-ST: STRIDE: A few works integrated multiple threat modeling frameworks for specific tasks including risk analysis and mitigation, defense framework design, and vulnerability analysis. Bolbot et al. [65] integrated ATT&CK and STRIDE alongside cybersecurity analysis methodologies for risk analysis and mitigation. Sadlek et al. [72] also used both ATT&CK and STRIDE to identify attack paths. Straub [130] compared the capabilities of ATT&CK, STRIDE, and Cyber Kill Chain in the context of offensive and defensive use. He concludes that while STRIDE is useful for defensive purposes, it lacks the features required for direct offensive use. Additionally, STRIDE does not have an explicit steps to deploy an attack against the targeted vulnerability, which is a key feature of ATT&CK. Overall, Straub's analysis suggests that while STRIDE and ATT&CK both have their strengths and weaknesses, they serve different purposes and can be used in different ways depending on the specific goals of a given security operation.

4) A-RF-SC: Security Controls: To achieve threat-informed defense, native security controls can be mapped to ATT&CK. Security Stack Mappings [131] produces mapping files for different cloud platforms, including Microsoft Azure, Amazon Web Service, and Google Cloud Platform, to aid organizations. The online repository offers supporting resources, including scoring rubrics, mapping data formats, and mapping tools that produce the ATT&CK navigator for mapping files. In practice, the security teams are utilizing the mapping of ATT&CK TTPs to Azure-native security controls [12]. Bromander et al. [44] developed a graph-based data model that linked objects obtained from ATT&CK, STIX [132], detection maturity model [133] and the Diamond model [134].

The National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) was developed in 2014 and utilized to strengthen the defense and resiliency of federal networks and critical infrastructure. Kwon et al. [43] proposed a Cyber Threat Dictionary that can map all attack and defense tactics to the Facility Cybersecurity Framework (FCF) through

a correlation matrix [135]. FCF is specifically designed for facility-related control systems and operational technology, which motivated the authors to use the ATT&CK for ICS matrix for mapping with FCF.

Although ATT&CK includes mitigation techniques against the TTPs, MITRE provides a separate and comprehensive framework named D3FEND [136], which is a knowledge graph of cybersecurity countermeasures [137]. ATT&CK is designed from the adversaries perspective while D3FEND was built from the defenders' perspective. D3FEND was also used in academic research works such as Luh et al. [84].

5) A-RF-MI: Miscellaneous: Threat modeling frameworks include ATT&CK, CAPEC, PASTA, WASC and OWASP. Other frameworks including Microsoft's DREAD, OCTAVE, Intel's Threat Agent Risk Assessment (TARA) and Threat Agent Library (TAL) are used for supporting security design, analysis and testing. PASTA (Process for Attack Simulation & Threat Analysis) has been used for threat modeling in industrial IoT [138]. Some frameworks including STIX (the Structured Threat Information eXpression), PRE-ATT&CK and ODNI's CTF (Cyber Threat Framework) are useful for supporting attack information sharing. These frameworks can be integrated with ATT&CK to generate more comprehensive and valuable risk models, thereby facilitating the identification of more effective security controls.

Jadidi et al. [73] proposed a unified threat-hunting model for ICS that combines ATT&CK for ICS and the Diamond model of intrusion analysis to predict the future behavior of the adversaries. The model can provide endpoint security logs, user behavior analytics and network or application threat analytics, which are useful to organizations. The authors evaluated their model against real-life attacks including the Ukrainian power grid attack by Black Energy 3, the DoS attack on SIEMENS PLC and Tank 101 underflow.

According to Mundt et al. [74], integrating CTI with Information Security Management Systems (ISMS) can result in robust data security approaches. They suggest that implementing and automating CTI processes within an ISMS can be facilitated using the ATT&CK framework, which is commonly used by security researchers in conjunction with ISMS. To illustrate the interactions between the CTI and ISMS processes, including communication and data exfiltration, the authors use Business Process Modeling Notation (BPMN) diagrams. The proposed approach involves human actors such as a cyber analyst or Chief Information Security Officer (CISO) and follows the guidelines outlined in ISO/IEC 27000:2018. By incorporating the ATT&CK framework into their ISMS, organizations can improve their ability to detect and respond to threats, thus enhancing their overall data security [74].

Hemberg et al. [37] proposed a framework to combine ATT&CK, NIST, CWEs, CVEs and CAPEC. The authors proposed a bidirectional data graph named BRON to gain further insight from alerts, threats and vulnerabilities by creating links between collected information of the frameworks mentioned above. The relational links were achieved via linking ATT&CK techniques to attack patterns, then attack patterns to CWEs and finally, CWEs to CVEs. Luh et al. [84] considered ATT&CK, D3FEND and the NIST SP 800-53 to build their attack scenarios while Osquery-ATT&CK [139] maps ATT&CK to Osquery [140] for enterprise threat hunting. Osquery performs continuous testing for memory leaks, thread safety and binary reproducibility on all supported platforms, including Windows, macOS and Linux (e.g. CentOS) [141]. Sigma rules tagged with a $attack.tXXXX$ tag can generate the ATT&CK Navigator [142] heatmap from a directory containing sigma rules. Last, the Atomic Red Team [143] is a collection of atomic tests that are mapped to ATT&CK. The tests can be performed using command-line and aids security teams to conveniently test their environments.

D. Use of ATT&CK in Academia and Industry

ATT&CK has gained significant attention from cybersecurity researchers in both academia and industry. While initially used by the industry to improve their tools and services, academic researchers have also recognized its usefulness in evaluating their research. This has resulted in a rapid development of new tools that integrate and incorporate ATT&CK tactics and techniques. Security analysts and specialists use ATT&CK in conjunction with other security frameworks, standards, policies, compliance and guidelines to obtain comprehensive recommendations on how to secure systems. Considering ATT&CK as a baseline knowledge-base of TTPs, industrial research heavily involves the framework to evaluate their products, including SIEM (Security, Information, and Event Management), EDR (Endpoint Detection and Response) and deception tools.

Cyber Threat Intelligence. Academic researchers primarily focus on text classification and NLP for retrieving intelligence from CTI reports. On the other hand, the industry primarily uses ATT&CK matrices and navigators to filter and score threats based on threat groups, techniques, platform and associated mitigation. They also develop tools and APIs (using ATT&CK) for standard CTI sharing between organizations and developing extended threat detection tools.

Intrusion Detection. Academia mostly attempts to categorize ATT&CK tactics and techniques, build knowledge graphs and apply machine learning for detection and mitigation. The industry adopts and tailors ATT&CK to develop their incident management and response tools.

Offensive Security. Academia uses ATT&CK to create offensive security taxonomies, analyze past offensive security competition data and model adversarial behavior. The industry involves red and purple team exercises and organizes penetration testing using ATT&CK.

Cyber Risk Assessment. Both academic and industrial researchers use ATT&CK for assessing cyber risk by mapping threat behaviors with vulnerabilities and then proposing ways to mitigate the identified risks. Academic scholars attempt to connect other frameworks with ATT&CK for development of better risk management. Security vendors adhere to this mapping for conducting bespoke cyber risk management for their users.

Professional Training. Academic work focuses on theoretical analysis and modeling whereas industry addresses the training of their employees (red/purple teams), staff and clients, with practical exercises.

Threat-driven Approaches. Academic research primarily attempts to propose new threat modeling frameworks aligned with ATT&CK. In contrary, the industry focuses on tailoring threat modeling frameworks to use them in commercial products.

Product Evaluation. Academia undertakes research regarding the ATT&CK evaluation process. Industrial work involves product evaluations to determine if their developed security solutions can detect and consequently mitigate known threat actors.

