applied sciences

MDPI

Article

Analysis of Cyber-Intelligence Frameworks for AI Data Processing

Alberto Sánchez del Monte [1] and Luis Hernández-Álvarez [2,*]

[1] Doctoral School "Studii Salamantini", Computer Engineering, University of Salamanca, 37008 Salamanca, Spain; idu030355@usal.es
[2] Institute for Physical and Information Technologies (ITEFI), Spanish National Research Council (CSIC), 28006 Madrid, Spain
* Correspondence: luis.hernandez@csic.es

Abstract: This paper deals with the concept of cyber intelligence and its components as a fundamental tool for the protection of information today. After that, the main cyber-intelligence frameworks that are currently applied worldwide (Diamond Model, Cyberkill Chain, and Mitre Att&ck) are described to subsequently analyse them through their practical application in a real critical cyber incident, as well as analyse the strengths and weaknesses of each one of them according to the comparison of seventeen variables of interest. From this analysis and considering the two actions mentioned, it is concluded that Mitre Att&ck is the most suitable framework due to its flexibility, permanent updating, and the existence of a powerful database. Finally, an explanation is given for how Mitre Att&ck can be integrated with the research and application of artificial intelligence in the achievement of the objectives set and the development of tools that can serve as support for the detection of the patterns and authorship of cyberattacks.

Keywords: artificial intelligence; Cyberkill Chain; cyber intelligence; Diamond Model; indicators of compromise; machine learning; Mitre Att&ck; tactics; techniques and procedures

Citation: Sánchez del Monte, A.; Hernández-Álvarez, L. Analysis of Cyber-Intelligence Frameworks for AI Data Processing. *Appl. Sci.* **2023**, *13*, 9328. https://doi.org/10.3390/app13169328

Academic Editors: Huiyu (Joe) Zhou, Tao Jiang, Yuling Chen and Yilei Wang

Received: 28 June 2023
Revised: 7 August 2023
Accepted: 15 August 2023
Published: 17 August 2023

1. Introduction

Recent advances in cyber technologies (Internet of Things devices, cloud computing, mobile communication networks, etc.) have caused a paradigm shift in terms of services, business, and data management and transmission. All of these activities are migrating from the physical to the cyber-enabled world [1], where they are more accessible and their execution is more convenient for the general user. However, the security of our information in this cyber world (or cybersecurity) [2] should also be guaranteed, a task that is not always easy due to the complexity and sophistication of existing cyberattacks [3].

Cyber intelligence, that is, the technologies to acquire and analyse information to identify, track, and predict cyber capabilities, intentions, and activities to offer courses of action that enhance decision making [4], has become an indispensable branch of cybersecurity. The growing inability to mount an adequate response to attacks on information systems or operations has progressively directed the efforts of organisations towards the application of effective preventive measures that make it possible to avoid these attacks, or at least reduce them. This is conducted by implementing preparatory actions that increase resilience in the event of a cyberattack, resulting in a considerable increase in the importance of cyber intelligence in recent years [5]. Frameworks [6] of cyber intelligence can be characterised as schemes that allow for building and organising work more efficiently by providing common concepts, libraries, entities, and design patterns. In this sense, there are currently different frameworks that allow the structuring of information and its transformation into intelligence through a generally cyclical process. The aim of this work is to study the most relevant cyber-intelligence frameworks (specifically, Diamond Model, Cyberkill Chain, and Mitre Att&ck) using a real cyberattack example in order to determine the most suitable one for its combination with artificial intelligence (AI) tools. The final goal of this combination

is to successfully process and analyse large-scale information regarding cyberattacks, where information, in this context, is defined as in the International Organization of Standards (ISO) publication ISO/IEC 27000:2018: *"any communication or representation of knowledge such as facts, data, events, things, processes, ideas, concepts, or opinions in any medium or form, including textual, numeral, graphic, cartographic, narrative, or audiovisual that, within a certain context, has a particular meaning"* [7,8]. This would allow for automating and exploiting the generated intelligence, allowing better protection of organisations and the detection of behavioural patterns to infer the actions of attackers or guide Law Enforcement Agencies in their fight against cybercrime. To the authors' knowledge, this is the first work that studies the three aforementioned frameworks by comparing them in a real application. In this sense, the novelties presented in this study are:

- The provision of a detailed explanation and the current status of the state of the art of the three most relevant cyber-intelligence frameworks: Diamond Model, Cyberkill Chain, and Mitre Att&ck.
- A case study of a real cyberattack for the three mentioned frameworks, emphasising the strengths, weaknesses, and best perspective offered by each one of them.
- The definition of seventeen variables of interest in order to compare, among other characteristics, the efficacy, adaptability, and simplicity of the frameworks.
- An analysis, based on these seventeen characteristics, of the most appropriate framework to combine with AI methods and, more specifically, machine-learning models. With this analysis, we also conclude the suitability of each framework depending on the specific situation and knowledge of interest.

The rest of this article is structured as follows: Section 2 discusses the concept and discipline of cyber intelligence, while Section 3 includes the current literature status regarding cyber-intelligence frameworks. Then, Section 4 applies the models to a specific case study of a real attack. The results obtained are analysed and discussed in Section 5. Finally, in Section 6, the conclusions are derived, and future works related to the subject under study are proposed.

2. Background of Cyber Intelligence

2.1. Concept and Characteristics

The classic concept of intelligence is related to the quality of the mind that allows us to assimilate, understand, reason, make decisions, and form a vision or idea of a specific reality [9]. In relation to this, in the context of security, intelligence can be understood as "*The product of the collection, evaluation, analysis, integration and interpretation of all available information that is immediately or potentially significant to planning and operations*" [10]. Applying this definition to the domain of cyberspace approximates the concept of cyber intelligence, a term with increasing presence and relevance in today's society in the face of exponential criminal growth, which requires reactive but especially preventive responses. Cyber intelligence is therefore an eminently proactive discipline that uses various branches of information security to achieve its objectives (vulnerability management, threat management, incident response, etc.) [11]. This is achieved by developing products that support the decision-making process regarding the risks to which organisations are exposed. In this sense, [10] defines cyber intelligence as "*Intelligence activities in support of cybersecurity. Cyber threats are mapped, the intentions and opportunities of cyber adversaries are analysed in order to identify, locate and attribute sources of cyber-attacks*". This concept can therefore be grouped into three main branches of application in cybersecurity, which will be described later: *cyber threat intelligence*, *incident response*, and *vulnerability management*.

The data used to produce the intelligence must be evidence-based and meet minimum quality criteria. It must be useful to the organisation based on its characteristics and Priority Information Requirements (PRIs) [11]. In addition, the data must be processable and manageable, a basic characteristic for processing them using machine-learning techniques [12]. Of particular interest in cyberspace is the concept of OSINT (Open-Source Intelligence Techniques) [13], which allows the management of existing data from all kinds of open

sources to be processed for intelligence purposes. In order to be able to structure and process this information and, in particular, to represent it in a visual and user-friendly way, a large number of cyber-intelligence platforms have been developed in recent years that collect intelligence from various information *feeds*, generating exchanges mainly through the use of STIX [14] or TAXII [15] standards.

2.2. Levels and Typologies

The diverse typologies of recipients and target audiences present in the management of cyber intelligence make it necessary to establish a stratification or distinction; thus, three levels can be observed [16]:

- The strategic level is focused on supporting decision making on the policies and objectives of an organisation. In this sense, the knowledge, study, and possible evolution of the malicious actors involved that can influence the organisation's risks are essential. An example is the analysis of the organisation's exposure to the main groups that exploit ransomware-type malware or carry out Advanced Persistent Threat (APT) actions.
- The tactical level is aimed at supporting the planning of specific actions that enable the achievement of the organisation's strategic objectives, for example, the analysis of the attack Tactics, Techniques, and Procedures (TTPs) of a given malicious actor.
- The operational level refers to the knowledge that allows decisions to be taken in a short space of time in the framework of the actions necessary to prevent a given attack or incident, e.g., the analysis of indicators of compromise (IOCs) that represent a threat to the organisation.

Handling the data traditionally associated with operational intelligence, i.e., indicators of compromise (hashes, domains, IPs, etc.) reflected in the lower rungs of David Bianco's (2013) [17] panic pyramid (see Figure 1), is extremely complex due to the sheer variety, ease of substitution, and poor correlation between them. On the other hand, the data associated with strategic intelligence are sometimes diffuse, not easily processed, and very difficult to obtain in a structured way. Therefore, this research focuses on the development of tactical intelligence products through the extensive study of TTPs.

