A taxonomy for threat actors' delivery techniques

Villalón-Huerta, Antonio; Ripoll-Ripoll, Ismael; Marco-Gisbert, Hector

Published in:
Applied Sciences

DOI:
10.3390/app12083929

Published: 13/04/2022

Document Version
Publisher's PDF, also known as Version of record

applied sciences

MDPI

Article

A Taxonomy for Threat Actors' Delivery Techniques

Antonio Villalón-Huerta [1], Ismael Ripoll-Ripoll [2] and Hector Marco-Gisbert [2,*]

[1] S2 Grupo, Ramiro de Maeztu 7, 46022 Valencia, Spain; antonio.villalon@s2grupo.es
[2] Department of Computing Engineering, Universitat Politècnica de València, Camino de Vera s/n, 46022 Valencia, Spain; iripoll@disca.upv.es
* Correspondence: hecmargi@disca.upv.es

Abstract: The main contribution of this paper is to provide an accurate taxonomy for delivery techniques, which allows the detection of novel techniques and the identification of appropriate countermeasures. Delivery is a key stage for offensive cyber operations. During delivery, a threat actor tries to gain an initial foothold into the targeted infrastructure. It is the first step of an offensive cyber operation, where the threat actor interacts with its victim in a hostile way; thus, its success is mandatory for the global achievement of the operation. However, delivery techniques are not well structured among the literature, being in many cases a simple list of techniques with which, if one of them is slightly modified by the threat actor, its detection becomes very difficult. This situation hinders the modeling of hostile actors, a fact that makes it difficult to identify countermeasures to detect and neutralize their malicious activities. In this work, we analyze the current delivery techniques' classification approaches and the problems linked to them. From this analysis, we propose a novel taxonomy that allows the accurate classification of techniques, overcoming the identified problems and allowing both the discovery of new techniques and the detection of gaps in deployed countermeasures. Our proposal significantly reduces the amount of effort needed to identify, analyze, and neutralize hostile activities from advanced threat actors, in particular their initial access stage. It follows a logical structure that can be easy to expand and adapt, and it can be directly used in the industry's commonly accepted standards, such as MITRE ATT&CK.

Keywords: cyber kill chain; delivery; initial access; advanced persistent threat; MITRE ATT&CK

Citation: Villalón-Huerta, A.; Ripoll-Ripoll, I.; Marco-Gisbert, H. A Taxonomy for Threat Actors' Delivery Techniques. *Appl. Sci.* **2022**, *12*, 3929. https://doi.org/10.3390/app12083929

Academic Editor: Luis M. Camarinha-Matos

Received: 16 March 2022
Accepted: 8 April 2022
Published: 13 April 2022

1. Introduction

Computer Network Operations (CNO) are defined as the actions taken through the use of computers and networks to gain information superiority or to deny the adversary this enabling capability. CNO is an umbrella term that comprises three main activities [1]: Computer Network Attack (CNA), Computer Network Defense (CND), and Computer Network Exploitation (CNE). CND is about computer and network protection, whereas CNE is focused on information gathering, that is, in cyber espionage, and CNA is related to degradation, disruption, destruction, or manipulation actions. The offensive CNO are those related to CNA and CNE, and they are both defined by a series of mandatory steps for the operation to be successful. In each of these steps, a set of tactics, which define what an hostile actor is doing, are performed by specific techniques, which define how the hostile actor accomplishes a tactic.

In these offensive operations, the initial access, or delivery, is the first mandatory step in which the hostile actor approaches its target in an offensive way and has a direct contact with it. Although some reconnaissance techniques, a previous step, can be also executed with a hostile approach to the target, they are not always mandatory in an operation, as reconnaissance can be achieved by information-gathering techniques, such as passive or semi-passive, which are not considered hostile [2].

The delivery being the first mandatory hostile approach to a target, it is, as well, the first moment where an operation can be detected and neutralized; in fact, delivery

is considered a high-risk task for hostile actors, as it leaves traces in the target [3]. For this reason, it is a must for defenders to understand how delivery is performed by threat actors. Without a clear understanding of the tactic and their associated techniques, defense is harder and the success rate for the threat actor increases.

Our paper provides a suitable taxonomy for techniques exploited to achieve the delivery tactic; we have dissected the tactic and identified its key elements, defined them, and designed a taxonomy for them. These key elements are the malicious objects delivered to a target (delivery object) in a specific way (delivery vector) and that break the security perimeter of the target in a specific way (delivery path). With these three elements, we can classify all delivery techniques, and we can identify as well different approaches not commonly exploited but which would allow a hostile actor to achieve persistence.

The contributions of this paper are summarized as follows:

- To identify and define the key elements that compose the delivery tactic.
- To structure the delivery tactic approaches used in offensive Computer Network Operations (CNE or CNA).
- To provide an accurate taxonomy for techniques into the delivery tactic for these operations, thus allowing defenders to detect novel or uncommon techniques, identify specific countermeasures, and improve global security.

The rest of the paper is organized as follows. The background, Section 2, provides a brief introduction to the Cyber Kill Chain and to the MITRE ATT&CK framework, as two of the main frameworks for the modeling of offensive operations, both in their steps and in their tactics and techniques. In Section 3, we assess the problem of the lack of a unified taxonomy for the delivery tactics and its importance for the modeling of threat actors and operations. Section 4 analyzes the prior work in this field, stating that little research has been conducted in this sense. In Section 5, we propose a novel taxonomy for the techniques inside the delivery tactic, identifying the key aspects to classify particular techniques. In Section 6, we discuss the results of our work, comparing them with other approaches and identifying improvements, as well as future research lines. Finally, Section 7 summarizes the outcome of the overall work.

2. Background

2.1. Mitre ATT&CK

MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) is a globally accessible knowledge base of adversary tactics and techniques based on real-world observations. This knowledge, contributed by analysts all around the world, can be used as the base for the development of specific threat models and methodologies. Started in 2013 and published in 2015, ATT&CK develops a process for modeling an adversary's post-compromise behavior at a fine level. A description of the framework and the work performed can be found at [4].

Tactics specify what a threat actor is doing, at the highest level of description, to accomplish a certain mission. Techniques specify how tactics are implemented, and procedures describe a particular implementation of a technique. These tactics, techniques, and procedures represent the behavior of a threat actor from the highest level description (tactic) to the lowest level one (procedure). MITRE ATT&CK framework is today's de facto standard to structure tactics and techniques of advanced threat actors. As of March 2022, MITRE ATT&CK had defined 14 enterprise tactics—those related to the activities of an attacker onto its victim—and 188 enterprise techniques associated with those tactics and 379 sub-techniques. Apart from that, MITRE ATT&CK defines 14 mobile tactics, related to the compromise of mobile devices, and 92 mobile techniques. Beside tactics and techniques, ATT&CK identifies software (a generic term for tools, artifacts, malware, etc.) that can be used to implement one or more of the techniques, and which is out of the scope of this work.

In the ATT&CK Matrix for Enterprise, the framework represents tactics as the adversary's tactical goals for acting [5]. Although ATT&CK does not provide a kill-chain

approach to specify the arrangement of tactics, most of them are presented in the logical order that a threat actor follows in hostile operations. All of them can be achieved through different techniques, and a single technique that can be associated with one or more tactics. There is no formal structure in MITRE ATT&CK for techniques in each tactic, all of them being represented in a plain view. For example, for the Command and Control tactic, representing the goal of enabling the remote control of the compromised infrastructure, the framework identifies techniques such as Data Encoding, Data Obfuscation, Protocol Tunneling, or Remote Access Software. The structure of tactics and techniques in MITRE ATT&CK allows analysts to organize which adversarial actions belong to specific techniques and tactics, thus helping defensive teams to understand what a threat actor may be trying to achieve, how this actor is trying to achieve it and how to better defend against the threat [6].

MITRE ATT&CK also links Advanced Persistent Threat groups, APTs, to tactics, techniques, and software. With 110 identified groups at the time of this writing, all of them are named, aliased, described, and linked to specific techniques (including pre-attack and mobile) and software. In this way, an analyst can establish relationships between those entities to model an adversary and its activities against a target and, most importantly, to establish the defense mechanisms to prevent, detect, and respond to a threat.

MITRE ATT&CK represents an enormous effort to provide to the community a unified framework to identify the activities of advanced threat actors, from their TTP to the software they use, correlate information among those entities, and improve, not only the knowledge about APT, but also the defense mechanisms required for their detection and response. It constitutes a framework that, as usual, has to be improved with continuous work and contributions; in this sense, we miss in the MITRE ATT&CK a more defined structure for techniques inside each tactic. The standard specifies all tactics for a cyber kill-chain model but, for each tactic, all related techniques have a plain structure, broken only by the specification of sub-techniques and, particularly, implementations of a specific technique.