IV. RESEARCH APPROACHES (RA) USING ATT&CK

In this section, we first discuss scientific methods used to build attack scenarios, models and methods based on ATT&CK matrices. These approaches include machine learning (including natural language processing), probability theory, graph theory and game theory. Second, we study how ATT&CK has been used in implementation of testbeds and security tools. Third, we study the different methods (e.g. numerical or statistical, human-based and model-based evaluations) of evaluating research that has used ATT&CK.

A. RA-SM: Scientific Methods

1) RA-SM-ML: Machine Learning: Machine learning has widely been used for different ATT&CK-based research works. Al et al. [5] used statistical machine learning analysis on APT and software attack data (270 total attack instances), reported by ATT&CK, to identify correlations and associations among attack techniques. Dhir et al. [89] proposed to encode the labels of ATT&CK into a set of matrices to develop the relationship between reports and labels. The authors utilized a transformer for the semantic representation of CTI reports and built causal inference to ATT&CK. Holder et al. [90] also focused on causal inference applied to ATT&CK. The authors utilized explainable AI (XAI)-oriented defense recommendations and attack predictions based on ATT&CK patterns.

ML and neural networks are often used for detection purpose. For example, Ahn et al. [91] performed ML-based malicious file detection and visualization based on dynamic-analysis-based ATT&CK. Stoleriu et al. [92] proposed ML-based analysis and detection of APT attacks using ELK stack (Elasticsearch, Logstash and Kibana), where the authors retrieved a series of APT-based attacks included in the ATT&CK matrix. Hasan et al. [98] developed a decision support system for cyber threat detection and protection using ATT&CK tactics and techniques. Huang et al. [47] used deep learning and ATT&CK knowledge to develop a behavior analysis system for Windows malware. Hemberg et al. [144] built ATT&CK-based datasets for predicting threat techniques and attack patterns. Zurowski et al. [94] created a public dataset that includes ML-based tools, which are mapped to ATT&CK Enterprise techniques. Bagui et al. [93] developed an ML-based ATT&CK-oriented big data analysis framework for detecting reconnaissance and discovery tactics. Alnafrani et al. [95] developed an AI-based forensic investigative system, where authors used ATT&CK to understand potential attacker capabilities. Mayami et al. [99] created a semantic representation of adversarial TTPs, where the authors built a model of APT28 using ATT&CK. Similarly, other works ([49], [53]) built ML models to map vulnerabilities to adversarial tactics listed in ATT&CK.

2) RA-SM-NLP: Natural Language Processing: Natural Language Processing (NLP) is a field of study that involves the application of ML algorithms and models to analyze, understand and generate human language data. NLP has proven useful for CTI, particularly in retrieving summaries from threat reports. Liu et al. [145] used an attention transformer hierarchical recurrent neural network to extract ATT&CK information from CTI. Kuppa et al. [32] employed NLP techniques, such as the Multi-Head Joint Embedding Neural Network model, to automatically map CVEs to ATT&CK techniques. Chen et al. [70] developed an anomaly detection and threat hunting system that utilizes NLP and graph modeling. The authors used ATT&CK APT3 evaluation data and applied NLP techniques to process Windows logs for seeking suspicious patterns. Niakanlahiji et al. [75] presented an NLP-based trend analysis to present how to obtain knowledge regarding APTs from unstructured reports and developed an information retrieval system named SECCMiner that combines NLP processes and information retrieval system concepts to categorize APTs based on ATT&CK tactics. Husari et al. [85] also utilized NLP to characterize the temporal relationship of attack actions of an APT using ATT&CK and a machine readable language named STIX. Apart from the above-mentioned works, [76], [52], [77], [146], [28], [70], [147] have involved NLP and ATT&CK for automated threat intelligence, modeling and mapping.

3) RA-SM-PT: Probability Theory: Choi et al. [39] utilized a hidden Markov model to generate varied attack sequences based on user objectives. The authors considered the probability of starting each ATT&CK tactic as the initial state probability, probability of movement between each tactic as transition probability and probability of the occurrence of a particular technique (under the same tactics) as the emission probability. The attack sequence generation can leverage ICS datasets and provide various attack scenarios performed in real life by different malware including Stuxnet (Iran nuclear facilities), BlackEnergy3 & Industroyer (Ukraine power grid), Triton (Saudi Arabia petrochemical plant), Bad Rabbit (Ukrainian transportation) and LockerGoga (Norway aluminum company). Other works including [64], [148], [79] calculated probabilities of different attack scenarios to assess and mitigate risks. All these works recognized ATT&CK as a standard knowledge base of TTPs and utilized listed tactics and techniques for their simulated attack scenarios.

4) RA-SM-GM: Graph Modeling: Kriaa et al. [42] used graph theory due to the complex nature of APTs and comprehensive attack methods, which provides a better evaluation than some other existing methods. Here, the authors combined knowledge graphs and machine learning to detect and prevent adversarial techniques. Xiong et al. [36] proposed algorithms and graph-based mapping to provide insights into certain attacks, such as MAL file Access Token Manipulation. The authors proposed a threat modeling language called enterprise-Lang, which presents a domain-specific language based on the

Meta Attack Language (MAL [80]) framework. Here, MAL is directly associated with ATT&CK and leverages TTPs to define attack steps in the language. Hacks et al. [61] proposed an approach for integrating user actions and security behavior to attack simulations by mapping Security Behavior Analysis (SBA) to MAL through ATT&CK techniques. Hemberg et al. [37] proposed a graph-based linking technique called BRON that links ATT&CK techniques to attack patterns, patterns to weaknesses and weaknesses to CVEs. More works, including [46], [57], [100] utilized ATT&CK and graphs for threat intelligence and modeling.

5) RA-SM-GT: Game Theory: Outkin et al. [123] proposed a game-theoretic framework, called GPLADD, to constantly allocate resources (e.g. to sensing and assessment of attack indicators) against an uncertain stream of attacks. The attack data used for the evaluation of the framework are from ATT&CK. Nisioti et al. [86] utilized game theory to determine optimal investigating policies after a cyber incident. The proposed framework considers the cost for investigating an ATT&CK technique and available actions for the investigator with the attacker type and anti-forensics techniques being unknown. Luh et al. [84] proposed a game-theoretic framework, called PenQuest, to support security education and cyber risk assessment by simulating a game whether an attacker attempts to compromise an infrastructure and the defender attempts to protect it. As in the previous papers, attack data for the evaluation of PenQuest were drawn from ATT&CK.

B. RA-I: Implementations

1) RA-I-TE: Testbeds: Choi et al. [4] outlined vulnerabilities and threats for ICS and implemented a testbed to help fix cybersecurity issues by offering a better understanding of how to mitigate vulnerabilities. The authors set 52 techniques excluding duplicates in ten tactics mapped to 92 intrusion detection rules using the ATT&CK for Enterprise. Hong et al. [31] implemented a testbed where a simulated threat generator automatically generates cyber threats based on ATT&CK to help improve the coping ability of system security officers in dealing with cyber threats. Here, the threat generator allows for the addition of evolving cyber threats and the selection of the next threat. Halverson et al. [87] developed a testbed to evaluate the effectiveness of their developed tool TOMATO, which uses MITRE ATT&CK to simulate attacks and evaluate the observability and efficiency of a set of deployed monitoring techniques. The approach was integrated into an ELK stack, and evaluated on real SCADA devices within the Washington State University smart city testbed. Most papers that use ATT&CK for offensive security or professional training implemented a testbed to deploy the attack scenarios. For example, Ajmal et al. [54] developed a simulated environment to implement different attack scenarios. Luh et al. [84] developed a testbed for human experimentation-based evaluation of their proposed game model. Drašar et al. [100] created a small-scale network to emulate various ATT&CK-based attack scenarios.