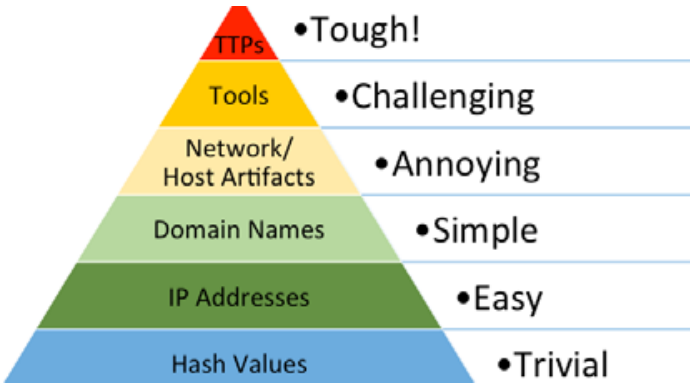

Figure 1. Panic pyramid [17].

On the other hand, three branches or typologies of cybersecurity have been identified as those where cyber intelligence has the greatest utility and application: cyber threat intelligence, incident response, and vulnerability management.

Threat intelligence or cyber threat intelligence (CTI) is focused on making decisions about the policies and objectives of an organisation in terms of information security or operation. To this end, it tries to collect and analyse all types of data to address the organisation's risks for the protection of its technological assets with three clear objectives: that the intelligence is relevant, that it is accurate, and that it is adjusted over time to needs. In this sense, it seems appropriate to adopt a cyclical model similar to that of classic military intelligence, widely discussed and studied in recent decades, whereby products

are produced through a recurring process and updated according to the reality present in each time period [9]. For the proper implementation of this cycle, smooth cooperation between the different actors involved is essential.

- Phase 1. Planning and management. In this phase, the RPIs are identified based on the prior definition of critical assets and relevant threats whose exploitation generates an impact.
- Phase 2. Collection. Data collection is carried out following structured methods based on the requirements of the previous phase.
- Phase 3. Processing. The collected data are processed with appropriate techniques.
- Phase 4. Analysis and production. This is a critical phase of the cycle in which the information obtained in previous phases is transformed into intelligence. Today, it requires the presence of the human factor.
- Phase 5. Dissemination. This is the stage in which the intelligence is provided to decision-makers so that they have the appropriate knowledge.
- Phase 6. Utilisation. Decision making based on the delivered product is considered another critical and decisive moment in the cycle.

The incident response (IR) branch is focused on the integral response to incidents detected in the organisation. The application of intelligence to this branch is based on the proposal in [18].

- Phase 1. Preparedness. This phase consists of establishing and forming an incident response team and acquiring the necessary tools and resources.
- Phase 2. Detection and analysis. The aim at this stage is to limit the number of incidents that will occur by selecting and implementing a set of controls based on the results of the risk assessments and, where appropriate, dealing with residual risks in the first instance.
- Phase 3. Containment, eradication, and recovery. Once it is known that an incident has been affected, the response actions are included in this phase in order to minimise the damage and try to facilitate business continuity in the shortest possible time.
- Phase 4. Post-incident activity. In this phase, the relevant reports are drawn up, and the incident is analysed ex post with a view to obtaining lessons learned and generating good practices.

The vulnerability management (VM) branch aims at the integral management of vulnerabilities in the organisation's infrastructure, where cyber intelligence plays a key role. For this purpose, it takes the approaches in [19,20] as a reference.

- Phase 1. Discovery. Take inventory of the assets to be protected in the organisation.
- Phase 2. Prioritisation. Analyse the risks associated with the commitment of each asset and its criticality for the provision of the service.
- Phase 3. Assessment. Determine a baseline risk profile to be acted upon.
- Phase 4. Information. Monitor assets and describe vulnerabilities.
- Phase 5. Remediation. Prioritise and remediate vulnerabilities according to the associated risk profile.
- Phase 6. Verification. Execute controls that verify that threats have been eliminated.

It would be of great interest to be able to apply AI techniques to each of the phases of the three branches. AI can identify patterns in large datasets to uncover emerging threats, improving the quality and speed of CTI. In addition, the accurate prediction of future vulnerabilities enables better vulnerability management and mitigation, strengthening the security posture. In relation to incident response, AI can speed up the process by automatically classifying incidents by severity and suggesting response actions, freeing human analysts to focus on critical tasks. Therefore, it is essential to find the most suitable cyber-intelligence framework for the application of AI algorithms.

3. Related Work: Cyber-Intelligence Frameworks

As we have mentioned before, there are currently three cyber-intelligence frameworks that stand out above the rest; they use different approaches, but all of them are very useful, as reflected in [21]. In this Section, we provide a description of their functioning and status in the state of the art.

3.1. Diamond Model

The Diamond Model is a framework proposed in [22] that seeks a comprehensive treatment of the analysis of an attack under a simple premise: *the study of an adversary developing capabilities on an infrastructure targeting a victim*. It is structured as a series of events that express the four key characteristics in the previous definition (adversary, capabilities, infrastructure, and victim) for each attack; these characteristics are closely related to each other and are configured as the vertices of a diamond-like rhombus (see Figure 2). In addition to the four key characteristics, meta-characteristics and trust values are defined, which make up the bulk of the model, as follows: key characteristics (adversary, capabilities, infrastructure, and victim); meta-characteristics (time stamp, phase, outcome, direction, methodology, and resources); and confidence values (each key characteristic or meta-characteristic will have a confidence estimate associated with it, representing the accuracy of the data source or the confidence in the conclusions drawn).

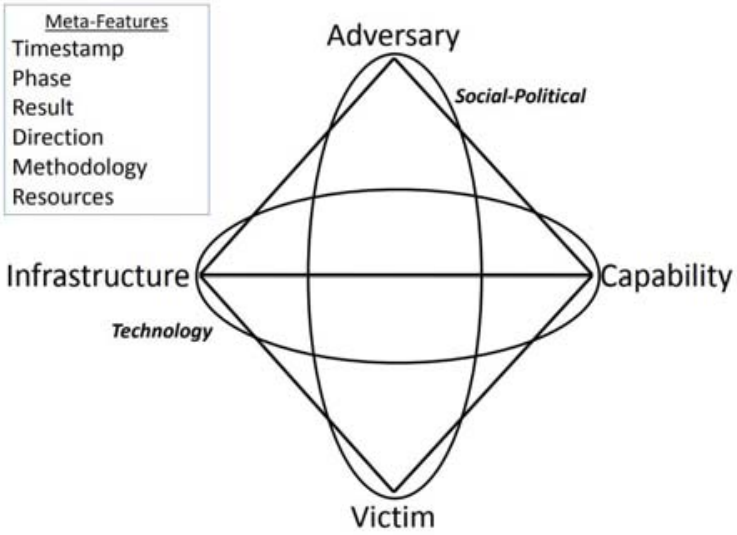

Figure 2. Diamond Model representation [22].

Referring to first-level parameters or key features, the adversary is the person or group of persons responsible for the exploitation of capacities. This parameter will generally be incomplete or even unknown in the early stages of the analysis. With the recent development of Crime as a Service (CaaS), the distinction between Operator and Customer becomes more apparent. Secondly, the capability includes the tools used by the adversary in the exploitation of the operation relating to (1) capacity/potential: vulnerabilities and areas of exposure it can employ in relation to the victim; (2) arsenal: the set of tools that the attacker can use, including command-and-control (C2) panels, understood not just as the simple technological infrastructure but as the channels, structures, and procedures that guide the operation of an attack. In third place, the infrastructure describes those physical or logical structures used for the deployment of the capabilities, being very variable in type and volume. It represents, for example, IP, domains, mail addresses, and physical devices. Specifically, and in line with what has been said about the proliferation of CaaS, it is defined as follows: Typology 1, which is fully controlled by attackers, and Typology 2, which is controlled by intermediaries or service providers (ISPs, domain registrars, etc.). Finally, the victim characteristic represents the target of the adversary against whom the capabilities

are directed. It can comprise organisations, individuals, email addresses, IP addresses, etc. In this sense, a distinction can be made between (1) victim-physical, meaning organisations or their employees, and (2) victim-asset, meaning the attack surface to be attacked.

On the other hand, there is a second level of parameters, meta-characteristics, which will not be detailed (they are not of interest for this application) but will be mentioned here: time stamp, phase, results, direction, methodology, and resources.