2.2. Cyber Kill Chain®

The Cyber Kill Chain® framework [7], developed by Lockheed Martin, is part of the Intelligence-Driven Defense® model for the identification and prevention of cyber intrusion activity, identifying what a threat actor must complete in order to achieve its ive. It was first described in [7] as a seven-step process suitable for CNA or CNE operations, as shown in Figure 1.

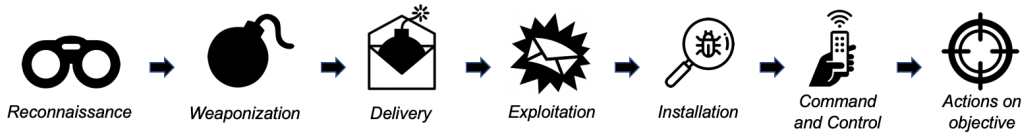

Figure 1. Cyber Kill Chain® as defined in [7].

These seven steps are defined as follows [7,8]:

1. Reconnaissance. Research, identification, and selection of targets.
2. Weaponization. Before attacking a target, the threat actor has to couple a remote access Trojan with an exploit into a deliverable payload.
3. Delivery. The transmission of weapons to the targeted environment to launch a particular operation.
4. Exploitation. After the weapon is delivered, the exploitation triggers an intruders' code.
5. Installation. The installation of an implant, just as a remote access Trojan, a backdoor, or any kind of malicious software, on the victim system, allowing the adversary to maintain persistence inside the environment.

6. Command and Control. The compromised hosts must beacon outbound to an Internet controller server to establish a C2 channel, thus allowing the threat actor to remotely control its target.
7. Actions on objectives. After progressing through the first six phases, the intruders can take actions to achieve their original goals, such as information theft, denial, or hop to a third-party infrastructure.

The cyber kill chain represents an industry-accepted methodology for understanding how an attacker will conduct the activities necessary to cause harm to an organization and has been largely discussed [9] (in ref. [10], the authors identify some of the discussions regarding the application of the Cyber Kill Chain). Some authors [11,12] have proposed the addition and removal of different stages in order to improve or adjust the original model, and the topic has also been discussed in technical conferences. Moreover, some efforts to unify models and variants, such as [13], have been made. Despite this, the original proposal has been widely used and applied to specific problems regarding advanced threat actors, such as those related to the modeling of the attack stages against critical infrastructures [14–17].

3. Problem Statement

In the modeling of offensive operations, the establishment of an accurate sequence of actions and the identification of the tactics and techniques that threat actors perform in order to achieve their goals is a key requirement for the prevention, detection, and neutralization of the threat. The analysis of the initial foothold into a target infrastructure is a must for this modeling of hostile activities. The Cyber Kill Chain "Delivery" stage or the MITRE ATT&CK "Initial access" tactic both represent this point of initial contact between the threat actor and its target.

The delivery tactic is usually linked to the delivery of a malicious payload to the target, embedded into a weaponized such as a particular file type or web link. In fact, in many references delivery is just identified as "payload delivery" [18–20] or "malware delivery" [21,22]. The delivered has been generated on a previous stage of the operation, usually called weaponization [7], and, after a successful delivery, the payload is detonated, starting the next stage of the attack, which is commonly identified as exploitation.

This focus on the delivery of malware or malicious payloads has relevant limitations. It refers only to specific delivery techniques, while other ones, whose use is increasing on a daily basis, are not considered in this concept. Malwareless operations do not use malicious payloads, not only to achieve the delivery tactic, but none of the required tactics perform a successful operation.

Nowadays, threat actors' delivery techniques include not only the weaponization of a malicious payload, but also different approaches, some of them even without a malicious payload, that allow hostile actors to accomplish their goal: to break the target's security perimeter and to open the way for the exploitation stage.

We have analyzed different approaches for the identification of a suitable up-to-date classification scheme for delivery techniques, especially for the ones not linked to the use of malicious code and simply being the abuse of legit resources. In Section 4 we present a summary of these approaches. However, no suitable approximation for such a structure that allows analysts to detect an ongoing operation has been identified. It is mandatory to analyze, understand, and identify the different techniques for delivery used nowadays, in order to be able to detect and neutralize them. Such a structure would allow analysts to identify gaps in their security countermeasures and to discover new techniques deployed for the delivery tactic.

4. Techniques and Limitations

Until this moment, no valid complete taxonomy for delivery techniques has been identified. All approaches are partial, providing a relationship of delivery techniques but without a particular structure, focusing on an specific type of delivery, or analyzing just

particular delivery techniques used by a given threat actor. We miss a global structure to classify delivery techniques, which allows not only this classification but also the identification of security gaps in the monitoring scheme for an organization. Such a taxonomy would allow analysts to detect the compromise of their infrastructures, as well as to identify those monitoring gaps and deploy countermeasures against previously unknown techniques.

As we have stated before, MITRE ATT&CK is the key reference for the identification of delivery techniques, identified as Initial Access in the framework. It focuses on the adversary tactics, techniques, and procedures (TTP) derived from real attacks [23]. However, this framework does not provide any classification for these techniques, exposing just a plain relationship for them and their sub-techniques. Although, such as an approximation is useful for the identification of particular techniques used in offensive operations, it lacks a whole structure, so it can not be taken as a valid reference for the definition of a delivery techniques' taxonomy.

The Cyber Kill Chain represents a starting point that provides an intelligence framework for understanding the multistage attack. It identifies the "Delivery" stage of a hostile operation but it does not provide any information about adversarial tactics and techniques. Following the Cyber Kill Chain stages, and with different kill chain models, many works [13,24–27] provide specific examples of delivery techniques; however, few of them discuss these techniques from a threat modeling perspective. In addition to particular examples, no valid taxonomy approach has been identified in these works. In the case of specific operations related to APT activities, we face the same situation; different works [28–30] analyze the delivery techniques used by Advanced Persistent Threats in their campaigns, providing particular examples of techniques, but none of them present a taxonomy for the delivery tactic. With a more general approach, ref. [31] analyzes life cycles and models for Advanced Persistent Threat operations.

In [32], Ping Chen et al. identify two types of delivery techniques: direct and indirect delivery. In direct delivery, the hostile actors send exploits to their targets, while in indirect delivery, they compromise a third party that is trusted by the target, and then they use this compromised third party to indirectly serve exploits to the target. For each category, the authors propose spear phishing and the watering hole, respectively, as examples of techniques. In this work, the goal of the authors is not to provide a taxonomy for delivery techniques, but to present a general survey on Advanced Persistent Threats; for this reason, they do not focus on a particular taxonomy. In addition, as the paper is dated to 2014 we consider this a valid initial approach that needs to be enhanced; over the years, advanced threat actors have developed new techniques for the delivery tactic that have to be considered: for example, the exploiting of public facing applications. A similar approach is used in [33], although, in this case the provided examples do not reflect the used categories.

As specified in Section 3, most analyses are focused on the delivery of a malicious payload through multiple ways. Malware delivery campaigns have been analyzed in [34], in which Ziyun Zhu et al. adopt three stages from the STIX data model (exploitation, installation and command, and control) to represent malware delivery campaigns. As this approach is focused on modeling whole malicious campaigns, the delivery tactic is linked to other stages inside an operation, which is an approach inappropriate for our particular focus on the analysis of the delivery tactic.

Being a malware with high impact campaigns during the last few years, ransomware delivery has been specifically analyzed in different works. In [35], Keertika Gangwar et al. propose an analysis and detection approach of ransomware based on its delivery mechanisms. The authors provide a feature selection and extraction from different ransomware families, but they do not identify any classification for the delivery techniques used in each case, focusing only on URL and indicators of compromise linked to ransomware. In [36], Pratyush Raunak et al. focus on the detection of ransomware delivered through a specific technique, namely, exploit kits. In [26], Tooska Dargahi et al. discuss the delivery of ransomware by techniques linked to social engineering, malvertisement, and traffic

distribution systems, providing an analysis for each of them. None of these works tries to establish a complete taxonomy for ransomware delivery techniques.

General delivery techniques have been analyzed in-depth, taking into account both their description and their countermeasures. General social engineering attacks, on which many delivery techniques are based, are modeled with graphs in [37]. Phishing is modeled in works such as [38–40] or [41]. Watering hole techniques are described in [42,43]. Even less common delivery techniques, such as baiting [44,45] or supply chain compromise [46–48] have been deeply analysed. Please note that although not widely used until now, supply chain compromise is an increasing trend for threat actors, as we will detail later in this paper.

As stated before, social engineering is the base of many delivery techniques; apart from its modeling, different taxonomies have been developed for social engineering attacks. In [49], Koteswara Ivaturi et al. divide social engineering techniques into two main categories: person to person and person to person via media. In [50], Katharina Krombholz et al. establish three parameters for a taxonomy definition: type, operator, and channel, while [51] presents a kill chain to classify social engineering attacks, with three mandatory steps: orchestration, exploitation, and execution. In [52], Hussain Aldawood et al. differentiate two parameters to establish an accurate taxonomy: who or what attacks are based on (human or technology) and how they are executed (physical, technical, social, and socio-technical). In this work, the authors also provide accurate examples of particular techniques for many social engineering attacks. These works present different taxonomies for social engineering attacks; in [53] we can find a summary of them, and a survey is presented in [54], where Fatima Salahdine et al. provide accurate classification schemes for this technique. However, not all delivery techniques include social engineering; therefore, we must generalize our taxonomy in order to provide a global valid approach for the delivery tactic.