2) RA-I-TO: Tools: ATT&CK aids adversarial emulation and consequent defensive tools that can assess certain attack scenarios. ATT&CK has been used to design and develop certain adversary emulation tools including Red or Purple team tools. Defensive tools are also designed and developed considering ATT&CK-based tactics and techniques. Halvorsen et al. [87] developed the TOMATO (Threat Observability and Monitoring Assessment) tool that can evaluate the observability of network security monitoring strategies. TOMATO provides observability scores and monitoring technique efficiency scores while using ATT&CK-based simulated attacks.

Red Teaming Tools. There are a few open-source ATT&CK test tools including CALDERA [149], Endgame Red teaming Automation [150], Red Canary Atomic Red [143] and Uber Metta [151]. These tools have adapted ATT&CK and provided platforms for red teams to simulate attacks. Each tool features a different set of tactics for penetrating a network and helps the administrator find out the security weaknesses or entry points. Since ATT&CK itself is always under development, these tools follow the same path, and new features are added on a regular basis.

Purple Teaming Tools. Purple Team ATT&CK Automation [152] is another automated adversary tactics emulation platform that is built on top of the Metasploit framework [153]. The platform integrated codes and techniques from ATT&CK, tools like CALDERA, and libraries like the Atomic Red Team [143] and RE:TERNAL [154], which is a centralized purple team orchestration service to test blue-team capabilities against red-team techniques. All included simulations of the tool are mapped and aligned to ATT&CK. There are other ATT&CK-oriented tools as well, which are used for generating detection rules (e.g. sigma rules). For example, S2AN [155] is a standalone tool that creates an ATT&CK Navigator [142] based on a directory containing sigma rules [156] and Suricata signatures. Kriaa et al. [42] used the Grakn tool to create targeted knowledge graphs and query them using the *graql* language. The authors built a knowledge graph for their proposed approach using ATT&CK, to gather knowledge on attacks from different sources. This offers capabilities to detect attack techniques and then learn to predict them by processing event logs.

Appropriate datasets are necessary to aid the community with mapping real data to open source projects such as Sigma, Atomic Red Team, Threat Hunter Playbook, and ATT&CK knowledge base. The project entitled *Security Datasets* [157] is an open-source dataset collection that facilitates adversary emulation, enables security and threat actor analysis and adversarial behavior, and provides datasets for Capture-The-Flag (CTF) competitions.

C. RA-E: Evaluations

1) RA-E-NE: Numeric Evaluation: Al et al. [5] utilized hierarchical clustering to investigate the association among techniques included in ATT&CK and later discovered 98 different clusters representing these associations. The authors evaluated the mutual information (of the techniques in the fine-grain clusters, as well as the coarse-grain clusters directly from the datasets) by measuring fine-grain associations (within the same cluster) for APTs using both technique-based and cluster-based normalized mutual information (NMI). The *max-*

imum predictability of each technique can be calculated based on its cluster assignment.

Hemberg et al. [37] evaluated their graph model through different statistical analyses. The number of edges (links) is calculated as they connect different ATT&CK techniques, patterns, weaknesses, and associated CVEs. By calculating the query times for threats connected to the Top 10 CVEs, threats, and vulnerabilities for the top 25 CWEs and riskiest software, the authors measured the relational linkage statistics for tactics, techniques, and attack patterns over the number of edges in the graph. Similarly, the authors measured the counts and distributions of vulnerability connections and affected product configurations.

Kim et al. [38] provided a severity scoring methodology for APT-based and fileless cyber attacks and later evaluated the scores with the cyber kill chain and ATT&CK. The authors evaluated APTs and fileless cyberattacks that occurred between 2010 and 2020. They calculated scores for the APT groups: powerliks, Rozena, Duqu 2.0, Kovter, Petya, Sorebrect, WannaCry, Magniber, Emotet and Gandcrab.

2) RA-E-HE: Human Evaluation: Hacks et al. [61] integrated human behavior analysis to the attack simulations and attempted to calculate probabilities of an attack being successful. Authors conducted surveys where employees would answer the questionnaire of Security Behavior Analysis and their answers were given as inputs to a vulnerability assessment tool for conducting attack simulation on an IT infrastructure. Further, evaluating a model or association by domain experts is often helpful. Al et al. [5] recruited six domain experts with at least five years of experience and knowledge in the area of cyber threat intelligence and ATT&CK. According to the experts, 93% of the fine-grain associations of ATT&CK techniques (within the same cluster) and 90% of the coarse-grain associations (inter-cluster) present strong correlations, which validates their way of utilizing hierarchical clustering techniques.

Oconnor [67] developed a lab (e.g. post-exploit lab) for practicing and improving experiential learning, payloads writing, detection evasion, attack functionality, post-exploitation tools development and network traffic manipulation based on ATT&CK. The author discussed ethical issues and introduced to the students the Computer and Fraud Abuse Act (CFAA), Electronic Communications Privacy Act (ECPA), the Digital Millennium Copyright Act (DCMA) and the corresponding university's acceptable use policy. Last, Luh et al. [84] involved students to evaluate their proposed game theoretic model for technical education.

3) RA-E-ME: Model Evaluation: Most of the works that use ATT&CK to develop a threat model, later evaluate it based on the reliability in providing security assessments and suggesting security settings. For example, Xiong et al. [36] evaluated enterpriseLang by modeling two attack scenarios: the Ukraine cyber attack of 2015 and the Cayman National Bank cyber heist of 2016. The authors used the Enterprise ATT&CK matrix as a knowledge base for the proposed language.

Choi et al. [39] evaluated their Hidden Markov Model-based attack sequence generator by validating whether the attack

sequence from initial access to impact follows the pattern of real-life malware. The authors adopted ATT&CK to design the attack sequence. They confirmed that this model generated the actual attack sequence of Triton, which was discovered in the Saudi Arabia petrochemical plant. Ampel et al. [30] compared their CVET model against benchmark classical machine learning, deep learning, and pre-trained language models for text classification tasks to understand how these models perform while linking CVEs to ATT&CK. The authors showed that CVET achieves the highest accuracy (76.93%) and F1-score (76.18%) among the compared models.

V. CONCLUSIONS AND FUTURE DIRECTIONS

This paper provides a comprehensive review of research and industry applications of the MITRE ATT&CK framework and proposes a taxonomy for categorizing literature that uses ATT&CK. In this section, we will recapitulate the essential points discussed in the preceding sections and delve into contemporary challenges, constraints and potential future research works associated with ATT&CK.

Holistic Approach. ATT&CK takes a holistic approach to cybersecurity, covering defensive and offensive techniques. It provides a comprehensive list of adversary tactics and techniques used in cyber attacks, making it an essential resource for threat intelligence, threat modeling, risk assessment and offensive security. This approach makes it possible to understand better the adversary and their tactics, which is essential for developing effective defense strategies.

Open and Community-Driven. ATT&CK is continually updated based on community feedback and contributions. This collaborative approach ensures that the framework remains up-to-date and relevant, providing organizations with the latest information on adversary tactics and techniques.

Common Medium for Knowledge Sharing. ATT&CK provides a common language for the cybersecurity industry in terms of threat intelligence, making it easier for organizations to communicate and collaborate on cybersecurity. This common language ensures that everyone is on the same page, which is essential for effective communication and collaboration in the emerging threat landscape.

Wide Coverage. ATT&CK covers a wide range of attack techniques across different platforms and technologies, including Windows, Linux and macOS. It also covers ICS, Cloud and Mobile platforms. This broad coverage makes it a valuable resource for organizations with different IT environments.