This model can be applied by looking at different perspectives based on the vertex that is taken as the main characteristic among the four (see Figure 2) or the axis of two existing ones that are taken as the most relevant, so the socio-political axis (adversary and victim) and the technological axis (infrastructure and capacity) are configured. This theoretical framework is very useful for the comprehensive analysis of cyberattacks, especially because of the ease with which it is possible to foresee the adversary's future movements. It allows the study of the aetiology of the action and the generation of hypotheses of authorship with a wide margin for the analyst. However, it is very difficult to gather information in a structured way, as it lacks its own taxonomy. This framework was applied in [23], where it was combined with machine-learning techniques (Bayesian Networks) to integrate alert correlation detection. Once an alert is generated, it automatically reconstructs the past threat scenarios and predicts future threats and vulnerabilities. Formally, and according to the authors, given a characteristic F and a confidence value σ, an event E can be represented as follows:

$$E = ((F_1, \sigma_1), (F_2, \sigma_2), (F_3, \sigma_3), \ldots (F_n, \sigma_n))$$

where n is the number of characteristics involved. A typical example might be the following: adversary, capability, victim, infrastructure, initial timestamp, final timestamp, phase, outcome, direction, methodology, and resources.

3.2. Cyberkill Chain

Focused mainly on APT attacks, this framework has had a strong impact on the field of cyber intelligence since its publication in 2010 [24]. It was developed by the US company *Lockheed Martin* and tries to represent a series of steps that an attacker must execute to reach his or her final objective based on the F2T2EA (Find, Fix, Track, Target, Engage, Assess) concept, a methodology of reference in the US military doctrine [25] (see Figure 3). Cyberkill Chain establishes seven steps, consisting of (1) Reconnaissance: getting to know the victim through noninvasive techniques; (2) Weaponisation: generating the malicious payload to be delivered; (3) Delivery: delivering the artefact developed or acquired in the previous step; (4) Exploitation: achieving code execution on the victim's system through the exploitation of a vulnerability or other means; (5) Installation: installing the final piece of malware; (6) Command and Control (C2): establishing a channel to communicate with the malware on the victim's system; and (7) Actions on Targets: achieving the goal of the attack, having gained full access and communication.

This chain is useful because it provides a structured and systematic approach to understanding and addressing cyberattacks from start to finish, making it easier to identify threats and implement strategies to defend against them. Its advantages include:

- Early warning or prevention, analysing potential weaknesses in the technological infrastructure at each stage of a potential attack before it can take place.
- Optimisation of resources, focusing investments and efforts on the most vulnerable stages in the infrastructure.
- Raising awareness of workers who do not have knowledge of cybersecurity, offering a graphic and consecutive structure that allows a better understanding of what a cyberattack is and the risks it generates in the organisation.

By applying the Cyberkill Chain, it is possible to analyse attack campaigns in order to see similarities and differences between the TTPs of different attackers and thus the presence of patterns that point to a specific malicious actor. Furthermore, by compartmentalising

actions, it is possible to observe, from a higher level, the possible targets towards which the ongoing actions are directed and to anticipate the possible success of an attack.

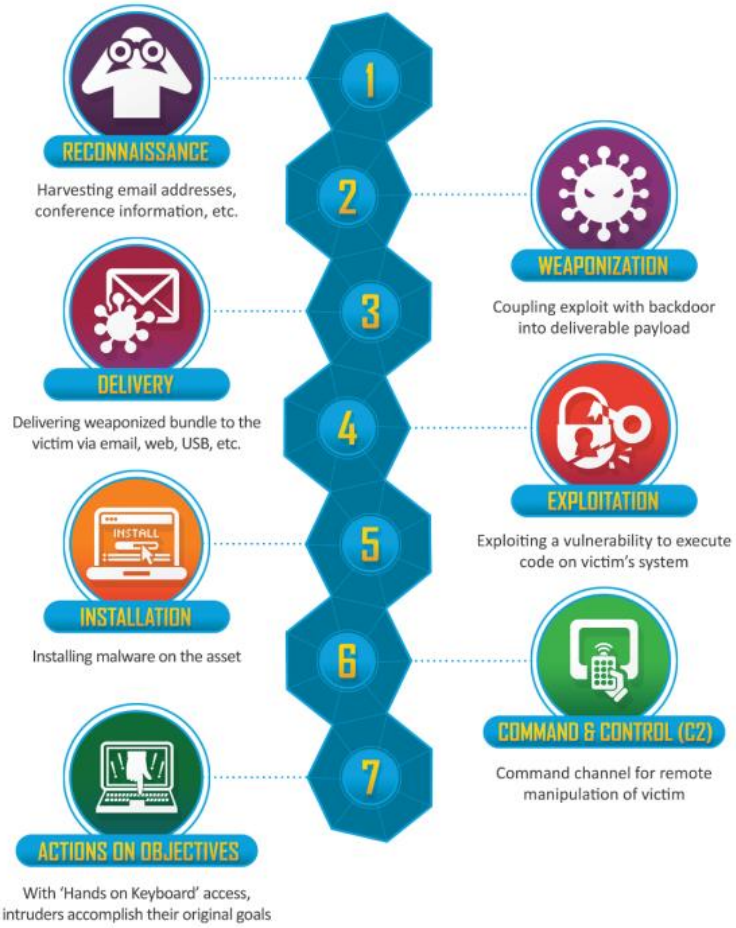

Figure 3. Cyberkill Chain [26].

It contemplates indicators of three typologies:

- Atomic: indicators that cannot be broken down into smaller parts and retain their meaning in the context of an attack (IP, domains, etc.);
- Computational: derived from the data obtained in an incident (hash);
- Behavioural: collections of atomic and computational indicators (TTPs).

Formally, following the mathematical representation proposed in the Diamond Model, given a step S, an event E can be represented as follows in the Cyberkill Chain model:

$$E = ((S_1), (S_2), (S_3), \ldots (S_n))$$

where n is the number of steps involved.

The great popularity of this framework offers the possibility of finding a wide range of technical reports from different consultancies and CERT/CSIRTs that follow its methodology. In turn, its structure inspired the development of the Mitre model's tactics. However, it has a very static and inflexible structure, especially for attacks that go beyond intrusions, such as those executed by APT groups, which has caused it to become progressively outdated. Based on the APT approach, ref. [27] implemented a series of algorithms after the extraction, selection, and classification of features at each of the phases of the Cyberkill Chain.

3.3. Mitre Att&ck

MITRE is a non-profit organisation founded in 1958 in the US that focuses on research, development, and innovation in information technology. As part of this work, the ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) model [28] was developed in 2015 as a knowledge- and information-sharing hub for cyberattacks focused on the development and application of the concept of TTPs, whereby tactics represent why an attacker performs certain actions to carry out their objective, techniques represent how the attacker performs the actions, and procedures represent the detailed steps for the implementation of the techniques.

This framework is increasingly deployed worldwide for its versatility and especially for its faithful representation of an attack based on observations of real attacks modelled with ATT&CK. The data implemented in the TTP database are drawn from intelligence reports produced by public and private entities around the world and have become a repository of great interest and utility for cybersecurity worldwide (see Figure 4).

Figure 4. Interest in Mitre Att&ck according to worldwide Google searches. Source: Google trends.

The backbone of the model consists of the representation of the TTPs by means of matrices in which the columns represent each of the defined tactics. The values of the matrix represent the techniques that can be applied in the analysis of an attack.

Formally, considering the tactics as columns and the techniques as rows, the matrix M can be defined as M_{ij}, where "i" is the index of the technique, and "j" is the index of the tactic. So, for a particular cyberattack that uses certain techniques and, consequently, certain tactics, the value 1 can be assigned to the corresponding cells of the matrix, and 0 can be assigned to the others. For example, if technique 3 is used in tactic 2, then $M_{32} = 1$.

So, considering the elements of the matrix M, an event E can be represented as follows:

$$E = ((M_{11}), (M_{12}), (M_{13}), \ldots (M_{mn}))$$

where m is the number of tactics involved, and n is the number of techniques involved in each tactic. There are different technical domains depending on the analysis objective: Enterprise, focused on attacks on entities; Mobile, referring to attacks on mobile environments; and ICS, referring to possible incidents in Industrial Control Systems. Likewise, each technical domain is different depending on whether it is applied to one operating system or another. The main applications of this framework are the detection and analysis of attacks, simulation, and Red Team in infrastructures and, in particular, CTI or threat intelligence.