As phishing is one of the most widely used techniques for the delivery tactic, it has been largely analyzed and its particular implementations have been classified. In [55], Junaid Ahsenali Chaudhry et al. identify four phishing techniques: spear phishing, clone phishing, malware-based phishing, and search engine phishing. This approach is purely focused on specific technical aspects in order to identify phishing countermeasures; therefore, it is not suitable to establish a taxonomy, even an initial one. In [56], Justinas Rastenis et al. define a taxonomy for e-mail based phishing attacks, based on different features of the malicious e-mail used in an operation. The authors highlight the lack of e-mail-based phishing attacks' taxonomy and propose a novel one, but only with a focus on this particular technique; thus, it can not be considered a general purpose approach that is valid for all delivery techniques. In [57], Gaurav Varshney et al. propose five categories for web phishing techniques (the authors define them as "Tactics", an approximation that we consider inconsistent with the current definitions of tactics and techniques): Spoofing website text and images, web link manipulation, malicious use of scripting languages, Java Script popups, fake address bars, and utilizing browser vulnerabilities. However, this approach focuses only on web phishing, and does not consider other phishing techniques.

The literature review for delivery techniques and their classification, detailed in this section, can be grouped into six main families:

- General models, such as the MITRE ATT&CK or kill-chain models, where delivery is considered as a tactic that can be performed through different approaches.
- Threat actors reports, which analyze specific delivery techniques exploited in real operations.
- Initial classification approaches, which try to propose a classification scheme for delivery techniques but whose focus is not this scheme.
- Malware-focused analysis, which present the mechanisms used to deliver general or particular malware samples to a target.
- General techniques' description, which provide an analysis for well-known delivery techniques in a general context, typically a whole hostile operation, without delving into the delivery internals.

- Particular techniques analysis, which provide an in-depth dissection of specific techniques such as social engineering or phishing, or of particular elements such as malware.

In Table 1, a tabular comparative study featuring the main characteristics of the different analyzed approaches is shown.

Table 1. Comparative literature study.

Family	References	Pros	Cons
General models	[13,24–27]	Industry standards Specifications based on real attacks Useful for the identification of particular techniques in offensive operations	Plain structure Not an in-depth analysis Not designed for the identification of security gaps
Threat actors reports	[28–31]	Real world cases In-depth analysis for each case New delivery techniques are presented	Focus on specific delivery techniques No structure proposal
Initial classifications	[32,33]	Initial structure for techniques Real techniques mapping	Not focused on delivery, but general approaches Date of publication
Malware-focused	[26,34–36]	In-depth analysis for malware delivery Detection oriented Malware as a relevant threat	Focus on specific s: malware and malware related Not designed to identify security gaps outside malware ecosystem
General techniques	[37–48]	Delivery techniques analyzed with a global operation perspective: completeness Real world cases	No classification proposal Not in-depth analysis
Particular techniques	[49–57]	In-depth analysis of particular techniques Structure proposals for these techniques	Focus on particular techniques, without considering a global delivery scheme

5. Our Proposal

Initial access, or delivery, is just the compromise of the target security perimeter. This security perimeter is the boundary within security control measures, which are in effect to protect assets [58]. The compromise is always a break in from outside the target premises to inside them, no matter where the tactic is initiated from; please note that in our proposal, we identify inbound and outbound logical paths for delivery, but this classification refers only to the initial connection for a logical compromise, not to the whole tactic. To compromise the target perimeter, we identify three mandatory elements: an artifact, a transport vector from this artifact to the target's premises, and a path to break the perimeter. In this sense, in order to establish a taxonomy for delivery techniques, we provide the following definitions:

Delivery Object, is the object used to break the target's perimeter. This object is usually a deliverable artifact generated by a weaponizer, in which the malicious payload is embedded, typically in the form of an application data file such as Adobe Portable Document Format or Microsoft Office. However, our concept of object includes not only ad hoc, malicious artifacts, such as links or files, but also points out the infrastructure to be abused by hostile actors, such as public facing services.
Delivery Vector, is the transport used to deliver the artifact to its target. Examples of delivery vectors include USB memory drives, mail messages, hardware implants, or supply chains.
Delivery Path, is the way the delivery vector breaks the target's perimeter. Although in some cases this delivery path is directly linked to the delivery vector, in other cases they are independent, as we well analyze later in this work. Examples of delivery paths include both physical and logical routes to the target.

To achieve the delivery tactic, an object is used or abused by a threat actor, who delivers it to its target by a delivery vector and breaks the perimeter through a specific path. The path identifies which point is compromised, the vector identifies how it is compromised, and the object identifies what is used to achieve the compromise. For all of these three concepts, we propose a taxonomy based both on the characterization of the techniques and on the related countermeasures to prevent and to detect them. We have not identified any delivery technique that does not have all of these items, so we consider all of them as mandatory for a successful delivery.

The delivery object is divided into two types: dynamic and static objects. This proposed division reflects the techniques exposed by threat actors in the use of malicious artifacts and in the abuse of infrastructure features to achieve the Initial Access. Dynamic objects are those that contain a malicious payload that detonates when they are used or accessed in some form. We identify two sub types of dynamic objects: weaponized and not weaponized, depending whether the malicious payload is coupled with another object. The first ones are weaponized by the threat actor, for example in the form of a link or file (logical weaponization) or directly into removable media (physical weaponization), and sent to the target in order to exploit a local vulnerability or weakness when they are accessed. On the other hand, non-weaponized dynamic objects are directly launched against the target without a couple, usually to exploit a remote vulnerability or weakness in order to break the security perimeter. We consider especially relevant this division of dynamic objects, as weaponization or its absence is a key factor for the technique; weaponized objects are usually linked to operations in which the end user is deceived, as the couple hides the malicious payload, while non-weaponized objects are usually related to the exploitation of technical vulnerabilities. Moreover, the countermeasures to be applied in each case are different: when dealing with weaponized objects, where the target is a human, awareness is a must, but when dealing with non-weaponized objects, where the target is an infrastructure, the main countermeasures are related to technical vulnerability management.

Static objects are those that do not contain a malicious payload, but they are abused by the threat actor in order to break the security perimeter of its target. In this case, we also identify two sub types of static objects: those that pre-exists in a legitimate form in the target's infrastructure, with independence from the threat actor and those not legitimate, which are generated by the actor. The first ones are just abused by the threat actor in an operation against a target, facing as a legitimate user, and the second ones are ad hoc generated, in the form of backdoor, to provide the threat actor with a delivery, and in some cases an exploitation and a persistence or capability; this generation is typically performed by exploiting a particular vulnerability or weakness of the target. Again, this division is relevant for the identification of the used techniques: legit objects are pre-existing ones, just abused by a threat actor, and the detection of these techniques are usually based on anomaly patterns, while illegitimate objects are created by the exploitation of a vulnerability or weakness, and their detection is mostly based on misuse patterns.

Typical examples of static objects include external-facing accounts, both legit abused by the actor (pre-existing), and generated for the delivery.

Delivery object-proposed taxonomy is shown in Figure 2. As we have previously stated, these objects are used or abused by a threat actor to get initial access to its target. We can identify the two main families of delivery objects: dynamic and static. Inside both of them, we differentiate the specific types of objects that we have detailed in our work.

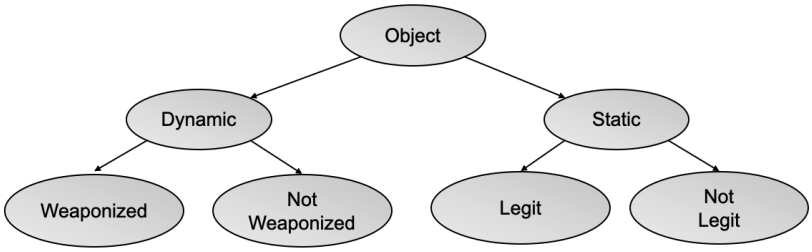

Figure 2. Delivery Objects' taxonomy.

Taking into account the delivery vector, we differentiate between those that compromise the target's infrastructure in first place and those that compromise a third party infrastructure to, as a second step, achieve the compromise of the target. This approach is linked to [32], in which Ping Chen et al. define direct and indirect delivery as a starting point for an initial classification, as stated before, and it is consistent with the identification of the first contact between the threat actor and its target. We define two sub types of direct vectors: those that are deliberate and those that are unintentional. In the first one, the threat actor abuses an insider from the target in order to use or abuse the delivery object. In unintentional delivery, the threat actor can abuse a non-malicious element in two ways: the syntactic (an actual vulnerability or weakness in the infrastructure) or semantic (a decoy to a user, for example in spear phishing attacks). Please note that syntactic or semantic refers only to the delivery, not to the exploitation: once delivered, a semantic attack can either exploit a vulnerability or not. This proposed division of direct delivery represents the main differences in the Initial Access techniques from the perspective of how the target is compromised, and provides an uncommonly in depth analyzed perspective: those of the insiders.