Mapping to Other Frameworks. As we have seen in the existing literature, ATT&CK can be mapped to other cybersecurity frameworks, such as the NIST Cybersecurity Framework, ISO/IEC 27001, COBIT, etc. This mapping provides a way to merge different frameworks to achieve particular needs.

Flexibility. ATT&CK is customizable. It enables organizations to utilize it to their specific needs such as create custom intelligence, threat models, risk assessments and offensive security strategies. This customization makes the framework more relevant and valuable to specific organizations and industries.

Even though ATT&CK is a reputed knowledge base of TTPs, there are a few limitations of it.

Evolving Threat Landscape. The threat landscape constantly evolves and attackers are constantly developing new TTPs. ATT&CK may only sometimes reflect the latest threats and must be updated regularly to stay current.

Limited Geographical Coverage. ATT&CK is based on observations of attacks that have taken place in the United States, Europe and other developed regions. The tactics and techniques used by attackers in other parts of the world may need to be better represented in the framework.

Focus on Specific Threat Actors. ATT&CK focuses on a limited set of well-known threat actors and may need to fully capture the tactics and techniques used by other, less well-known groups.

Tactical Level. ATT&CK provides a tactical-level view of adversary tactics and techniques and does not provide a comprehensive view of the overall attack lifecycle.

Despite the widespread adoption of ATT&CK for improved threat mitigation and prevention, there remain a few untapped scenarios for researchers and developers to contribute to. The following require answers in future studies.

Real-time Threat Intelligence and Incident Response. Real-time threat intelligence is critical for quickly detecting and responding to attacks. We find a lack of research that utilizes ATT&CK to address these issues. Researchers and experts can work on developing real-time threat intelligence capabilities that can leverage ATT&CK to identify and respond to attacks more quickly.

Risk Quantification. Cyber risk quantification (CRQ) is a major challenge in both fields of cyber research and in the progress of industry. Accurate risk assessments are crucial for ensuring effective spending, as demonstrated by the demands of Chief Information Security Officers (CISOs). Extended research on ATT&CK can address this challenge by incorporating CRQ methods that are derived from ATT&CK and seamlessly integrate threat behaviors and quantitative data from threat intelligence sources, such as threat event frequency [158].

Collaboration between Academic and Industrial Research. ATT&CK provides a platform for academic and industry stakeholders to showcase the performance of their methods or implement their software and serve their clients. However, ongoing revision and expansion of the framework concepts and data are essential to keep up with evolving threat behaviors. Integrating industry and academic perspectives through collaboration is crucial in determining the need for new techniques or tactics and developing effective mitigation methods against newly discovered threat mechanisms or sub-techniques. One way, researchers can reduce the gap is to develop new ideas in academia and evaluate these new frameworks, techniques, or workflows in the industry.

Developing Industry-specific Threat Models. While ATT&CK covers a wide range of platforms and technologies, industry-specific threat models can provide a more tailored approach to identifying and responding to attacks in particular attack scenarios. Researchers and experts can further work on developing industry-specific threat models that leverage ATT&CK.

With the evolution and improvement of language models and chatbots like chatGPT, cyber threat intelligence and modeling have new areas to explore. Overall, emerging technologies lead to continuously new cyber threats and ATT&CK is required to be updated on a regular basis. Each of these updates can initiate new research directions for academic researchers and industrial experts.

We believe that future research and development will benefit from close collaborations between academic and industrial researchers. For example, academia can utilize theoretical attack and defense models that involve ATT&CK and then the industry can test their products against these models. Likewise, the industry can share data, from the evaluation of their products, with academic scholars for fostering novel scientific ideas in the field, which can then feed back to their products and services.

REFERENCES

[1] A. Georgiadou, S. Mouzakitis, and D. Askounis, "Assessing MITRE ATT&CK risk using a cyber-security culture framework," *Sensors*, vol. 21, no. 9, p. 3267, 2021.

[2] D. J. Bodeau, C. D. McCollum, and D. B. Fox, "Cyber threat modeling: Survey, assessment, and representative framework," MITRE CORP MCLEAN VA MCLEAN, Tech. Rep., 2018.

[3] M. Bromiley, "SANS 2022 ATT&CK and D3FEND report: Incorporating frameworks into your analysis and intelligence," SANS Institute, January 2022.

[4] S. Choi, J. Choi, J.-H. Yun, B.-G. Min, and H. Kim, "Expansion of ICS testbed for security validation based on MITRE ATT&CK techniques," in *13th USENIX Workshop on Cyber Security Experimentation and Test (CSET)*, 2020.

[5] R. Al-Shaer, J. M. Spring, and E. Christou, "Learning the associations of MITRE ATT&CK adversarial techniques," in *2020 IEEE Conference on Communications and Network Security (CNS)*. IEEE, 2020, pp. 1–9.

[6] A. Pennington, A. Applebaum, K. Nickels, T. Schulz, B. Strom, and J. Wunder, "Getting started with ATT&CK," MITRE Corp, McLean, VA, Tech. Rep., 2019.

[7] O. Alexander, M. Belisle, and J. Steele, "MITRE ATT&CK for industrial control systems: Design and philosophy," *MITRE Corporation, Bedford, MA, USA*, 2020.

[8] CLAROTY, "Supporting the MITRE ATT&CK for ICS framework," https://security.claroty.com/white-paper/supporting-mitre-ics, 2021.

[9] Cylance, "How to use the MITRE ATT&CK enterprise framework," Research Desk, https://www.demandtalk.com/whitepaper/it-infra/how-to-use-the-mitre-attck-enterprise-framework/, October 2019.

[10] C. Secure, "Why endpoint security is critical to today's ciso," Cisco Public, https://www.cisco.com/c/en/us/products/collateral/security/white-paper-c11-744950.pdf, May 2021.

[11] FORTINET, "Assess your endpoint security," https://www.fortinet.com/content/dam/fortinet/assets/white-papers/wp-assess-your-endoint-security.pdf, March 2022.

[12] ATTACKIQ, "Leveraging MITRE ATT&CK to secure the cloud," https://attackiq.com/lp/leveraging-mitre-attack-to-secure-the-cloud/, 2021.

[13] M. Parmar and A. Domingo, "On the use of cyber threat intelligence (cti) in support of developing the commander's understanding of the adversary," in *MILCOM 2019-2019 IEEE Military Communications Conference (MILCOM)*. IEEE, 2019, pp. 1–6.

[14] D. B. Fox, E. I. Arnoth, C. W. Skorupka, C. D. McCollum, and D. Bodeau, "Enhanced cyber threat model for financial services sector (FSS) institutions," *The Homeland Security Systems Engineering and Development Institute, McLean, VA, USA*, 2018.

[15] T. D. Wagner, K. Mahbub, E. Palomar, and A. E. Abdallah, "Cyber threat intelligence sharing: Survey and research directions," *Computers & Security*, vol. 87, p. 101589, 2019.

[16] D. Schlette, M. Caselli, and G. Pernul, "A comparative study on cyber threat intelligence: The security incident response perspective," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 4, pp. 2525–2556, 2021.

[17] G. Cascavilla, D. A. Tamburri, and W.-J. Van Den Heuvel, "Cybercrime threat intelligence: A systematic multi-vocal literature review," *Computers & Security*, vol. 105, p. 102258, 2021.

[18] A. Ibrahim, D. Thiruvady, J. G. Schneider, and M. Abdelrazek, "The challenges of leveraging threat intelligence to stop data breaches," *Frontiers in Computer Science*, vol. 2, p. 36, 2020.

[19] A. Dutta and S. Kant, "An overview of cyber threat intelligence platform and role of artificial intelligence and machine learning," in *International Conference on Information Systems Security*. Springer, 2020, pp. 81–86.