Finally, the presence of a taxonomy of TTPs has made it possible over time to bring together homogenised information on the parameters of different attack groups, the software involved, vulnerabilities according to their Common Vulnerability Exposed (CVE), etc. Currently, there is a scarcity of research focused on the use of AI in the Mitre Att&ck model. The most relevant is likely the study conducted in [29], which applied clustering algorithms to determine possible associations of TTPs. On the other hand, and beyond AI, there are studies on the prediction of possible sequences of TTPs using game theory [30] and Markov chains [31].

3.4. Framework Comparison

Each of the three analysed frameworks has points of interest that can be of great value in an intelligence analysis and enrich it. Specifically, the Diamond Model offers a holistic and strategic vision of attacks with an approach to the classic concept of intelligence; Cyberkill Chain focuses on tactical aspects that an attacker executes; and Mitre Att&ck develops a wide range of concepts from the technical point of view that allow a detailed analysis of an attack.

On the other hand, Cyberkill Chain and Mitre Att&ck are structured and organised in different phases or stages, which can help to understand and visualise the attacker's actions. In short, the combination of detail, adaptability, widespread adoption, practical utility, and versatility have made the three models analysed stand out and become widely recognised in the field of cybersecurity and threat intelligence. Their popularity is also reinforced by their continued endorsement and use by the global cybersecurity community.

While it is true that the three models reflected above are widely known and used in the cybersecurity community, there are other alternatives that will not be analysed in this document because they are less used, but we consider their mention of interest:

- The NIST Cybersecurity Framework [32] is a framework that focuses on cybersecurity risk management and provides guidelines in areas such as identification, protection, detection, response, and recovery. Although it is widely used, it is not focused on cyber-intelligence analysis but rather on the risk analysis of entities.
- DREAD (Damage, Reproducibility, Exploitability, Affected Users, Discoverability) [33] is another method developed by Microsoft to assess and classify the risks associated with security threats in software and information technology systems.

Parallel to Att&ck, Mitre has developed framework projects for various purposes in the cybersecurity field that are not so focused on intelligence, such as TARA [34] (Threat Assessment and Remediation Analysis) for risk management, CAPEC (Common Attack Pattern Enumeration and Classification) for vulnerabilities and attack pattern analysis [35], and D3FEND [36] for the attack response strategy.

4. Materials and Methods

In order to observe the behaviour of each of the models in the face of a real cyberattack, a practical application was carried out in order to show the weaknesses and strengths of each model and to obtain elements of judgement to support the decision-making process regarding which cyber-intelligence framework to use in the research. To this end, a series of items were developed to be applied to each framework ex post so that the phases or sections of each model could be constructed following the proposal in [37].

The analysed cyberattack corresponds to a ransomware attack registered in a Spanish public entity in 2021. This public entity employs more than 7000 employees, spread throughout Spain's geography, and manages a budget of around 30,000 million euros, depending, in any case, on the transfers associated with the general state budgets managed by another governmental entity. A ransomware attack is a criminal activity that bases its success on the execution of threats to the victim, either through the possible deletion of the stolen information or through possible open publication. This type of attack has become widespread in recent times due to the financial gain it offers.

For security reasons, temporal and nominal references will be made under the pseudonym RASK; similarly, domains and other IOCs with the identity of the victim will be modified accordingly to avoid possible identification.

On 9 July 2021, a ransomware-type cybersecurity incident was detected in the systems of the Spanish public entity (RASK), with a massive infection by the "RYUK" malware. This attack is said to have affected several information and communication systems of this Administration, as well as email and web services, and workstations of civil servants of the organisation. The first evidence of the attack was detected in the early hours of 9 July 2021, and it was determined that it was the well-known ransomware-type code of the RYUK family. Evidence analysed during the investigation suggested that the network

intrusion may have been carried out using compromised credentials that allowed access to the network via Citrix. Thus, the prior sale of two user credentials in underground forums (08s-in08 and admdp08) was detected, the latter being an administrator account providing access to the following services:

vtagex.rask[.]en (users 08s-in08 and admdp08)
mytime.rask[.]en:1124 (user 08s-in08)
intraprod.rask[.]en (user PROD08)
e-mail.rask[.]es (users admdp08, 08s-in08 and 08dpucr)
supportcx.rask[.]es (user admdp08)
RASK Office 365 (user 08s-in08@rask.es)

The attack vector used by the attackers consisted of accessing RASK's infrastructure by using legitimate credentials stolen in another operation and sold in underground forums following the usual practice of these types of groups, which outsource the obtaining of access and focus on the intrusion and encryption itself. The fact that the attacker had "admin" access credentials indicates that the victim may not have been specifically and expressly selected by the attacker, which would favour the thesis of a purely cybercriminal attack and not one of cyber espionage or a specific search for sensitive information. Thus, the motivation for this attack would be to obtain sufficient financial gain through criminal activities involving threats to RASK, an entity that, due to its volume and importance, could bring in sufficient profits to make the attack worthwhile.

The first malicious connections to the infrastructure were recorded on 1 March 2021. Filtering connections made by one of the users revealed logins to machines with Russian alphabet characters. DNS, firewall, and proxy logs of the organisation were analysed, and the presence of several dll files was detected, the analysis of which showed that they were beacons of the Cobalt Strike and/or SystemBC software (e.g., qws.dll). When the attacker gained access to the network, he deployed the Cobalt Strike Beacon tool, which made connections with the following command-and-control (C2) servers throughout March 2021:

Timestamp (UTC)/IP of server C2/Domain of server C2:
01/07/2021 17:31 ---.26.29[.]242 culunk[.]com
01/07/2021 22:40 ---.141.84[.]190 smadst.com
01/07/2021 22:48 ---.141.84[.]190 smadst[.]com
06/07/2021 16:53 ---.26.29[.]245 eochea[.]com
06/07/2021 16:54 ---.26.29[.]245 eochea[.]com
06/07/2021 17:31 ---.141.87[.]76 dorkedit[.]com
06/07/2021 17:54 ---.26.29[.]245 eochea[.]com
06/07/2021 18:06 ---.141.87[.]76 dorkedit[.]com
06/07/2021 18:53 ---.26.29[.]245 eochea[.]com
06/07/2021 23:01 ---.26.29[.]245 eochea[.]com
08/07/2021 15:27 ---.26.29[.]245 eochea[.]com
08/07/2021 19:31 ---.26.29[.]245 eochea[.]com
08/07/2021 21:35 ---.26.29[.]245 eochea[.]com
08/07/2021 23:20 ---.26.29[.]245 eochea[.]com
08/07/2021 23:24 ---.26.29[.]245 eochea[.]com

This tool allowed the attacker to perform network reconnaissance, obtain more credentials of different users (including administrators) after accessing the Domain Controller, and identify computer names and servers. On 8 July, at 21:27, the file "desktop.dll", malware from the BazarLoader family, was detected. On 9 July, at 04:29:35, a file "82.exe" was observed executing on various computers from the path C:\Windows\Temp\, belonging to the Ryuk family of malware.

Once the attacker had completed network reconnaissance, he deployed and executed the Ryuk malware on as many computers as possible through lateral movements. This was accomplished by using administrator credentials and relying on the PsExec utility, which allows remote command execution. In addition, the malware includes its own replication capabilities that allowed it to spread across the network very quickly. These actions took

place on 9 July 2021, the day on which the compromise and encryption of information were detected.

An analysis of the information in open sources shows that the IPs used in the attack correspond to IP ranges associated with command-and-control panels of the UNC1878/Wizard Spider group.

The investigatory actions focused on the detection of the attack vector (key action for further investigation), the characterisation of the tools used in the attack (Cobalt Strike, SystemBC, BazarLoader, Ryuk, PsExec), and the search for IOCs (mainly IP directions). These actions were carried out without the application of any of the intelligence frameworks analysed in this document. As previously mentioned, attribution to the UNC1878 group was carried out only by associating IPs with the group's own IP ranges, without considering valuable information such as TTPs, as well as the context and background of this attack.

Prior to the treatment by each of the three frameworks or models, we proceed to structure all the information of the incident so that we can have a global vision of it.

4.1. Application of the Diamond Model

The incident data are structured according to the Diamond Model following the four vertices. To simplify the analysis and to avoid bias, confidence values have been omitted.