In indirect delivery, we find the compromise of trusted and untrusted third parties. A hostile actor can compromise an untrusted infrastructure that, indirectly, compromises the actual target on some interaction between them, typically through web navigation over a malicious web page. On the other hand, the compromise of a trusted third party and the exploiting of a trusted relationship with the actual target allow the threat actor to achieve delivery in a more concise way. This compromise of a trusted third party is usually in the form of compromise of a supply chain or in the compromise of a third party with an infrastructural trust point with the target. Please note that, from the compromised party's point of view, an indirect delivery vector must be seen as direct. The difference between trusted and untrusted parties is a key one, as a trusted party will have more available attack surface against the target than an untrusted one; thus, countermeasures against them must be more strict.

The delivery vectors' proposed taxonomy is shown in Figure 3. Those vectors represent the transport used to use or abuse the delivery object in order to get initial access to the target. These vectors can be exploited in their own target (Direct) or in a party which has some kind of relationship with the final target (Indirect). Both of them have particular vectors, and we consider especially relevant the deliberate vector, representing the use of insiders in a target organization that voluntarily provide initial access to a threat actor. These insiders are not generally considered in literature, as we will detail later in our work.

Finally, from the perspective of the delivery path, we identify two main views for an organization security perimeter: the logical and the physical view. The human fact is a key piece in security that has been largely analyzed [59–61], and some even works [62–64] define a human perimeter for organizations. However, we will focus on the logical and physical perimeters: although many delivery techniques, such as spear phishing, rely on human vulnerabilities, the delivery itself has to be performed, breaking a logical or a physical protection. Please note that the concept "perimeter" refers not only to the target's owned infrastructures, but also to the infrastructures related to the target and used while delivering, for example, to cloud services. So in this sense, we can define two main types of delivery path: the logical and the physical.

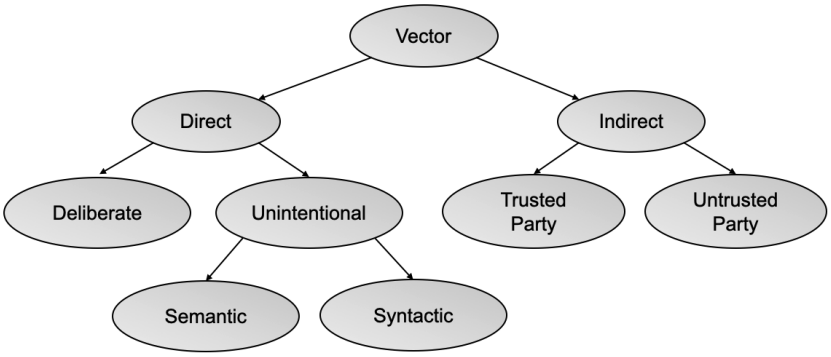

Figure 3. Delivery Vectors' taxonomy.

Inside the logical delivery path, we differentiate inbound and outbound paths, depending on from where the first malicious connection for the delivery is started. If this first connection is started from the organization's premises, such as in phishing techniques, we refer to the outbound logical path, while if it is started outside these premises, such as in the abuse of valid accounts, we refer to the inbound logical path. This distinction is specially relevant for our taxonomy, as it allows us to fine tune the identification of particular techniques and their identification, thus enabling organizations to establish better protection mechanisms against the threat. In both cases, it is mandatory to monitor external-facing systems to detect the compromise, but when dealing with inbound logical path techniques, the monitoring efforts must be directed to applications and services exposed to internet. If we deal with an outbound logical path, these monitoring efforts must be directed to the legit external services offered to their own organization.

Regarding the physical delivery path, we differentiate between connected and not connected approaches; in this case, a not connected physical delivery path is the one that breaks the physical security perimeter of the organization once, not connecting the delivery object to the target IT infrastructure. On the other hand, a connected physical delivery path represents a double security perimeter violation: the first one, the physical, gets into the target, and the second one, logical, connects the delivery object to the target infrastructure. Again, this difference is relevant for the identification of the particular technique used by a threat actor and thus for the identification and deployment of appropriate countermeasures. While dealing with connected approaches, in which we find a double perimeter compromise, it is possible to establish two layers of security countermeasures. On the other hand, in not connected approaches there is a single compromise, so from the perimeter's point of view only a checkpoint can be established, although other countermeasures, not specifically perimeter-related, can also be deployed, especially for the monitoring of the object activities in the target.

The full delivery path-proposed taxonomy is shown in Figure 4. As we have previously stated, the delivery path represents the compromised perimeter for the target, the physical and logical perimeters being the considered ones in our work. Inside both of them we identify the different approaches that detail this compromise, as these approaches allow analysts to detect known delivery techniques and to identify novel ones.

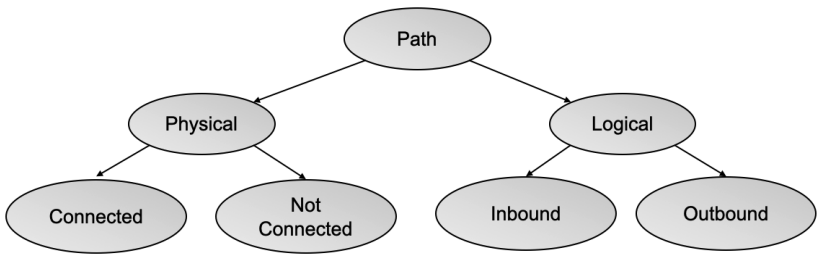

Figure 4. Delivery Paths' taxonomy.

By setting the object, the vector, and the path we can classify all delivery techniques into our taxonomy. These items provide a global view of the tactic, as they themselves define the delivery process: an object is sent through a specific vector to the target, physically or logically breaking its perimeter, to achieve the tactic goal. In Table 2, we summarize the proposed taxonomy.

Table 2. Proposed taxonomy for delivery techniques.

Object	Dynamic	Weaponized	
		Not Weaponized	
	Static	Legit	
		Not legit	
Vector	Direct	Deliberate	
		Unintentional	Syntactic
			Semantic
	Indirect	Trusted Party	
		Untrusted Party	
Path	Physical	Connected	
		Not Connected	
	Logical	Inbound	
		Outbound	

Following our proposed approach, we can classify all the delivery techniques and identify security gaps to establish countermeasures against them. We have selected two of the most widely used techniques for Initial Access, spear phishing, and the abuse of valid user accounts on external-facing infrastructure. We can classify them into the proposed categories for delivery object, vector, and path, as an example regarding how our proposed taxonomy can be applied.

Spear phishing is a particular type of phishing, in which the target and context are previously investigated so that the email is tailored to the receiver [65,66]. These actions are executed by sending a malicious object (typically a file or a link) by e-mail to a particular target [67]. This object is specially crafted to detonate when it is accessed by the receiver, who opens it as a legitimate e-mail; when it detonates, the malicious payload is executed and the threat actor can continue with further steps of the cyber-kill chain. Following our proposed taxonomy, this technique uses a weaponized dynamic object, is based on a semantic unintentional direct vector, and follows an outbound logical path.

Regarding the abuse of valid user accounts on external-facing infrastructure, in this case the threat actor just obtains valid credentials and abuses them to remotely access the targeted infrastructure. For example, these credentials can be guessed by brute force or obtained from a data leak. Once the threat actor gets these credentials, it has access to the infrastructure and can start the execution of the rest of the cyber-kill chain actions. In our taxonomy, this technique uses a legit static object, is based on a semantic unintentional direct vector and follows an inbound logical path.

5.1. Mapping to MITRE ATT&CK

As stated in this work, MITRE ATT&CK is the main public effort to establish a classification of TTP used by threat actors; for this reason, we have performed a mapping of the MITRE ATT&CK Enterprise "Initial Access" (the given name in the framework to the delivery) tactic onto our proposed structure.

At the time of this writing, MITRE ATT&CK Enterprise "Initial Access" tactic (last modified on 19 July 2019), identified as TA0001, consists of techniques that use various

entry vectors to gain an initial foothold within a network. Techniques used to gain a foothold include targeted spear phishing and exploiting weaknesses on public-facing web servers. Footholds gained through initial access may allow for continued access, such as valid accounts and the use of external remote services, or may be limited-use, due to changing passwords. For this particular tactic, MITRE ATT&CK identifies the techniques shown in Table 3.

Table 3. MITRE ATT&CK Initial Access techniques.