[20] A. Zibak, C. Sauerwein, and A. C. Simpson, "Threat intelligence quality dimensions for research and practice," *Digital Threats: Research and Practice*, 2022.

[21] M. S. Abu, S. R. Selamat, A. Ariffin, and R. Yusof, "Cyber threat intelligence–issue and challenges," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 10, no. 1, pp. 371–379, 2018.

[22] W. Tounsi and H. Rais, "A survey on technical threat intelligence in the age of sophisticated cyber attacks," *Computers & security*, vol. 72, pp. 212–233, 2018.

[23] V. Mavroeidis and S. Bromander, "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)*. IEEE, 2017, pp. 91–98.

[24] R. Brown and R. M. Lee, "2021 SANS cyber threat intelligence survey," in *Tech. Rep.* SANS Institute, 2021.

[25] ——, "The evolution of cyber threat intelligence (CTI): 2019 SANS CTI survey," *SANS Institute. Available online: https://www.sans.org/white-papers/38790/, Accessed on July 12, 2021.*, 2019.

[26] D. Shackleford, "Cyber threat intelligence uses, successes and failures: The SANS 2017 CTI survey," *SANS Institute*, 2017.

[27] D. Tayouri, N. Baum, A. Shabtai, and R. Puzis, "A survey of mulval extensions and their attack scenarios coverage," *IEEE Access*, 2023.

[28] L. Sadlek, P. Čeleda, and D. Tovarňák, "Current challenges of cyber threat and vulnerability identification using public enumerations," in *Proceedings of the 17th International Conference on Availability, Reliability and Security*, 2022, pp. 1–8.

[29] M. K. Ahn and J. R. Lee, "Research on system architecture and methodology based on MITRE ATT&CK for experiment analysis on cyber warfare simulation," *Journal of the Korea Society of Computer and Information*, vol. 25, no. 8, pp. 31–37, 2020.

[30] B. Ampel, S. Samtani, S. Ullman, and H. Chen, "Linking common vulnerabilities and exposures to the MITRE ATT&CK framework: A self-distillation approach," *arXiv preprint arXiv:2108.01696*, 2021.

[31] S. Hong, K. Kim, and T. Kim, "The design and implementation of simulated threat generator based on MITRE ATT&CK for cyber warfare training," *Journal of the Korea Institute of Military Science and Technology*, vol. 22, no. 6, pp. 797–805, 2019.

[32] A. Kuppa, L. Aouad, and N.-A. Le-Khac, "Linking CVE's to MITRE ATT&CK techniques," in *The 16th International Conference on Availability, Reliability and Security*, 2021, pp. 1–12.

[33] N. Munaiah, A. Rahman, J. Pelletier, L. Williams, and A. Meneely, "Characterizing attacker behavior in a cybersecurity penetration testing competition," in *2019 ACM/IEEE International Symposium on Empirical Software Engineering and Measurement (ESEM)*. IEEE, 2019, pp. 1–6.

[34] A. V. Outkin, P. V. Schulz, T. Schulz, T. D. Tarman, and A. Pinar, "Defender policy evaluation and resource allocation using MITRE ATT&CK evaluations data," *arXiv preprint arXiv:2107.04075*, 2021.

[35] R. Pell, S. Moschoyiannis, E. Panaousis, and R. Heartfield, "Towards dynamic threat modelling in 5g core networks based on MITRE att&ck," *arXiv preprint arXiv:2108.11206*, 2021.

[36] W. Xiong, E. Legrand, O. Åberg, and R. Lagerström, "Cyber security threat modeling based on the MITRE enterprise ATT&CK matrix," *Software and Systems Modeling*, pp. 1–21, 2021.

[37] E. Hemberg, J. Kelly, M. Shlapentokh-Rothman, B. Reinstadler, K. Xu, N. Rutar, and U.-M. O'Reilly, "Linking threat tactics, techniques, and patterns with defensive weaknesses, vulnerabilities and affected platform configurations for cyber hunting," *arXiv preprint arXiv:2010.00533*, 2020.

[38] K. Kim, F. A. Alfouzan, and H. Kim, "Cyber-attack scoring model based on the offensive cybersecurity framework," *Applied Sciences*, vol. 11, no. 16, p. 7738, 2021.

[39] S. Choi, J.-H. Yun, and B.-G. Min, "Probabilistic attack sequence generation and execution based on MITRE ATT&CK for ics datasets," in *Cyber Security Experimentation and Test Workshop*, 2021, pp. 41–48.

[40] S. Arshad, M. Alam, S. Al-Kuwari, and M. H. A. Khan, "Attack specification language: Domain specific language for dynamic training in cyber range," in *2021 IEEE Global Engineering Education Conference (EDUCON)*. IEEE, 2021, pp. 873–879.

[41] A. P. Golushko and V. G. Zhukov, "Application of advanced persistent threat actorstechniques aor evaluating defensive countermeasures," in *2020 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus)*. IEEE, 2020, pp. 312–317.

[42] S. Kriaa and Y. Chaabane, "SecKG: Leveraging attack detection and prediction using knowledge graphs," in *2021 12th International Conference on Information and Communication Systems (ICICS)*. IEEE, 2021, pp. 112–119.

[43] R. Kwon, T. Ashley, J. Castleberry, P. Mckenzie, and S. N. G. Gourisetti, "Cyber threat dictionary using MITRE ATT&CK matrix and NIST cybersecurity framework mapping," in *2020 Resilience Week (RWS)*. IEEE, 2020, pp. 106–112.

[44] S. Bromander, M. Swimmer, M. Eian, G. Skjotskift, and F. Borg, "Modeling cyber threat intelligence." in *ICISSP*, 2020, pp. 273–280.

[45] V. Legoy, M. Caselli, C. Seifert, and A. Peter, "Automated retrieval of ATT&CK tactics and techniques for cyber threat reports," *arXiv preprint arXiv:2004.14322*, 2020.

[46] J. Fairbanks, A. Orbe, C. Patterson, E. Serra, and M. Scheepers, "Att&ck tactics in android malware control flow graph through graph representation learning and interpretability." in *Proceedings of the 2021 IEEE International Conference on Big Data (REU 2021 Symposium)*, 2021.

[47] Y.-T. Huang, C. Y. Lin, Y.-R. Guo, K.-C. Lo, Y. S. Sun, and M. C. Chen, "Open source intelligence for malicious behavior discovery and interpretation," *IEEE Transactions on Dependable and Secure Computing*, 2021.

[48] K. Kurniawan, A. Ekelhart, and E. Kiesling, "An att&ck-kg for linking cybersecurity attacks to adversary tactics and techniques," 2021.

[49] Y. Lakhdhar and S. Rekhis, "Machine learning based approach for the automated mapping of discovered vulnerabilities to adversial tactics," in *2021 IEEE Security and Privacy Workshops (SPW)*. IEEE, 2021, pp. 309–317.

[50] G. Lee, S. Shim, B. Cho, T. Kim, and K. Kim, "Fileless cyberattacks: Analysis and classification," *ETRI Journal*, vol. 43, no. 2, pp. 332–343, 2021.

[51] O. Mendsaikhan, H. Hasegawa, Y. Yamaguchi, and H. Shimada, "Automatic mapping of vulnerability information to adversary techniques," in *The Fourteenth International Conference on Emerging Security Information, Systems and Technologies SECUREWARE2020*, 2020.

[52] M. D. Purba, B. Chu, and E. Al-Shaer, "From word embedding to cyber-phrase embedding: Comparison of processing cybersecurity texts," in *2020 IEEE International Conference on Intelligence and Security Informatics (ISI)*. IEEE, 2020, pp. 1–6.