- Victim: The public entity analysed (RASK) is a victim of the Public Administration sector in Spain, with a geographical location distributed throughout the Spanish territory. Its popularity is high, and its political positioning is neutral. The economic capacity is low, as it does not have its own resources. The maturity of the organisation is low, as demonstrated by subsequent audits. The organisation is highly critical, as it is an essential entity for the exercise of the functions of the Spanish state. The types of systems affected are desktops and servers, including the five domain controllers. The information is not classified, but it is personal information subject to legislation. The organisation is not known to have exposed CVEs. The victim belongs to the Spanish Administration Sector, which is seriously lacking in cybersecurity, as shown in successive national reports on the state of security of ICT systems published by the national CSIRT [38].
- Capability: The malware used was at least Cobalt Strike, Ryuk, Bazar Loader, and SystemBC. There is no evidence of vulnerability exploitation because it was not necessary, as the attacker had administrator credentials. The malware used does not reflect great sophistication as they are evolutions of known malware widely used by cybercriminals in their attacks. It requires the intervention of the adversary, but no victims for the attack. Although the initial method of obtaining credentials is unknown, there is no evidence of the application of social engineering techniques. It is not part of any campaign to exploit or distribute malware through phishing or other types of attacks.
- Infrastructure: Once the information had been analysed from a technical point of view, the following IP addresses and domains that made up the main C2s were provided:

  ---.26.29[.]242 (Media Land LLC- Saint Petersburg 09-09-2020) culunk[.]com resolutions (registration 22/02/2021)
  --.141.84[.]190 (Media Land LLC- Saint Petersburg 14-11-2019) resolutions by smadst[.]com (registration 22/02/2021)
  ---.26.29[.]245 (Media Land LLC- Saint Petersburg 09-09-2020) eochea[.]com resolutions (registration 03/02/2021)
  --.141.87[.]76 (Media Land LLC- Saint Petersburg 25-12-2020) dorkedit[.]com resolutions (registration 03/03/2021)

The domains culunk[.]com, smadst[.]com, eochea[.]com, and dorkedit[.] were registered in close temporal proximity and have registration, hosting, and SSL certificate consistencies with previously identified UNC1878 domains [39]. The sets of UNC1878 domains were registered through *NameCheap* or *OpenProvider*, used their own name servers, are hosted on dedicated servers at the Russian Federation Media Land LLC IP IPS, and use multiple SSL certificate chains.

- Adversary: Probable attribution by identifying TTPs, as well as by matching IP ranges and domains with Cobalt Strike servers, can presumably be associated with UNC1878, an Eastern European cybercriminal group with connections to Ukraine and Russia, whose purpose is economic. UNC groups can evolve, eventually merging with other groups and potentially drifting into actors with recognised threat names such as "Advanced Persistent Threats" (APTs) or "Financially-Motivated Hacking Groups" (FINs) [40]. Some expert research has attributed the name "Group One" to the UNCT1878 actor, stating that its targets are "indiscriminate" and its infections are "opportunistic" and assigning it the following characteristics [41]:
  1. Infection vector: phishing emails, usually containing links.
  2. Speed of execution: the time between initial infection and encryption has recently been reduced from around 2–5 days to between 3 and 6 hours.
  3. Consistent use of self-signed Cobalt Strike samples.
  4. Use of legitimate tools along the post-engagement infection chain: Cobalt Strike, Empire, Meterpreter, Mimikatz, Kerbrute, Kerberoast, BloodHound, AdFind.
  5. Absence of exfiltration or publication of information about their victims.

According to various cybersecurity vendors, one-fifth of ransomware-related intrusions in 2020 were due to Ryuk, 83% of which were attributed to the UNC1878 group. As for the origins of this group, they are currently unknown. Despite directing its attacks at targets without following any detected pattern, some researchers have pointed out that the UNC1878 group is currently selecting targets preferentially linked to the provision of healthcare services in the United States (US) [42]. While the UNC1878 group has so far been described as a single uncategorised entity, other cybersecurity specialists have indicated that behind this threat actor is the same group as the one housed under the Wizard Spider moniker, also known as Gold Blackbourn [43]. Public information on Wizard Spider states that it is a threat actor that has been credited with Russian origins and the development of the Trickbot banking Trojan. The main targets of this actor are organisations in the fields of defence, finance, public administration, healthcare, and telecommunications on a global scale [44].

4.2. Application of the Cyberkill Chain Model

The data associated with the incident are structured according to the seven steps of the Lockheed Martin model (see Table 1) so that each step includes the associated indicators of compromise and any other information that may be of interest in analysing this attack.

Table 1. Application of the Cyberkill Chain model to the case under analysis.

ATTACK PHASE	INDICATORS
1. RECOGNITION	Target recognition and access Purchase of access credentials in underground forums: vtagex.rask[.].co.uk (users 08s-in08 and admdp08) myhours.rask[.].co.uk:1124 (user 08s-in08) intraprod.rask.co.uk (user PROD08) e-mail.rask[.]es (users admdp08, 08s-in08 and 08dpucr) supportcx.rask[.]es (user admdp08) Office 365 by RASK (user 08s-in08@rask[.]es)
2. WEAPONISATION	DLL_Bazar Loader file: "desktop.dll" DLL_CobaltStrike file "qws.dll" (08/07/2021 21:31) DLL_CobaltStrike file "test.dll" (06/07/2021 17:31) Ryuk file "82.exe" Ryuk file "6hr.exe" Ryuk file "6hr.exe" (06/07/2021 17:31) Cobalt Strike Beacon Cobalt Strike 87fb204.exe Beacon Cobalt Stike f59173f.exe [. . .]

Table 1. *Cont.*

ATTACK PHASE	INDICATORS
3. DEPLOYMENT	Access with administrator credentials admdp08 PsExec lateral movements (since 01/07/2021 12:05) Deployment of Cobalt Strike Beacons (since 06/07/2021 17:21) Access to Domain Controller (DC) listings (06/07/2021 18:14) [. . .]
4. EXPLOITATION	Displays BazarLoader "desktop.dll" in DC and executes SystemBC and Cobalt Strike malware (08/07/2021 21:27 21:31)
5. INSTALLATION	Malware Ryuk "82.exe" (09/07/2021 19:24) and "6hr.exe" (09/07/2021 4:17) in C:\Windows.
6. C2	Cobalt Strike and SystemBC connections to the following C2: IP Address-Domain ---.26.29.242-culunk[.]com IP Address-Domain ---.26.29[.]245-eochea[.]com IP Address-Domain --.141.84[.]190-smadst[.]com IP address-Domain --.141.210[.]78-choopa[.]com IP address-Domain --.141.87[.]60-vultr[.]com IP address-Domain --.141.87[.]76-dorkedit[.]com [. . .]
7. ACTIONS TO OBJECTIVES	Massive encryption of information on computers with AES256 symmetric algorithm, and subsequent encryption of AES key with RSA asymmetric algorithm.

4.3. Application of the Mitre Att&ck Model

The data associated with the incident are structured according to the v10.1 matrix version in the web browser (see Table 2) and include the indicated techniques with their corresponding numerical identifiers.

Table 2. Application of the Mitre Att&ck model to the case under analysis.

TACTICS		TECHNIQUES
1	RECONNAISSANCE (TA0043)	T1589: Gather Victim Identity Information; T1591: Gather Victim Org Information.
2	RESOURCE DEVELOPMENT (TA0042)	T1584: Compromise Infrastructure; T1588: Obtain Capabilities.
3	INITIAL ACCESS (TA0001)	T1078: Valid Accounts
4	EXECUTION (TA0002)	-
5	PERSISTENCE (TA0003)	T1078: Valid Accounts
6	PRIVILEGE ESCALATION (TA0004)	T1078: Valid Accounts
7	DEFENCE EVASION (TA0005)	T1078: Valid Accounts
8	ACCESS CREDENTIALS (TA0006)	-
9	DISCOVERY (TA0007)	T1069: Permission Groups Discovery

Table 2. *Cont.*

	TACTICS	TECHNIQUES
10	LATERAL MOVEMENT (TA0008)	T1210: Exploitation of Remote Services; T1021: Remote Services
11	COLLECTION (TA0009)	T1005: Data from Local System
12	COMMAND AND CONTROL (TA0011)	T1071: Application Layer Protocol
13	EXFILTRATION (TA0010)	T1041: Exfiltration Over C2 Channel
14	IMPACT (TA0040)	T1486: Data Encrypted for Impact

As reflected in the previous table, it can be seen that the possession of administrator credentials (admdp08) reduced the need to deploy techniques in various tactics, paving the way for attackers, especially in privilege escalation and persistence acquisition. Although the indicators of compromise are not explicitly shown, a structured matrix is obtained with the sequence used in the attack that represents the TTPs, which are much more reliable indicators for the analysis of an attack given the volatility of the IOCs. The representation of the sequence through a matrix allows comparisons to be made with other attacks, which, in turn, can be captured in a Mitre matrix. In this sense, this model allows the comparison of the RASK attack with other attacks and a mathematical treatment to help in this task.