Technique ID	Name	Sub-Techniques
T1189	Drive-by Compromise	N/A
T1190	Exploit Public-Facing Application	N/A
T1133	External Remote Services	N/A
T1200	Hardware Additions	N/A
T1566	Phishing	- Spearphishing Attachment - Spearphishing Link - Spearphishing via Service
T1091	Replication Through Removable Media	N/A
T1195	Supply Chain Compromise	- Compromise Software Dependencies and Development Tools - Compromise Software Supply Chain - Compromise Hardware Supply Chain
T1199	Trusted Relationship	N/A
T1078	Valid Accounts	- Default Accounts - Domain Accounts - Local Accounts - Cloud Accounts

T1189, Drive-by Compromise, refers to the threat actor gaining access to a system through a user visiting a website over the normal course of browsing. In this technique, the object is a dynamic and weaponized; the vector is indirect, through an untrusted party; and the path is logical and outbound.

T1190, the Exploit Public-Facing Application, refers to the threat actor taking advantage of a weakness in an Internet-facing computer or program using software, data, or commands in order to cause unintended or unanticipated behavior. In this technique, the object is dynamic and not weaponized; the vector is direct, unintentional, and syntactic; and the path is logical and inbound.

T1133, External Remote Services, refers to the threat actor leveraging external-facing remote services to initially access and/or persist within a network. In this technique, the object is static and legit; the vector is direct, unintentional, and syntactic; and the path is logical and inbound.

T1200, Hardware Additions, refers to the threat actor introducing computer accessories, computers, or networking hardware into a system or network that can be used as a vector to gain access. In this technique, the object is static and legit; the vector is direct and unintentional; and the path is physical and connected.

T1566, Phishing, refers to the threat actor sending phishing messages to gain access to victim systems; all forms of phishing are electronically delivered social engineering. T1566 presents three sub-techniques, and in all of them the object is dynamic and weaponized; the vector is direct, unintentional, and semantic; and the path is logical and outbound.

T1091, Replication Through Removable Media, refers to the threat actor moving onto systems, possibly those on disconnected or air-gapped networks, by copying malware to

removable media and taking advantage of Autorun features when the media is inserted into a system and executed. In this technique, the object is dynamic and weaponized into removable media; the vector is direct and unintentional; and the Path is physical and connected.

T1195, Supply Chain Compromise, refers to the threat actor manipulating products or product delivery vectors prior to receipt by a final consumer for the purpose of data or system compromise. In this technique, the object can be dynamic or static, depending on how the supply chain is abused; the vector is indirect, through a trusted party; and the Path can be physical or connected (sub-technique T1195.003) or logical and inbound (sub-techniques T1195.001 and T1195.002). This a clear case where MITRE ATT&CK does not delve into the particularities of technique.

T1199, Trusted Relationship, refers to the threat actor breaching or otherwise leveraging organizations who have access to intended victims. In this technique, the object is static, as it does not contain malware for the delivery and legit, as exploited trusted relationships pre-exist in the infrastructure. The vector is indirect through a trusted party and the Path is logical and outbound. As in T1195, again MITRE ATT&CK does not provide enough information to delve into a more specific classification of this particular technique.

T1078, Valid Accounts, refers to the threat actor obtaining and abusing credentials of existing accounts as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion. In this technique, the object is static and legit in all of the sub-techniques exposed by MITRE ATT&CK; the vector is direct, unintentional, and syntactic; and the path is logical and inbound.

As we can see, all MITRE ATT&CK techniques for "Initial Access" can be mapped onto our taxonomy; this mapping is summarized in Table 4. If we analyze each of the elements from our taxonomy and their mapping to MITRE ATT&CK, we get interesting findings about the framework, especially those related to important gaps.

Table 4. MITRE ATT&CK techniques' classification by threat group.

Object (T1195)	Dynamic	Weaponized (T1189, T1566, T1091)	
		Non-Weaponized (T1190)	
	Static	Legit (T1078, T1199, T1133)	
		Not legit (T1200)	
Vector	Direct	Deliberate	
		Unintentional	Syntactic (T1190, T1133, T1200, T1091, T1078)
			Semantic (T1566)
	Indirect	Trusted Party (T1195, 1199)	
		Untrusted Party (T1189)	
Path	Physical	Connected (T1200, T1091, T1195.003)	
		Not Connected	
	Logical	Inbound (T1190, T1133, T1195.001, T1195.002, T1078)	
		Outbound (T1189, T1566, T1199)	

Regarding the delivery object, all techniques but one are classified into low-level nodes. The technique in upper nodes is T1195, Supply Chain compromise. MITRE ATT&CK does not provide enough information for its fine classification, although it is becoming a commonly used technique and the framework defines three particular sub techniques inside it. In fact, supply chain attacks increased in number and sophistication in the year 2020 and this trend has continued in 2021, posing an increasing risk for organization [68–70]. Therefore, the number of published research works related to supply chain cyber security

is increasing in last years, especial since COVID-19 pandemic [71,72]. We find it mandatory to provide a more exhaustive analysis of this technique from the perspective of the delivery object, identifying the different approaches through static and dynamic objects that this technique can be executed with. This analysis would provide organizations better countermeasures to prevent, detect and neutralize supply chain attacks.

Regarding the delivery vector, all techniques are classified into low-level nodes. In this case we find an important gap; as MITRE ATT&CK does not consider deliberate delivery, this is the abuse of an insider from the target organization voluntary helping the hostile actor to achieve its goals. Although not usually considered when dealing with delivery, the insider threat has been a relevant problem for years; thus, we find it mandatory to identify delivery techniques (including the human aspects) for this threat. Dealing with the delivery vector, it is also interesting that phishing, being the most-used delivery technique, is the only one identified as semantic, as most techniques are classified as syntactic. The framework should delve into semantic delivery vectors, as people have always been the weakest link in the security chain and there are different delivery techniques that benefit from social engineering, as we have discussed in Section 6.

Finally, regarding the delivery path, MITRE ATT&CK identifies delivery techniques both for a physical and a logical compromise, although most of the delivery techniques analyzed from hostile actors reports are based on a logical delivery. We must highlight the fact that the not connected physical delivery path has no linked techniques; this means that these kinds of delivery approaches are not considered in MITRE ATT&CK; thus, most defensive teams are also not considering them in their security countermeasures. The framework should delve into different techniques to physically break the security perimeter of an organization and deploy an autonomous, not connected implant.

If we delve into the particular delivery techniques that threat actors are performing, the data from MITRE ATT&CK allows the linking between groups and techniques. In Table 5, this relationship is shown, exposing the number of threat groups using each initial access technique or sub technique.

Table 5. Delivery techniques exploited by threat actors.

Technique ID	Name	Number of Groups
T1189	Drive-by Compromise	24
T1190	Exploit Public-Facing Application	16
T1133	External Remote Services	20
T1200	Hardware Additions	1
T1566.001	Spear phishing Attachment	64
T1566.002	Spear phishing Link	34
T1566.003	Spear phishing via Service	7
T1091	Replication Through Removable Media	4
T1195.001	Compromise Software Dependencies and Development Tools	0
T1195.002	Compromise Software Supply Chain	6
T1195.003	Compromise Hardware Supply Chain	0
T1199	Trusted Relationship	5
T1078.001	Valid Accounts: Default	0
T1078.002	Valid Accounts: Domain	10
T1078.003	Valid Accounts: Local	8
T1078.004	Valid Accounts: Cloud	2

Please note that a single threat group can be executing more than one initial access technique, and also that those techniques or sub-techniques with zero groups mean only that they have been observed in real operations but attribution has not been possible. With this information, we can conclude that different spear phishing techniques are the most widely used, while supply chain compromises can be only performed by specific threat actors; particularly, no identified threat actor is able to compromise the hardware or dependencies and developmental tool supply chains, although MITRE ATT&CK identifies these techniques as the ones used to gain initial access. Of course these results are consistent with the findings we have exposed in our paper, related to phishing as a key delivery technique and supply chain compromise as a growing trend. As we have previously performed with MITRE ATT&CK techniques, we can map the number of groups performing each technique onto our taxonomy, as shown in Table 6.

Table 6. MITRE ATT&CK groups classification.

Object (6)	Dynamic	Weaponized (133)	
		Non-Weaponized (16)	
	Static	Legit (45)	
		Not legit (1)	
Vector	Direct	Deliberate	
		Unintentional	Syntactic (61)
			Semantic (105)
	Indirect	Trusted Party (11)	
		Untrusted Party (24)	
Path	Physical	Connected (5)	
		Not Connected	
	Logical	Inbound (62)	
		Outbound (134)	

Regarding the delivery object, most groups are able to use techniques based on weaponized objects in order to gain initial access to their targets. Only one of them is able to gain access through not legit objects, in this case, through hardware additions. These data show the importance of protecting organizations against malware coupled with legitimate objects, as the techniques relying on weaponized objects are the most-used ones. This protection can be achieved through perimeter security elements such as web traffic inspection devices or sandboxes for mail attachments or links. While all delivery techniques are important, the probability of being compromised through Weaponized Objects is much higher than the probability of being compromised through a hardware addition; therefore, on a prior basis most organizations must allocate more resources to protect themselves against a malware compromise than to protect themselves against a hardware addition or a supply chain compromise. Finally, it is important to note that only six groups are able to execute different techniques based on undefined delivery objects, all of them through supply chain compromises. As we have stated in this paper, these compromises are not widely exploited, but supply chain attacks are a growing trend.