[53] E. Aghaei and E. Al-Shaer, "Threatzoom: neural network for automated vulnerability mitigation," in *Proceedings of the 6th Annual Symposium on Hot Topics in the Science of Security*, 2019, pp. 1–3.

[54] A. B. Ajmal, M. A. Shah, C. Maple, M. N. Asghar, and S. U. Islam, "Offensive security: Towards proactive threat hunting via adversary emulation," *IEEE Access*, vol. 9, pp. 126 023–126 033, 2021.

[55] A. Brazhuk, "Towards automation of threat modeling based on a semantic model of attack patterns and weaknesses," *arXiv preprint arXiv:2112.04231*, 2021.

[56] A. Elitzur, R. Puzis, and P. Zilberman, "Attack hypothesis generation," in *2019 European Intelligence and Security Informatics Conference (EISIC)*. IEEE, 2019, pp. 40–47.

[57] J. Fairbanks, A. Orbe, C. Patterson, J. Layne, E. Serra, and M. Scheepers, "Identifying ATT&CK tactics in android malware control flow graph through graph representation learning and interpretability," in *2021 IEEE International Conference on Big Data (Big Data)*. IEEE, 2021, pp. 5602–5608.

[58] L. Franklin, M. Pirrung, L. Blaha, M. Dowling, and M. Feng, "Toward a visualization-supported workflow for cyber alert management using threat models and human-centered design," in *2017 IEEE Symposium on Visualization for Cyber Security (VizSec)*. IEEE, 2017, pp. 1–8.

[59] S. N. G. Gourisetti, M. Mylrea, T. Ashley, R. Kwon, J. Castleberry, Q. Wright-Mockler, P. McKenzie, and G. Brege, "Demonstration of the cybersecurity framework through real-world cyber attack," in *2019 Resilience Week (RWS)*, vol. 1. IEEE, 2019, pp. 19–25.

[60] A. Gylling, M. Ekstedt, Z. Afzal, and P. Eliasson, "Mapping cyber threat intelligence to probabilistic attack graphs," in *2021 IEEE International Conference on Cyber Security and Resilience (CSR)*. IEEE, 2021, pp. 304–311.

[61] S. Hacks, I. Butun, R. Lagerström, A. Buhaiu, A. Georgiadou, and A. Michalitsi Psarrou, "Integrating security behavior into attack simulations," in *The 16th International Conference on Availability, Reliability and Security*, 2021, pp. 1–13.

[62] S. Hacks, L. Persson, and N. Hersén, "Measuring and achieving test coverage of attack simulations extended version," *Software and Systems Modeling*, pp. 1–16, 2022.

[63] A. Hassanzadeh and R. Burkett, "SAMIIT: Spiral attack model in IIoT mapping security alerts to attack life cycle phases," in *5th International Symposium for ICS & SCADA Cyber Security Research 2018 5*, 2018, pp. 11–20.

[64] M. Ahmed, S. Panda, C. Xenakis, and E. Panaousis, "MITRE ATT&CK-driven cyber risk assessment," in *Proceedings of the 17th International Conference on Availability, Reliability and Security*, 2022, pp. 1–10.

[65] V. Bolbot, S. Basnet, H. Zhao, O. V. Banda, and B. Silverajan, "Investigating a novel approach for cybersecurity risk analysis with application to remote pilotage operations," in *European Workshop on Maritime Systems Resilience and Security*, 2022.

[66] A. Oruc, A. Amro, and V. Gkioulos, "Assessing cyber risks of an INS using the MITRE ATT&CK framework," *Sensors*, vol. 22, no. 22, p. 8745, 2022.

[67] T. OConnor, "Helo darkside: Breaking free from katas and embracing the adversarial mindset in cybersecurity education," in *Proceedings of the 53rd ACM Technical Symposium on Computer Science Education V. 1*, 2022, pp. 710–716.

[68] D. Kim, Y. Kim, M.-K. Ahn, and H. Lee, "Automated cyber threat emulation based on ATT&CK for cyber security training," *Journal of the Korea Society of Computer and Information*, vol. 25, no. 9, pp. 71–80, 2020.

[69] S. P. Rao, H.-Y. Chen, and T. Aura, "Threat modeling framework for mobile communication systems," *Computers & Security*, vol. 125, p. 103047, 2023.

[70] C. K. Chen, S. C. Lin, S. C. Huang, Y. T. Chu, C. L. Lei, and C. Y. Huang, "Building machine learning-based threat hunting system from scratch," *Digital Threats: Research and Practice*, 2022.

[71] C. Adam, M. F. Bulut, D. Sow, S. Ocepek, C. Bedell, and L. Ngweta, "Attack techniques and threat identification for vulnerabilities," *arXiv preprint arXiv:2206.11171*, 2022.

[72] L. Sadlek, P. Čeleda, and D. Tovarňák, "Identification of attack paths using kill chain and attack graphs," in *2022-2022 IEEE/IFIP Network Operations and Management Symposium (NOMS)*. IEEE, 2022, pp. 1–6.

[73] Z. Jadidi and Y. Lu, "A threat hunting framework for industrial control systems," *IEEE Access*, vol. 9, pp. 164 118–164 130, 2021.

[74] M. Mundt and H. Baier, "Towards mitigation of data exfiltration techniques using the MITRE ATT&CK framework," in *International Conference on Digital Forensics and Cyber Crime*. Springer, 2022, pp. 139–158.

[75] A. Niakanlahiji, J. Wei, and B.-T. Chu, "A natural language processing based trend analysis of advanced persistent threat techniques," in *2018 IEEE International Conference on Big Data (Big Data)*. IEEE, 2018, pp. 2995–3000.

[76] G. Ayoade, S. Chandra, L. Khan, K. Hamlen, and B. Thuraisingham, "Automated threat report classification over multi-source data," in *2018 IEEE 4th International Conference on Collaboration and Internet Computing (CIC)*. IEEE, 2018, pp. 236–245.

[77] P. Karuna, E. Hemberg, U. M. O'Reilly, and N. Rutar, "Automating cyber threat hunting using NLP, automated query generation, and genetic perturbation," *arXiv preprint arXiv:2104.11576*, 2021.

[78] Y. Shin, K. Kim, J. J. Lee, and K. Lee, "Art: Automated reclassification for threat actors based on ATT&CK matrix similarity," in *2021 World Automation Congress (WAC)*. IEEE, 2021, pp. 15–20.

[79] T. He and Z. Li, "A model and method of information system security risk assessment based on MITRE ATT&CK," in *2021 2nd International Conference on Electronics, Communications and Information Technology (CECIT)*. IEEE, 2021, pp. 81–86.

[80] P. Johnson, R. Lagerström, and M. Ekstedt, "A meta language for threat modeling and attack simulations," in *Proceedings of the 13th International Conference on Availability, Reliability and Security*, 2018, pp. 1–8.

[81] H. Manocha, A. Srivastava, C. Verma, R. Gupta, and B. Bansal, "Security assessment rating framework for enterprises using MITRE ATT&CK matrix," *arXiv preprint arXiv:2108.06559*, 2021.

[82] D. Mashima, "MITRE ATT&CK based evaluation on in-network deception technology for modernized electrical substation systems," *Sustainability*, vol. 14, no. 3, p. 1256, 2022.

[83] L. L. Dhirani, E. Armstrong, and T. Newe, "Industrial iot, cyber threats, and standards landscape: evaluation and roadmap," *Sensors*, vol. 21, no. 11, p. 3901, 2021.