5. Results

Following the methodology proposed in [45], seventeen variables of interest were included to evaluate the potential applications of AI to each framework. This is why the approach addresses not only mathematical perspectives, such as the ease of parameterisation or the creation of variables in the information submitted or even the existence of datasets, but also relevant considerations to analyse the power or utility of the framework and the capacity for adaptation (among other aspects). In this way, it is ensured that a comprehensive analysis is carried out. Hence, in order to study each of the presented frameworks and their suitability for large-scale data-based AI research, each of them is assessed with the following variables of interest:

- Maturity: reflects that the development of the standard has reached a sufficient degree.
- Flexibility: refers to the capacity to adapt to other environments outside the framework.
- Popularity: relative to the extent and use in the global community.
- Own taxonomy: existence of the framework's own categorisation of its characteristics.
- Datasets: existence of open sources of data repositories referring to that framework.
- Proprietary software: development of native tools that allow its application.
- Adaptation to different attacks: indicates whether the framework can be used for different types of attacks (ransomware, APT attacks, DDoS, etc.).
- Update: whether there is constant updating by the community or developer.
- Ease of use: usability of the framework by inexperienced users.
- Parameterisation: indicates the creation of variables or arguments to define the most relevant points of interest of an attack.
- Granularity: indicates whether the level of detail of the model is high.
- Visualisation: indicates whether the information can be viewed in graphical form.
- Easy integration with other systems: reflects possible integration with identification or protection systems (e.g., IDS/IPS or AntiVirus)

- Orientation: indicates which parameter is the primary focus: the attackers, the organisation's assets, or the software used in the attack.
- Scalability: indicates whether a framework has the ability to keep properly functioning when the amount of data changes in size or volume.
- Interoperability: the capacity of a framework to share data and facilitate information and knowledge exchange with other tools.
- Performance: indicates whether a framework is efficient in working with large-scale data.

Table 3 indicates whether each of the frameworks fulfils the described requirements according to its execution in the cyberattack example covered in this work. The realisation of these criteria is important to produce successful results in any AI-based research. Certainly, some of the mentioned characteristics play an important role in this sense, such as the existence of validated datasets, the level of granularity, scalability, performance, or flexibility. It might seem like some others, for example, the ease of use, popularity, or maturity, should take second place in this context, but they complete all implications that implementing and constructing an AI model supposes. Therefore, it is our belief that the accomplishment of all mentioned variables is important to categorise a framework as suitable and adequate for merging it with AI algorithms for large-scale data analysis.

Table 3. Analysis of the variables proposed in each of the models.

	DIAMOND MODEL	**CYBERKILL CHAIN**	**MITRE ATT&CK**
MATURITY	YES	YES	YES
FLEXIBILITY	NO	NO	YES
POPULARITY	NO	YES	YES
OWN TAXONOMY	NO	NO	YES
DATASETS	NO	NO	YES
PROPRIETARY SOFTWARE	NO	NO	YES
ADAPTATION TO DIFFERENT ATTACKS	YES	NO	YES
UPDATE	NO	NO	YES
EASE OF USE	YES	NO	NO
PARAMETERISATION	NO	NO	YES
GRANULARITY	YES	NO	YES
VISUALISATION	YES	YES	YES
EASY INTEGRATION WITH OTHER SYSTEMS	NO	YES	YES
ORIENTATION	ACTIVE ATTACKERS	ATTACKERS	ACTIVE ATTACKERS SOFTWARE
SCALABILITY	NO	NO	YES
INTEROPERABILITY	YES	YES	YES
PERFORMANCE	NO	NO	YES

According to the analysis shown in Table 3, it can be concluded that the Mitre Att&ck framework is the most suitable for processing large-scale data for cyber-intelligence purposes based on the following points of interest:

While it is true that the Diamond Model presents good results in terms of maturity, ease of use, visualisation—with its characteristic diamond that helps to understand the information in a simple way—and even granularity, with the presence of detailed features and meta-features, this model has significant shortcomings in variables that are especially relevant for the application of AI, such as the lack of parameterisation capacity, low scalability, reduced flexibility, and the absence of datasets.

Cyberkill Chain stands out for its maturity, popularity—it is widely known in the community—and ability to easily integrate with other systems, but like the Diamond Model, it does not possess the characteristics necessary for optimal AI implementation, such as flexibility, parameterisation, scalability, and the existence of datasets.

Mitre Att&ck has flexibility, has its own taxonomy, is referenced in datasets, has proprietary software, is regularly updated, and allows for parameterisation and granularity.

These factors are essential for the implementation of AI, as the existence of structured data and the ability to adapt and customise the model and to have a high level of detail can facilitate the training of machine-learning algorithms. Furthermore, its ability to work successfully with datasets of variable volume and to share its knowledge with other tools are also appropriate for its combination with AI algorithms. However, other variables that may be of interest for an overall analysis of the power of the framework, such as popularity, maturity, and orientation, show that it outperforms the rest of the models by a wide margin.

This idea is reinforced by the powerful dataset available on the MITRE website, which allows extensive data processing for machine-learning techniques, and the large community that develops new implementations on a regular basis. The use of the other two models analysed would require the creation of an ad hoc dataset without a homogeneous taxonomy as a starting point, which would make it extremely difficult to process the data to achieve the objectives of this research.

Once the use of the Mitre Att&ck framework has been considered, the treatment that can be given to it in order to achieve the objectives of applying AI techniques is presented in Figure 5. It can be seen that the processing of the data collected from various sources (including the official MITRE repository) will allow the enrichment of each of the phases of the cyber-intelligence branches (CTI, IR, and VM) through the development of modules that will be seen later (generation of attack sequences and determination of attack authorship). All the information obtained must pass through the sieve of the chosen framework, i.e., Mitre Att&ck, so all the information must be converted into matrices or, where appropriate, vectors, to which the appropriate machine-learning techniques will be applied to obtain sequences or authorship. Although this application will make it possible to delve deeper into purely technical aspects, it should be borne in mind that the Diamond Model and Cyberkill Chain offer a better understanding of the socio-political sphere and its role in the context of an attack, which can help and, in many cases, be decisive in dealing with a cyberattack.

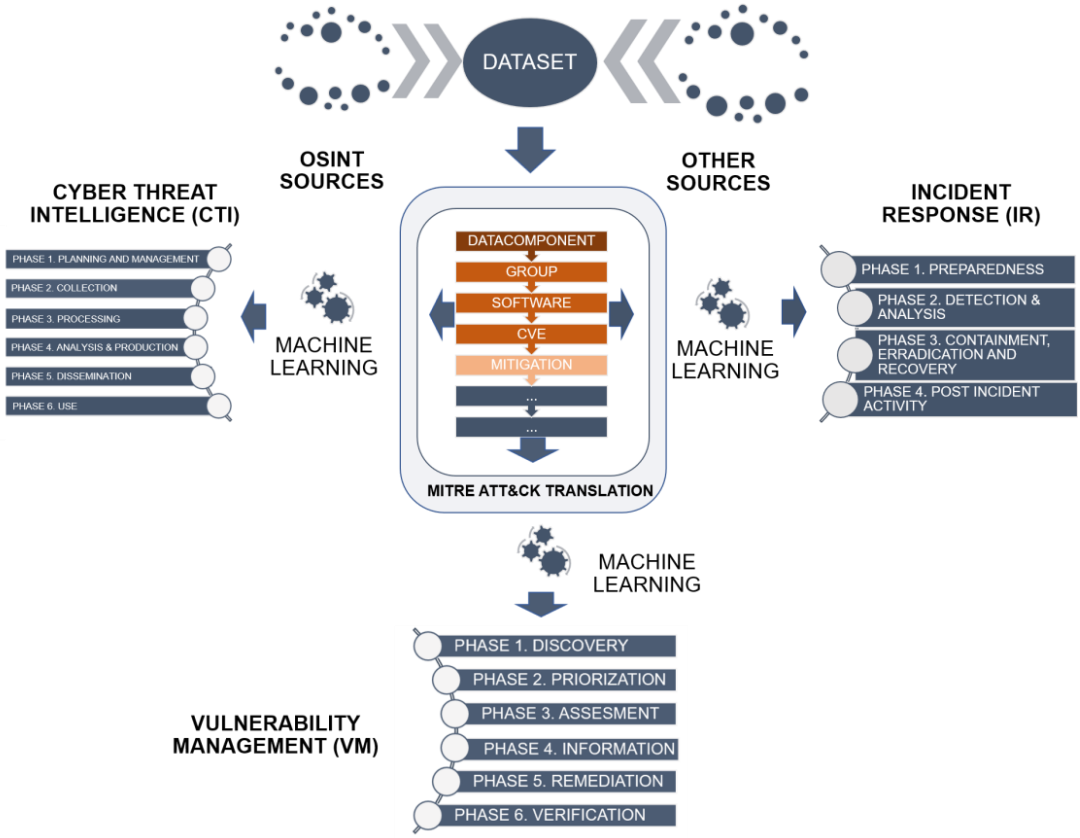

Figure 5. Mitre Att&ck framework application to machine-learning research in cyber intelligence.