Regarding the delivery vector, Semantic delivery is the most widely used vector. This implies that most groups exploit social engineering techniques to gain access to the target infrastructure, a fact that highlights the importance of security awareness for most organizations. The use of untrusted parties to gain access to the target is also relevant. Threat actors rely on the trojanization of web sites visited by the users of the targeted organization to gain access to their victims. Although this technique can be considered a non-directed one (there is no guarantee about who is visiting the trojanized web site),

advanced threat actors analyze their targets and identify the sites those targets will visit with high probability. This fact again highlights the special relevance of the security countermeasures that must be implemented in order to protect navigation traffic. Finally, the fact that no threat group is identified as being able to exploit Deliberate delivery, that is, that no threat group is exploiting insiders to gain access to a target, is especially relevant

Finally, regarding the delivery path, most initial access is gained through a logical delivery. As physical delivery is usually harder to exploit, most threat actors focus on logical paths to gain access to their targets. The protection of the logical perimeter, both of inbound and outbound connections, is highlighted once again. Finally, as we have previously stated, no threat group is identified to be able to exploit not connected delivery paths. As few countermeasures will be implemented to protect this kind of compromise, this fact leaves a potential window of opportunity for threat actors.

5.2. A Practical Example

In this section we provide a practical example for our proposed taxonomy and its usefulness. For this case study, we have chosen the supply chain compromise delivery technique. As we have previously stated, supply chain compromise is a growing trend in advanced hostile operations; thus, it is mandatory to design and implement security countermeasures to face this technique.

In order to protect an organization against supply chain techniques, the first step is to understand how they are implemented by threat actors. MITRE ATT&CK being the main framework for tactics and techniques, it is the first reference to analyze supply chain compromises. As we have stated, this framework provides three sub-techniques, two of them regarding software supply chain compromises and the last one regarding hardware supply chain compromises. With a main focus on software-related compromises, hardware supply chain attacks are in the background. This is consistent with an in-depth literature review, where most research is focusing nowadays on software supply chain attacks, that is, on the compromise of the software delivered to the target, both commercial [73] and open source [74]. On the other hand, hardware supply chain is, in general terms, less considered. The hardware supply chain security is analyzed and modeled in [75]. Hardware implants in supply chain attacks are analyzed in works such as [76], where the authors focus on the security of electronic devices, or [77], where Jacob Harrison et al. provide a review of Printed Circuit Boards' malicious hardware implants through the supply chain.

This initial literature review, whose aim is to identify the security countermeasures to be implemented in order to protect an organization, presents two main problems that can lead organizations to leave relevant security gaps that can be exploited by advanced threats. The first problem is related to the focus on software supply chain attacks. These compromises are the more common ones, as hardware compromises usually require much more effort, human and economic, and their scope is limited to a reduced group of targets. Different Advanced Persistent Threat groups, such as APT29 or Sandworm, are able to compromise the software supply chain, while the groups with hardware compromise capabilities are less common. However, hardware supply chain compromises are still a relevant threat to organizations; thus, they must be conveniently considered when designing and implementing a protection plan.

The second problem is related to the hardware versus software approach. This distinction is too simple in some cases and it usually refers to the way an artifact is delivered to the target, without considering other elements. In our proposed taxonomy, it focuses only on the delivery path. By adopting this simple hardware or software consideration, without evaluating other elements of the compromise, relevant protection gaps can be left by a security team.

To face these common problems, our proposed taxonomy helps defensive teams to cover security gaps by considering uncommon delivery approaches. In addition, our taxonomy also allows the identification of novel techniques, in order to evaluate their likelihood and impact and, if applicable, to establish countermeasures to face them. Regarding supply

chain compromises as a delivery technique, our taxonomy considers not only the delivery path point of view, but also the vector and the object. If we map supply chain related techniques onto our proposed taxonomy, both the ones defined in MITRE ATT&CK and unusual techniques identified in the literature review, we can find gaps that can lead to security breaches through a supply chain compromise.

In relation to the Path, as we have stated, supply chain techniques are mostly linked to software and hardware delivery, not considering situations such as:

- The mix of both approaches: the delivery of trojanized software through physical means, for example, through any removable media. This delivery technique is identified in our taxonomy, and it is a key threat to be considered in air-gapped networks, where software is installed or updated through physical media.
- The physical delivery of a trojanized element that is not directly connected to the target infrastructure, for example, a device to remotely listen to a conversation.

If these supply chain delivery techniques are not considered in a threat model, defensive teams will not be able to identify and establish appropriate countermeasures. Through the dissection of the delivery technique and the identification of its components, our taxonomy includes all the relevant elements to identify these approaches to the delivery.

In relation to the delivery vector, all supply chain compromises are Indirect, by their own definition. The abuse of untrusted parties is not usually considered in the literature, as major well-known supply chain attacks, such as SolarWinds [73,78] or Kaseya [79] are based on a trusted party to compromise their final target. Hostile actors took advantage of this gap in 2021, as most organizations are not aware of these attacks. For example, the Lazarus group have developed techniques to compromise its targets through the trojanization of general-purpose software available on Internet [80]. This advanced threat actor is able to download the malicious software to the target infrastructure through social engineering techniques, thus successfully developing a supply chain compromise approach through untrusted parties. This approach, observed in 2021, would have been considered by applying our proposed taxonomy, as it identifies not only trusted Parties but also untrusted ones as indirect delivery vectors.

Finally, regarding the delivery object, none of the works we have analyzed focuse on the relevance of this element for supply chain delivery techniques. In fact, the MITRE ATT&CK framework does not provide enough detail for their exposed supply chain techniques to map them onto relevant categories of our taxonomy. This lack of analysis can result in security gaps for an organization. All supply chain compromises are based on the manipulation of the delivered product at any stage of the chain. However, the type of manipulation is relevant for its detection. For example, a trojanization through dynamic objects can be detected by malware analysis, while a trojanization through a static object would not be detected by that analysis, and would require a hardening check. If the object is not considered, organizations cannot identify and implement appropriate security countermeasures to detect supply chain compromises. Our taxonomy, in this case the delivery object, allows analysts to identify different types of manipulation and to deploy the relevant countermeasures in each case to face them.

In this practical example, we have applied our proposed taxonomy to the identification of novel and uncommon supply chain delivery techniques. We have shown how our work helps analysts to establish a model for delivery techniques that allows them to anticipate in hostile operations through the analysis of the delivery object, vector, and path. In this way, cyber security levels can be increased and global protection for an organization is enhanced. Although we have focused on a supply chain compromise, our findings and proposed taxonomy can be applied to all kind of delivery techniques used by advanced threat actors.

6. Discussion

In order to provide an initial taxonomy for delivery techniques, we have analyzed the different existing approaches to accomplish the Initial Access tactic performed by

advanced threat actors. In this analysis, one major finding is that voluntary delivery is not considered among the analyzed techniques. A deeper classification for deliberate actions is processed in different works regarding the insider threat [81–86], although such a fine structure is outside the scope of this paper. Being a MITRE ATT&CK, the commonly accepted framework for tactics, techniques, and procedures, we consider that it should identify such approaches for a deliberate initial access, thus providing mechanisms to mitigate these techniques.

A major finding during our research is that different well-known delivery techniques are not considered in current frameworks. This gap between currently used delivery techniques and those identified in key references, such as the MITRE ATT&CK, which is a primary source for security analysts, may lead to an opportunity window for threat actors, as defensive teams are not considering some hostile approaches; thus, they are not implementing countermeasures against them. In this sense, we consider our taxonomy to help analysts identify those lacking techniques that can be executed by threat actors, thus helping organizations to identify appropriate countermeasures against them.

In addition, also regarding this framework, we have identified an important lack of formal structure in MITRE ATT&CK techniques for different particular tactics. This framework being the main effort and the de facto standard to identify and analyze tactics and techniques from advanced threat actors, we consider that it should define a taxonomy, or at least a classification, for the identified techniques in each case, thus providing analysts more concise information about them and increasing defensive capabilities to prevent, detect, and neutralize threats. This work will be shared with MITRE in order to be considered to enhance the ATT&CK framework.