[84] R. Luh, S. Eresheim, S. Größbacher, T. Petelin, F. Mayr, P. Tavolato, and S. Schrittwieser, "PenQuest reloaded: A digital cyber defense game for technical education," in *2022 IEEE Global Engineering Education Conference (EDUCON)*. IEEE, 2022, pp. 906–914.

[85] G. Husari, E. Al-Shaer, B. Chu, and R. F. Rahman, "Learning APT chains from cyber threat intelligence," in *Proceedings of the 6th Annual Symposium on Hot Topics in the Science of Security*, 2019, pp. 1–2.

[86] A. Nisioti, G. Loukas, S. Rass, and E. Panaousis, "Game-theoretic decision support for cyber forensic investigations," *Sensors*, vol. 21, no. 16, p. 5300, 2021.

[87] J. Halvorsen, J. Waite, and A. Hahn, "Evaluating the observability of network security monitoring strategies with TOMATO," *IEEE Access*, vol. 7, pp. 108 304–108 315, 2019.

[88] A. Y. Wong, E. G. Chekole, M. Ochoa, and J. Zhou, "Threat modeling and security analysis of containers: A survey," *arXiv preprint arXiv:2111.11475*, 2021.

[89] N. Dhir, H. Hoeltgebaum, N. Adams, M. Briers, A. Burke, and P. Jones, "Prospective artificial intelligence approaches for active cyber defence," *arXiv preprint arXiv:2104.09981*, 2021.

[90] E. Holder and N. Wang, "Explainable artificial intelligence (XAI) interactively working with humans as a junior cyber analyst," *Human-Intelligent Systems Integration*, vol. 3, no. 2, pp. 139–153, 2021.

[91] G. Ahn, K. Kim, W. Park, and D. Shin, "Malicious file detection method using machine learning and interworking with MITRE ATT&CK framework," *Applied Sciences*, vol. 12, no. 21, p. 10761, 2022.

[92] R. Stoleriu, A. Puncioiu, and I. Bica, "Cyber attacks detection using open source ELK stack," in *2021 13th International Conference on Electronics, Computers and Artificial Intelligence (ECAI)*. IEEE, 2021, pp. 1–6.

[93] S. Bagui, D. Mink, S. Bagui, T. Ghosh, T. McElroy, E. Paredes, N. Khasnavis, and R. Plenkers, "Detecting reconnaissance and discovery tactics from the MITRE ATT&CK framework in Zeek Conn Logs using Spark's machine learning in the big data framework," *Sensors*, vol. 22, no. 20, p. 7999, 2022.

[94] S. Zurowski, G. Lord, and I. Baggili, "A quantitative analysis of offensive cyber operation (OCO) automation tools," in *Proceedings of the 17th International Conference on Availability, Reliability and Security*, 2022, pp. 1–11.

[95] R. Alnafrani and D. Wijesekera, "AIFIS: Artificial intelligence (AI)-based forensic investigative system," in *2022 10th International Symposium on Digital Forensics and Security (ISDFS)*. IEEE, 2022, pp. 1–6.

[96] S. Samtani, H. Chen, M. Kantarcioglu, and B. Thuraisingham, "Explainable artificial intelligence for cyber threat intelligence (XAI-CTI)," *IEEE Transactions on Dependable and Secure Computing*, vol. 19, no. 04, pp. 2149–2150, 2022.

[97] O. Grigorescu, A. Nica, M. Dascalu, and R. Rughinis, "CVE2ATT&CK: BERT-based mapping of CVEs to MITRE ATT&CK techniques," *Algorithms*, vol. 15, no. 9, p. 314, 2022.

[98] K. Hasan, S. Shetty, and S. Ullah, "Artificial intelligence empowered cyber threat detection and protection for power utilities," in *2019 IEEE 5th International Conference on Collaboration and Internet Computing (CIC)*. IEEE, 2019, pp. 354–359.

[99] F. Maymí, R. Bixler, R. Jones, and S. Lathrop, "Towards a definition of cyberspace tactics, techniques and procedures," in *2017 IEEE International Conference on Big Data (Big Data)*. IEEE, 2017, pp. 4674–4679.

[100] M. Drašar, S. Moskal, S. Yang, and P. Zat'ko, "Session-level adversary intent-driven cyberattack simulator," in *2020 IEEE/ACM 24th International Symposium on Distributed Simulation and Real Time Applications (DS-RT)*. IEEE, 2020, pp. 1–9.

[101] H. Kim, H. Kim *et al.*, "Comparative experiment on TTP classification with class imbalance using oversampling from CTI dataset," *Security and Communication Networks*, vol. 2022, 2022.

[102] K. Kim, Y. Shin, J. Lee, and K. Lee, "Automatically attributing mobile threat actors by vectorized ATT&CK matrix and paired indicator," *Sensors*, vol. 21, no. 19, p. 6522, 2021.

[103] I. K. Sahu and M. J. Nene, "Model for IaaS security model: MISP framework," in *2021 International Conference on Intelligent Technologies (CONIT)*. IEEE, 2021, pp. 1–6.

[104] T. Zhao, T. E. Gasiba, U. Lechner, and M. Pinto-Albuquerque, "Exploring a board game to improve cloud security training in industry (short paper)," in *Second International Computer Programming Education Conference (ICPEC 2021)*. Schloss Dagstuhl-Leibniz-Zentrum für Informatik, 2021.

[105] T. Zhao, U. Lechner, M. Pinto-Albuquerque, and E. Ata, "Cloud of assets and threats: A playful method to raise awareness for cloud security in industry," *OpenAccess Series in Informatics*, 2022.

[106] G. van der Merwe, C. Muller, W. van der Merwe, and D. Blaauw, "Identifying adversaries' signatures using knowledge representations of cyberattack techniques on cloud infrastructure," in *International Conference on Cyber Warfare and Security*, vol. 17, no. 1, 2022, pp. 333–339.

[107] S. Zhang, P. Chen, G. Bai, S. Wang, M. Zhang, S. Li, and C. Zhao, "An automatic assessment method of cyber threat intelligence combined with ATT&CK matrix," *Wireless Communications and Mobile Computing*, vol. 2022, 2022.

[108] M. Odemis, C. Yucel, and A. Koltuksuz, "Detecting user behavior in cyber threat intelligence: development of Honeypsy system," *Security and Communication Networks*, vol. 2022, 2022.

[109] Y. Jo, O. Choi, J. You, Y. Cha, and D. H. Lee, "Cyberattack models for ship equipment based on the MITRE ATT&CK framework," *Sensors*, vol. 22, no. 5, p. 1860, 2022.

[110] R. C. D. Centre, "DeTTECT," https://github.com/rabobank-cdc/DeTTECT, 2022, (Accessed on 16/12/2022).

[111] "DeTT&CT: Mapping detection to MITRE ATT&CK," NVISO Labs, https://blog.nviso.eu/2022/03/09/dettct-mapping-detection-to-mitre-attck/, March 2022, (Accessed on 09/21/2022).

[112] A. Roberts, "Structured intelligence–what does it even mean?" in *Cyber Threat Intelligence*. Springer, 2021, pp. 37–64.

[113] H. M. Farooq and N. M. Otaibi, "Optimal machine learning algorithms for cyber threat detection," in *2018 UKSim-AMSS 20th International Conference on Computer Modelling and Simulation (UKSim)*. IEEE, 2018, pp. 32–37.

[114] A. R. Sharma, "How MITRE ATT&CK alignment supercharges your SIEM," Securonix, https://www.securonix.com/blog/how-mitre-attck-alignment-supercharges-your-siem, (Accessed on 10/19/2022).

[115] K. Sadrazamis, "MITRE ATT&CK-based analysis of cyber-attacks in intelligent transportation," 2022.