Alternative works in the current literature regarding AI and cybersecurity and cyber intelligence usually focus on the elaboration of user authentication protocols [46–48]; network situation awareness [49,50]; dangerous behaviour monitoring [51,52]; and abnormal traffic identification [53,54]. In all cases, the main goal of the proposed schemes is to predict or identify an abnormal situation. In our work, the three most relevant cyber-intelligence frameworks are analysed to evaluate their potential to merge with AI technologies not only with this purpose in mind but also with two additional goals: the precise identification of future vulnerabilities in the system and the creation of a protocol that can rapidly classify a cyber incident, automatically proposing response actions to mitigate its effect.

6. Conclusions

Nowadays, it is unquestionable that cyber intelligence is an essential area of cybersecurity. The difficulties in offering suitable responses to malicious activities have placed value on preventive measures, with cyber-intelligence frameworks becoming especially important. This paper analyses intelligence frameworks that can be useful for the application of machine-learning algorithms. To do so, firstly, an overview of the concept of cyber intelligence and all its variants and possible applications in cybersecurity is presented. Then, three cyber-intelligence frameworks are detailed: Diamond Model, Cyberkill Chain, and Mitre Att&ck; their strengths and weaknesses are provided from a perspective that takes into account the application not only from a mathematical point of view but also from a holistic perspective that ensures that the framework used is the most suitable. This study and analysis highlighted the practical application of the models to a real case study of a ransomware attack. Although the three frameworks offer different advantages, we conclude that the Mitre Att&ck framework is the most appropriate to combine with AI techniques due to its power, its suitability for data processing, and the existence of available datasets.

For future work, it is advisable to develop a comprehensive cyber-intelligence framework that integrates the characteristics of each of the three frameworks developed in this article, especially including the more classical aspects of intelligence offered by the Diamond Model, together with the more technical and more automated aspects of Mitre's model. Likewise, it seems appropriate to look for a methodology to deal with the categorical variables of the Mitre matrix; to analyse the suitability, strengths, and weaknesses of the available datasets; and to execute the whole set of data-wrangling tasks necessary for the further application of machine-learning algorithms to the Mitre Att&ck framework.

Author Contributions: Conceptualisation, A.S.d.M.; methodology, A.S.d.M.; software, A.S.d.M.; validation, A.S.d.M. and L.H.-Á.; formal analysis, A.S.d.M. and L.H.-Á.; investigation, A.S.d.M.; resources, A.S.d.M.; data curation, A.S.d.M.; writing—original draft preparation, A.S.d.M.; writing—review and editing, A.S.d.M. and L.H.-Á.; visualisation, A.S.d.M. and L.H.-Á.; supervision, L.H.-Á.; project administration, A.S.d.M. and L.H.-Á.; funding acquisition, L.H.-Á. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: This work was supported by the Spanish State Research Agency (AEI) of the Ministry of Science and Innovation (MCIN), project P2QProMeTe (PID2020-112586RBI00/ AEI/10.13039/501100011033). L.H.A. would like to thank CSIC Project CASDiM for its support.

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

References

1. Yan, K.; Liu, L.; Xiang, Y.; Jin, Q. Guest Editorial: AI and Machine Learning Solution Cyber Intelligence Technologies: New Methodologies and Applications. *IEEE Trans. Ind. Inform.* **2020**, *16*, 6626–6631. [CrossRef]
2. Kemmerer, R.A. Cybersecurity. In Proceedings of the 25th International Conference on Software Engineering, Portland, OR, USA, 3–10 May 2003; pp. 705–715. [CrossRef]
3. Kim, S.H.; Wang, Q.-H.; Ullrich, J.B. A comparative study of cyberattacks. *Commun. ACM* **2012**, *55*, 66–73. [CrossRef]
4. Ludwick, M.; McAllister, J.; Mellinger, A.O.; Sereno, K.A.; Townsend, T. *Cyber Intelligence Tradecraft Project: Summary of Key Findings*; Software Engineering Institute: Pittsburgh, PA, USA, 2013; Available online: https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=40201 (accessed on 4 August 2023).
5. Preuveneers, D.; Joosen, W.; Bernabe, J.B.; Skarmeta, A. Distributed Security Framework for Reliable Threat Intelligence Sharing. *Secur. Commun. Netw.* **2020**, *2020*, 8833765. [CrossRef]
6. Gordon, L.A.; Loeb, M.P.; Zhou, L. Integrating cost–benefit analysis into the NIST Cybersecurity Framework via the Gordon–Loeb Model. *J. Cybersecur.* **2020**, *6*, tyaa005. [CrossRef]
7. *ISO/IEC 27000:2018*; Information Security, Cybersecurity and Privacy Protection. International Organization of Standards: Geneva, Switzerland, 2018. Available online: https://www.iso.org/standard/73906.htmlg (accessed on 4 August 2023).
8. National Institute of Standards and Technology. Guide for Conducting Risk Assessments. 2012. Available online: https://doi.org/10.6028/NIST.SP.800-30r1 (accessed on 4 August 2023).
9. López-Muñoz, J. *Manual de Inteligencia*; Tirant Lo Blanch: València, Spain, 2019.
10. Centro Criptológico Nacional. Guía de Seguridad de las Tic (CCN-STIC-480A) Seguridad en el Control de Procesos y Scada Guia de Buenas Prácticas. February 2010. Available online: https://www.ccn-cert.cni.es/series-ccn-stic/guias-de-acceso-publico-ccn-stic/209-ccn-stic-480a-seguridad-en-sistemas-scada-guia-de-buenas-practicas/file.html (accessed on 1 May 2022).
11. Bautista, W. *Practical Cyberintelligence*; Packt Publishing: Birmingham, UK, 2018.
12. Bishop, C.M. Pattern Recognition and Machine Learning. In *Information Science and Statistics*; Springer: New York, NY, USA, 2006.
13. Glassman, M.; Kang, M.J. Intelligence in the internet age: The emergence and evolution of Open Source Intelligence (OSINT). *Comput. Hum. Behav.* **2012**, *28*, 673–682. [CrossRef]
14. The MITRE Corporation. Structured Threat Information eXpression (STIX™). Available online: https://makingsecuritymeasurable.mitre.org/docs/stix-intro-handout.pdf (accessed on 22 June 2023).
15. The MITRE Corporation. Trusted Automated eXchange of Indicator Information—TAXII™. Available online: https://makingsecuritymeasurable.mitre.org/docs/taxii-intro-handout.pdf (accessed on 22 June 2023).
16. Mattern, T.; Felker, J.; Borum, R.; Bamford, G. Operational Levels of Cyber Intelligence. *Int. J. Intell. CounterIntell.* **2014**, *27*, 702–719. [CrossRef]
17. Bianco, D.J. Enterprise Detection & Response: The Pyramid of Pain. Enterprise Detection & Response. 1 March 2013. Available online: http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html (accessed on 22 June 2023).
18. *NIST SP 800-61r2*; Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology. National Institute of Standards and Technology: Gaithersburg, MD, USA, 2012. [CrossRef]
19. *NIST SP 800-40ver2*; Creating a Patch and Vulnerability Management Program. National Institute of Standards and Technology: Gaithersburg, MD, USA, 2005. [CrossRef]
20. Vulnerability Management Life Cycle | NPCR | CDC. 20 January 2021. Available online: https://www.cdc.gov/cancer/npcr/tools/security/vmlc.htm (accessed on 22 March 2022).
21. Naik, N.; Jenkins, P.; Grace, P.; Song, J. Comparing Attack Models for IT Systems: Lockheed Martin's Cyber Kill Chain, MITRE ATT&CK Framework and Diamond Model. In Proceedings of the 2022 IEEE International Symposium on Systems Engineering (ISSE), Vienna, Austria, 24–26 October 2022; pp. 1–7. [CrossRef]
22. Caltagirone, S.; Pendergast, A.; Betz, C. *The Diamond Model of Intrusion Analysis*; Center for Cyber Threat Intelligence and Threat Research: Hanover, MD, USA, 2013; p. 62.
23. Shin, Y.; Lim, C.; Park, M.; Cho, S.; Han, I.; Oh, H.; Lee, K. Alert correlation using diamond model for cyber threat intelligence. In *Proceedings of the European Conference on Cyber Warfare and Security*; Academic Conferences International Limited: Oxfordshire, UK, 2019; pp. 444–450.
24. Hutchins, E.M.; Cloppert, M.J.; Amin, R.M. Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. *Lead. Issues Inf. Warf. Secur. Res.* **2011**, *1*, 80.
25. Means, C.D. *Applying Cognitive Work Analysis to Time Critical Targeting Functionality*; Defense Technical Information Center: Fort Belvoir, VA, USA, 2004; p. 161.
26. Lockheed Martin. Cyber Kill Chain®. Available online: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html (accessed on 26 June 2023).
27. Ahmed, Y.; Taufiq, A.; Arafatur, R.M. A cyber kill chain approach for detecting advanced persistent threats. *Comput. Mater. Contin.* **2021**, *67*, 2497–2513. [CrossRef]