As identified research lines, we propose, in the first place, a deeper analysis of supply chain compromises as a key delivery vector. As we have stated before, supply chain attacks are not the most widely used technique, but their popularity among threat actors is increasing and their impact is high. We have provided a practical example to improve the identification and detection of supply chain compromises through our proposed taxonomy, but of course more research has to be performed. Refs. [46,87] provide a framework and catalog of supply chain attack patterns identifying objects of the compromise, types, time frames, and, as a key element, points of attack within the supply chain. Ref. [88] proposes a threat model for supply chain attacks, and ref. [89] provides a threat analysis for these attacks. Much work has been performed in this line, but most of it is focused on the analysis of particular approaches, lacking a formalization and with an abstract, technology-agnostic structure for their classification. This kind of analysis should improve an organization security by providing a deeper knowledge about supply-chain-based initial access, thus enabling appropriate countermeasures against these kinds of hostile actions, so we miss a deeper work from this perspective.

As we have stated, another research line we identify is the analysis of the deliberate human factor in offensive operations; when dealing with advanced actors, they have capabilities to employ not only technological approaches for an initial access or for other tactics, but also to use insiders to achieve their goals. and a relevant challenge is to determine if an action delivered by an insider is a justifiable threat [90]. The detection of these internal hostile actors is mandatory in order to provide an adequate level of protection. Although in classical security the insider threat has been well studied over the years, we consider that these analysis must be carried to cyber operations, following a kill-chain approach [91,92], where the mix of people and technology can lead to a high impact for an organization.

Finally, we identify a third research line related to the application of computational intelligence to the identification and classification of delivery techniques. Our taxonomy can be used as a general classification scheme and can help analysts to select relevant features to model delivery techniques. With these features, main computational intelligence approaches can be exploited to identify and classify techniques. Fuzzy logic systems or neural networks have been successfully applied in many different fields, such as fault

detection [93–95] or smart cities [96,97]. Related to delivery techniques, the role of fuzzy logic in supply chain management [98,99], resilience [100,101], or risk assessment [102,103] are relevant research fields.

7. Conclusions

Our work provides an initial taxonomy for delivery techniques in order to better understand the global tactic and to protect organizations against threat actors achieving initial access into a target. Delivery is a key tactic for advanced threat operations; part of the global success of an offensive operation relies on the correct achievement of the delivery, as it is the first stage of the operation in which the threat actor interacts with its target in a hostile way. For this reason, an accurate classification and structure for the techniques linked to the delivery tactic is a must in order to identify capabilities, to profile advanced actors, and to develop, implement, and maintain security countermeasures against them. However, we have identified an absence of a suitable classification scheme for the techniques related to the delivery stage in hostile cyber operations by advanced threat actors. Even MITRE ATT&CK, the key reference in the subject, lacks a suitable approach to classify the different techniques inside the delivery tactic. As this tactic is mandatory in all kind of offensive operations, we consider it especially relevant to establish a suitable taxonomy for it, thus helping organizations to better understand this stage and enhancing their prevention, detection, and neutralization capabilities.

In this work, we have delved into how the delivery tactic is achieved. To establish such a taxonomy, we have dissected the tactic as a way to model it. We identify the different elements that define the delivery and we deploy them into a classification that provides this taxonomy. As stated before, as the MITRE ATT&CK is considered the key reference for tactics and techniques used by threat actors, we have aligned our approach with this framework and classified all the identified techniques into our proposed taxonomy. We consider our work to significantly contribute to improving, not only the threat model for hostile advanced actors, but also the detail organizations must consider for a suitable protection against them, in this case against the delivery tactic.

Tactics and techniques are one of the first key points to model advanced threat actors and to deploy capabilities in order to prevent, to detect, and to neutralize them. We consider our proposal as a starting point towards a commonly accepted taxonomy that helps research to better understand hostile actors, especially advanced ones. In future works, our proposal can be fine tuned to provide a more accurate approach to the Initial Access performed by advanced threat actors; we consider that all improvements must be aligned with industry standards, such as MITRE ATT&CK, in order to be useful to the security community. In addition, in this paper we have identified key research lines regarding delivery techniques whose relevance is growing or, is direct, which is not considered in main frameworks.

In this sense, we miss in main frameworks, such as MITRE ATT&CK, a deeper analysis of delivery techniques in three directions: supply chain attacks, as growing threats; deliberate delivery techniques, especially those regarding an insider; and physical perimeter breaking, with no further connection to the target infrastructure.

Author Contributions: Writing—original draft, A.V.-H., I.R.-R. and H.M.-G. 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.

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

References

1. Monte, M. *Network Attacks and Exploitation: A Framework*; John Wiley and Sons: Hoboken, NJ, USA, 2015.
2. Sood, A.K.; Enbody, R.J. Targeted cyberattacks: A superset of advanced persistent threats. *IEEE Secur. Priv.* **2012**, *11*, 54–61.
3. Yadav, T.; Rao, A.M. Technical aspects of cyber kill chain. In Proceedings of the International Symposium on Security in Computing and Communication, Kochi, India, 10–13 August 2015; pp. 438–452.
4. Strom, B.E.; Battaglia, J.A.; Kemmerer, M.S.; Kupersanin, W.; Miller, D.P.; Wampler, C.; Whitley, S.M.; Wolf, R.D. *Finding Cyber Threats with ATT&CK™-Based Analytics*; Technical Report; MITRE Technical Report MTR170202; The MITRE Corporation: McLean, VA, USA, 2017.
5. Xiong, W.; Legrand, E.; Åberg, O.; Lagerström, R. Cyber security threat modeling based on the MITRE Enterprise ATT&CK Matrix. *Softw. Syst. Model.* **2022**, *21*, 157–177.
6. Al-Shaer, R.; Spring, J.M.; Christou, E. Learning the associations of mitre ATT&CK adversarial techniques. In Proceedings of the 2020 IEEE Conference on Communications and Network Security (CNS), Avignon, France, 29 June–1 July 2020; pp. 1–9.
7. 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.
8. Garba, F.A.; Junaidu, S.B.; Ahmad, I.; Tekanyi, M. Proposed Framework for Effective Detection and Prediction of Advanced Persistent Threats Based on the Cyber Kill Chain. *Sci. Pract. Cyber Secur. J.* **2018**, *3*, 1–11.
9. Myers, L. The Practicality of the Cyber Kill Chain Approach to Security. CSO Online. 2013. Available online: https://www.computerworld.com/article/2485687/the-practicality-of-the-cyber-kill-chain-approach-to-security.html (accessed on 1 December 2021).
10. Zeng, W.; Germanos, V. Modelling Hybrid Cyber Kill Chain. In Proceedings of the International Workshop on Petri Nets and Software Engineering, Aachen, Germany, 23–28 June 2019.
11. Laliberte, M. A Twist on The Cyber Kill Chain: Defending against a JavaScript Malware Attack. *Dark Read.* **2017**. Available online: https://www.darkreading.com/attacks-breaches/a-twist-on-the-cyber-kill-chain-defending-against-a-javascript-malware-attack (accessed on 4 December 2021).
12. Bryant, B.D.; Saiedian, H. A novel kill-chain framework for remote security log analysis with SIEM software. *Comput. Secur.* **2017**, *67*, 198–210. [CrossRef]
13. Pols, P. *The Unified Kill Chain: Designing a Unified Kill Chain for Analyzing, Comparing and Defending against Cyber Attacks*; Technical Report; Cyber Security Academy: The Hague, The Netherlands, 2017.
14. Hahn, A.; Thomas, R.K.; Lozano, I.; Cardenas, A. A multi-layered and kill-chain based security analysis framework for cyber-physical systems. *Int. J. Crit. Infrastruct. Prot.* **2015**, *11*, 39–50. [CrossRef]
15. Case, D.U. Analysis of the cyber attack on the Ukrainian power grid. *Electr. Inf. Shar. Anal. Cent. (E-ISAC)* **2016**, *388*, 1–23.
16. Zhou, X.; Xu, Z.; Wang, L.; Chen, K.; Chen, C.; Zhang, W. Kill chain for industrial control system. In Proceedings of the MATEC Web of Conferences, EDP Sciences, Nanjing, China, 24–26 May 2018; Volume 173, p. 01013.
17. Lu, K.C.; Liu, I.H.; Li, J.S. A Survey of the Offensive and defensive in Industrial Control System. *Bull. Netw. Comput. Syst. Softw.* **2022**, *11*, 1–6.
18. Skormin, V.A.; Summerville, D.H.; Moronski, J.S. Detecting Malicious Codes by the Presence of Their "Gene of Self-replication". In Proceedings of the International Workshop on Mathematical Methods, Models, and Architectures for Computer Network Security, St. Petersburg, Russia, 21–23 September 2003; pp. 195–205.
19. Dornhackl, H.; Kadletz, K.; Luh, R.; Tavolato, P. Malicious behavior patterns. In Proceedings of the 2014 IEEE 8th international symposium on service oriented system engineering, Oxford, UK, 7–11 April 2014; pp. 384–389.
20. Chakkaravarthy, S.S.; Sangeetha, D.; Vaidehi, V. A survey on malware analysis and mitigation techniques. *Comput. Sci. Rev.* **2019**, *32*, 1–23. [CrossRef]
21. Provos, N.; Mavrommatis, P.; Rajab, M.A.; Monrose, F. All Your IFRAMEs Point to Us. In *Proceedings of the 17th Conference on Security Symposium (SS'08)*; USENIX Association: San Jose, CA, USA, 2008; pp. 1–15.
22. Kwon, B.J.; Srinivas, V.; Deshpande, A.; Dumitraş, T. Catching worms, trojan horses and pups: Unsupervised detection of silent delivery campaigns. *arXiv* **2016**, arXiv:1611.02787.
23. Takey, Y.S.; Tatikayala, S.G.; Samavedam, S.S.; Eswari, P.L.; Patil, M.U. Real Time early Multi Stage Attack Detection. In Proceedings of the 2021 7th International Conference on Advanced Computing and Communication Systems (ICACCS), Coimbatore, India, 19–20 March 2021; Volume 1, pp. 283–290.
24. Assante, M.J.; Lee, R.M. The industrial control system cyber kill chain. *SANS Inst. InfoSec Read. Room* **2015**, *1*. Available online: https://sansorg.egnyte.com/dl/HHa9fCekmc (accessed on 29 November 2021).
25. Bahrami, P.N.; Dehghantanha, A.; Dargahi, T.; Parizi, R.M.; Choo, K.K.R.; Javadi, H.H. Cyber kill chain-based taxonomy of advanced persistent threat actors: Analogy of tactics, techniques, and procedures. *J. Inf. Process. Syst.* **2019**, *15*, 865–889.
26. Dargahi, T.; Dehghantanha, A.; Bahrami, P.N.; Conti, M.; Bianchi, G.; Benedetto, L. A Cyber-Kill-Chain based taxonomy of crypto-ransomware features. *J. Comput. Virol. Hacking Tech.* **2019**, *15*, 277–305. [CrossRef]
27. Mirza, Q.K.A.; Brown, M.; Halling, O.; Shand, L.; Alam, A. Ransomware Analysis using Cyber Kill Chain. In Proceedings of the 2021 8th International Conference on Future Internet of Things and Cloud (FiCloud), Rome, Italy, 23–25 August 2021; pp. 58–65.
28. Bere, M.; Bhunu-Shava, F.; Gamundani, A.; Nhamu, I. How advanced persistent threats exploit humans. *Int. J. Comput. Sci. Issues (IJCSI)* **2015**, *12*, 170.