[116] A. Amro, V. Gkioulos, and S. Katsikas, "Assessing cyber risk in cyber-physical systems using the att&ck framework," *ACM Transactions on Privacy and Security*, vol. 26, no. 2, pp. 1–33, 2023.

[117] H. I. Kure, S. Islam, and H. Mouratidis, "An integrated cyber security risk management framework and risk predication for the critical infrastructure protection," *Neural Computing and Applications*, pp. 1–31, 2022.

[118] TLP.White, "Risk and vulnerability assessment (RVA) mapped to the MITRE ATT&CK framework infographic," https://www.cisa.gov/sites/default/files/publications/FY19_RVAs_Mapped_to_the_MITRE_ATTCK_Framework_508.pdf, (Accessed on 11/06/2022).

[119] ——, "RVAs mapped to the MITRE ATT&CK framework," https://irp.cdn-website.com/9a5fc83f/files/uploaded/FY20_RVAs_Mapped_to_the_MITRE_ATTCK_Framework_508_QVzrjj9OT2e6JWUkrOAu.pdf, (Accessed on 11/06/2022).

[120] GRANTEK, "RVAs mapped to the MITRE ATT&CK framework," https://grantek.com/wp-content/uploads/2020/04/2020CybersecurityWP.pdf, April 2020.

[121] AttackIQ, "The CISO's guide to better vulnerability management using MITRE ATT&CK," https://www.attackiq.com/wp-content/uploads/2021/12/90398r72vt8w.pdf, December 2021.

[122] W. Xiong, E. Legrand, O. Åberg, and R. Lagerström, "Cyber security threat modeling based on the MITRE Enterprise ATT&CK matrix," *Software and Systems Modeling*, vol. 21, no. 1, pp. 157–177, 2022.

[123] A. V. Outkin, P. V. Schulz, T. Schulz, T. D. Tarman, and A. Pinar, "Defender policy evaluation and resource allocation with MITRE ATT&CK evaluations data," *IEEE Transactions on Dependable and Secure Computing*, 2022.

[124] H. Y. Chen and S. P. Rao, "On adoptability and use case exploration of threat modeling for mobile communication systems," in *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security*, 2021, pp. 2417–2419.

[125] MITRE Corporation, "FiGHT (5G hierarchy of threats)," https://fight.mitre.org, 2022, (Online; accessed 16-December-2022).

[126] ——, "MITRE ATT&CK," https://attack.mitre.org, 2015-2022, (Online; accessed 16-December-2022).

[127] M. S. Barnum, "Common attack pattern enumeration and classification (capec) schema," *Department of Homeland Security*, 2008.

[128] MITRE Corporation, "Common Weakness Enumeration," https://cwe.mitre.org, 2022, (Accessed on 16/12/2022).

[129] N. Naik, P. Jenkins, P. Grace, and J. Song, "Comparing attack models for it systems: Lockheed martin's cyber kill chain, mitre att&ck framework and diamond model," in *2022 IEEE International Symposium on Systems Engineering (ISSE)*. IEEE, 2022, pp. 1–7.

[130] J. Straub, "Modeling attack, defense and threat trees and the cyber kill chain, att&ck and stride frameworks as blackboard architecture networks," in *2020 IEEE International Conference on Smart Cloud (SmartCloud)*. IEEE, 2020, pp. 148–153.

[131] T. C. for Threat-Informed Defense, "Security stack mappings," https://github.com/center-for-threat-informed-defense/security-stack-mappings, 2022, (Accessed on 16/12/2022).

[132] S. Barnum, "Standardizing cyber threat intelligence information with the structured threat information expression (STIX)," *MITRE Corporation*, vol. 11, pp. 1–22, 2012.

[133] R. Stillions, "The DML model," http://ryanstillions.blogspot.com/2014/04/the-dml-model_21.html, (Accessed on 10/05/2022).

[134] S. Caltagirone, A. Pendergast, and C. Betz, "The diamond model of intrusion analysis," Center For Cyber Intelligence Analysis and Threat Research, Hanover, MD, Tech. Rep., 2013.

[135] F. Cybersecurity, "Facility cybersecurity framework," https://facilitycyber.labworks.org, 2022, (Accessed on 16/12/2022).

[136] K. A. Akbar, S. M. Halim, Y. Hu, A. Singhal, L. Khan, and B. Thuraisingham, "Knowledge mining in cybersecurity: From attack to defense," in *IFIP Annual Conference on Data and Applications Security and Privacy*. Springer, 2022, pp. 110–122.

[137] "D3fend matrix — MITRE d3fend™," https://d3fend.mitre.org/, (Accessed on 07/21/2022).

[138] A. Wolf, D. Simopoulos, L. D'Avino, and P. Schwaiger, "The pasta threat model implementation in the iot development life cycle," *INFORMATIK 2020*, 2021.

[139] F. Mottini, "Osquery-ATT&CK," https://github.com/teoseller/osquery-attck, 2022, (Accessed on 16/12/2022).

[140] Osquery, "Osquery," https://github.com/osquery/osquery, 2022, (Accessed on 16/12/2022).

[141] "osquery: Easily ask questions about your Linux, Windows, and macOS infrastructure," https://osquery.io/, (Accessed on 09/21/2022).

[142] MITRE Corporation, "MITRE ATT&CK navigator," https://mitre-attack.github.io/attack-navigator/, 2021, (Accessed on 16/12/2022).

[143] Red Canary, "Atomic red team," https://github.com/redcanaryco/atomic-red-team, 2019, [Online; accessed 16-December-2022].

[144] E. Hemberg and U.-M. O'Reilly, "Using a collated cybersecurity dataset for machine learning and artificial intelligence," *arXiv preprint arXiv:2108.02618*, 2021.

[145] C. Liu, J. Wang, and X. Chen, "Threat intelligence ATT&CK extraction based on the attention transformer hierarchical recurrent neural network," *Applied Soft Computing*, vol. 122, p. 108826, 2022.

[146] M. Otgonpurev, "Effective application of natural language processing techniques in automated cyber threat intelligence," 2021.

[147] E. Domschot, "Automated labeling of MITRE ATT&CK tactics and techniques in malware threat reports," Ph.D. dissertation, New Mexico Institute of Mining and Technology, 2022.

[148] L. Evensjö, "Probability analysis and financial model development of MITRE ATT&CK enterprise matrix's attack steps and mitigations," 2020.

[149] MITRE Corporation, "Caldera," https://github.com/mitre/caldera, 2022, (Accessed on 16/12/2022).

[150] Endgame, "Red team automation," https://github.com/endgameinc/RTA, 2022, (Accessed on 16/12/2022).

[151] U. Common, "Metta," https://github.com/uber-common/metta, 2018, [Online; accessed 16-December-2022].

[152] Praetorian, "Purple team ATT&CK™ automation," https://github.com/praetorian-inc/purple-team-attack-automation, 2020, (Online; accessed 16-December-2022).

[153] Rapid7, "The Metasploit Framework," https://github.com/rapid7/metasploit-framework, 2020, (Accessed on 16/12/2022).

[154] J. Dreijer, "RE:TERNAL," https://github.com/d3vzer0/reternal-quickstart, 2020, (Accessed on 16/12/2022).

[155] 3CORESec, "S2AN," https://github.com/3CORESec/S2AN, 2021, [Online; accessed 16-December-2022].

[156] SigmaHQ, "Sigma," https://github.com/SigmaHQ/sigma, 2022, (Accessed on 16/12/2022).

[157] O. T. R. Forge, "Security Datasets," https://github.com/OTRF/Security-Datasets, 2022, (Accessed on 16/12/2022).

[158] J. Freund and J. Jones, *Measuring and managing information risk: a FAIR approach*. Butterworth-Heinemann, 2014.