28. Strom, B.E.; Applebaum, A.; Miller, D.P.; Nickels, K.C.; Pennington, A.G.; Thomas, C.B. *Mitre Att&ck: Design and Philosophy*; Technical Report; The MITRE Corporation: Bedford, MA, USA, 2018.
29. Al-Shaer, R.; Spring, J.M.; Christou, E. Learning the Associations of MITRE ATT&CK Adversarial Techniques. *arXiv* **2020**, arXiv:2005.01654.
30. Nisioti, A.; Loukas, G.; Rass, S.; Panaousis, E. Game-Theoretic Decision Support for Cyber Forensic Investigations. *Sensors* **2021**, *21*, 5300. [CrossRef] [PubMed]
31. Alavizadeh, H.; Jang-Jaccard, J.; Alpcan, T.; Camtepe, S.A. A Markov Game Model for AI-based Cyber Security Attack Mitigation. *arXiv* **2021**, arXiv:2107.09258.
32. *NIST CSWP 04162018*; Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. National Institute of Standards and Technology: Gaithersburg, MD, USA, 2018. [CrossRef]
33. Shostack, A. *Experiences Threat Modeling at Microsoft*; Shostack + Associates: Seattle, WA, USA, 2008.
34. Wynn, J. *Threat Assessment and Remediation Analysis (TARA)*; MITRE Corporation: Bedford, MA, USA, 2014; Available online: https://apps.dtic.mil/sti/pdfs/AD1016629.pdf (accessed on 4 August 2023).
35. Kanakogi, K.; Washizaki, H.; Fukazawa, Y.; Ogata, S.; Okubo, T.; Kato, T.; Kanuka, H.; Hazeyama, A.; Yoshioka, N. Comparative Evaluation of NLP-Based Approaches for Linking CAPEC Attack Patterns from CVE Vulnerability Information. *Appl. Sci.* **2022**, *12*, 3400. [CrossRef]
36. Kaloroumakis, P.E.; Smith, M.J. *Toward a Knowledge Graph of Cybersecurity Countermeasures*; MITRE Corporation: Bedford, MA, USA, 2020; p. 11.
37. Al-Mohannadi, H.; Mirza, Q.; Namanya, A.; Awan, I.; Cullen, A.; Disso, J. Cyber-Attack Modeling Analysis Techniques: An Overview. In Proceedings of the 2016 IEEE 4th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW), Vienna, Austria, 22–24 August 2016; pp. 69–76. [CrossRef]
38. Centro Criptológico Nacional. Resultados Informe INES CCN. Available online: https://www.ccn-cert.cni.es/soluciones-seguridad/ines/resultado-general.html (accessed on 29 March 2022).
39. ThreatConnect IOCs Wizard Spider. Available online: https://threatconnect.com/blog/threatconnect-research-roundup-threat-intelligence-update/ (accessed on 29 March 2022).
40. Mandiant. Going ATOMIC: Clustering and Associating Attacker Activity at Scale. Available online: https://www.mandiant.com/resources/clustering-and-associating-attacker-activity-at-scale (accessed on 29 March 2022).
41. ANSSI. Ryuk Ransomware. Available online: https://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-006.pdf (accessed on 29 March 2022).
42. CISA. Alert. Ransomware Activity Targeting the Healthcare and Public Health Sector. Available online: https://www.cisa.gov/uscert/ncas/alerts/aa20-302a (accessed on 29 March 2022).
43. Fact Sheet: Trickbot Malware. Available online: https://www.cisa.gov/uscert/sites/default/files/publications/TrickBot_Fact_Sheet_508.pdf (accessed on 29 March 2022).
44. Thai CERT EDTA. *Threat Group Cards: A Threat Actor Encyclopedia*; Thai CERT EDTA: Bangkok, Thailand, 2019.
45. Tatam, M.; Shanmugam, B.; Azam, S.; Kannoorpatti, K. A review of threat modelling approaches for APT-style attacks. *Heliyon* **2021**, *7*, e05969. [CrossRef] [PubMed]
46. Hernández-Álvarez, L.; Barbierato, E.; Caputo, S.; Mucchi, L.; Encinas, L.H. EEG Authentication System Based on One- and Multi-Class Machine Learning Classifiers. *Sensors* **2023**, *23*, 186. [CrossRef] [PubMed]
47. Zeng, J.; Wang, F.; Deng, J.; Qin, C.; Zhai, Y.; Gan, J.; Piuri, V. Finger Vein Verification Algorithm Based on Fully Convolutional Neural Network and Conditional Random Field. *IEEE Access* **2020**, *8*, 65402–65419. [CrossRef]
48. Lu, X.; Xiao, L.; Xu, T.; Zhao, Y.; Tang, Y.; Zhuang, W. Reinforcement Learning Based PHY Authentication for VANETs. *IEEE Trans. Veh. Technol.* **2020**, *69*, 3068–3079. [CrossRef]
49. Yang, H.; Jia, Y.; Han, W.-H.; Nie, Y.-P.; Li, S.-D.; Zhao, X.-J. Calculation of Network Security Index Based on Convolution Neural Networks. In *Artificial Intelligence and Security*; Sun, X., Pan, Z., Bertino, E., Eds.; Lecture Notes in Computer Science; Springer International Publishing: Cham, Switzerland, 2019; pp. 530–540. [CrossRef]
50. Li, X.; Zhang, X.; Wang, D. Spatiotemporal Cyberspace Situation Awareness Mechanism for Backbone Networks. In Proceedings of the 2018 4th International Conference on Big Data Computing and Communications (BIGCOM), Chicago, IL, USA, 7–9 August 2018; pp. 168–173. [CrossRef]
51. Marir, N.; Wang, H.; Feng, G.; Li, B.; Jia, M. Distributed Abnormal Behavior Detection Approach Based on Deep Belief Network and Ensemble SVM Using Spark. *IEEE Access* **2018**, *6*, 59657–59671. [CrossRef]
52. Aljamal, I.; Tekeoğlu, A.; Bekiroglu, K.; Sengupta, S. Hybrid Intrusion Detection System Using Machine Learning Techniques in Cloud Computing Environments. In Proceedings of the 2019 IEEE 17th International Conference on Software Engineering Research, Management and Applications (SERA), Honolulu, HI, USA, 29–31 May 2019; pp. 84–89. [CrossRef]

53. Kong, L.; Huang, G.; Wu, K.; Tang, Q.; Ye, S. Comparison of Internet Traffic Identification on Machine Learning Methods. In Proceedings of the 2018 International Conference on Big Data and Artificial Intelligence (BDAI), Beijing, China, 22–24 June 2018; pp. 38–41. [CrossRef]
54. Kong, L.; Huang, G.; Zhou, Y.; Ye, J. Fast Abnormal Identification for Large Scale Internet Traffic. In Proceedings of the 8th International Conference on Communication and Network Security, in ICCNS '18, Qingdao, China, 2–4 November 2018; Association for Computing Machinery: New York, NY, USA, 2018; pp. 117–120. [CrossRef]