29. Ussath, M.; Jaeger, D.; Cheng, F.; Meinel, C. Advanced persistent threats: Behind the scenes. In Proceedings of the 2016 Annual Conference on Information Science and Systems (CISS), Princeton, NJ, USA, 16–18 March 2016; pp. 181–186.
30. Nelson, T.; Kettani, H. Open Source PowerShell-Written Post Exploitation Frameworks Used by Cyber Espionage Groups. In Proceedings of the 2020 3rd International Conference on Information and Computer Technologies (ICICT), San Jose, CA, USA, 9–12 March 2020; pp. 451–456.
31. Quintero-Bonilla, S.; Martín del Rey, A. A new proposal on the advanced persistent threat: A survey. *Appl. Sci.* **2020**, *10*, 3874. [CrossRef]
32. Chen, P.; Desmet, L.; Huygens, C. A study on advanced persistent threats. In Proceedings of the IFIP International Conference on Communications and Multimedia Security, Aveiro, Portugal, 25–26 September 2014; pp. 63–72.
33. Siddiqi, M.A.; Ghani, N. Critical analysis on advanced persistent threats. *Int. J. Comput. Appl.* **2016**, *141*, 46–50.
34. Zhu, Z.; Dumitras, T. Chainsmith: Automatically learning the semantics of malicious campaigns by mining threat intelligence reports. In Proceedings of the 2018 IEEE European Symposium on Security and Privacy (EuroS&P), London, UK, 24–26 April 2018; pp. 458–472.
35. Gangwar, K.; Mohanty, S.; Mohapatra, A. Analysis and detection of ransomware through its delivery methods. In Proceedings of the International Conference on Recent Developments in Science, Engineering and Technology, Gurgaon, India, 13 October 2017; pp. 353–362.
36. Raunak, P.; Krishnan, P. Network detection of ransomware delivered by exploit kit. *ARPN J. Eng. Appl. Sci.* **2017**, *12*, 3885–3889.
37. Beckers, K.; Krautsevich, L.; Yautsiukhin, A. Analysis of social engineering threats with attack graphs. In *Data Privacy Management, Autonomous Spontaneous Security, and Security Assurance*; Springer: Berlin/Heidelberg, Germany, 2014; pp. 216–232.
38. Jakobsson, M. Modeling and preventing phishing attacks. In Proceedings of the Financial Cryptography, Roseau, Dominica, 28 February–3 March 2005; Volume 5.
39. Foozy, C.F.M.; Ahmad, R.; Abdollah, M.F. Phishing detection taxonomy for mobile device. *Int. J. Comput. Sci. Issues (IJCSI)* **2013**, *10*, 338–344.
40. Lacey, D.; Salmon, P.; Glancy, P. Taking the bait: A systems analysis of phishing attacks. *Procedia Manuf.* **2015**, *3*, 1109–1116. [CrossRef]
41. Särökaari, N. Phishing Attacks and Mitigation Tactics. Ph.D. Thesis, University of Jyväskylä, Jyväskylä, Finland, 2020.
42. Krithika, N. A Study On WHA (Watering Hole Attack)–The Most Dangerous Threat To The Organisation. *Int. J. Innov. Sci. Eng. Res. (IJISER)* **2017**, *4*, 196–198.
43. Subburaj, T.; Suthendran, K. DigitalWatering Hole Attack Detection Using Sequential Pattern. *J. Cyber Secur. Mobil.* **2018**, *7*, 1–12. [CrossRef]
44. Bowen, B.M.; Hershkop, S.; Keromytis, A.D.; Stolfo, S.J. Baiting inside attackers using decoy documents. In Proceedings of the International Conference on Security and Privacy in Communication Systems, Turin, Italy, 3–5 June 2009; pp. 51–70.
45. Chetioui, K.; Bah, B.; Alami, A.O.; Bahnasse, A. Overview of Social Engineering Attacks on Social Networks. *Procedia Comput. Sci.* **2022**, *198*, 656–661. [CrossRef]
46. Reed, M.; Miller, J.F.; Popick, P. *Supply chain attack patterns: Framework and Catalog*; Office of the Deputy Assistant Secretary of Defense for Systems Engineering: Washington, DC, USA, 2014.
47. Coufalíková, A.; Klaban, I.; Šlajs, T. Complex strategy against supply chain attacks. In Proceedings of the 2021 International Conference on Military Technologies (ICMT), Brno, Czech Republic, 8–11 June 2021; pp. 1–5.
48. Yeboah-Ofori, A.; Ismail, U.M.; Swidurski, T.; Opoku-Boateng, F. Cyberattack ontology: A knowledge representation for cyber supply chain security. In Proceedings of the 2021 International Conference on Computing, Computational Modelling and Applications (ICCMA), Brest, France, 14–16 July 2021; pp. 65–70.
49. Ivaturi, K.; Janczewski, L. A taxonomy for social engineering attacks. In Proceedings of the International Conference on Information Resources Management, Centre for Information Technology, Organizations, and People, Shenzhen, China, 26–27 November 2011; pp. 1–12.
50. Krombholz, K.; Hobel, H.; Huber, M.; Weippl, E. Advanced social engineering attacks. *J. Inf. Secur. Appl.* **2015**, *22*, 113–122. [CrossRef]
51. Heartfield, R.; Loukas, G. A taxonomy of attacks and a survey of defence mechanisms for semantic social engineering attacks. *ACM Comput. Surv. (CSUR)* **2015**, *48*, 1–39. [CrossRef]
52. Aldawood, H.; Skinner, G. An Advanced Taxonomy for Social Engineering Attacks. *Int. J. Comput. Appl.* **2020**, *177*, 1–11. [CrossRef]
53. Fan, W.; Lwakatare, K.; Rong, R. Social engineering: IE based model of human weakness for attack and defense investigations. *Int. J. Comput. Netw. Inf. Secur.* **2017**, *9*, 1–11. [CrossRef]
54. Salahdine, F.; Kaabouch, N. Social engineering attacks: A survey. *Future Internet* **2019**, *11*, 89. [CrossRef]
55. Chaudhry, J.A.; Rittenhouse, R.G. Phishing: Classification and countermeasures. In Proceedings of the 2015 7th International Conference on Multimedia, Computer Graphics and Broadcasting (MulGraB), Jeju, Korea, 25–28 November 2015; pp. 28–31.
56. Rastenis, J.; Ramanauskaitė, S.; Janulevičius, J.; Čenys, A.; Slotkienė, A.; Pakrijauskas, K. E-mail-based phishing attack taxonomy. *Appl. Sci.* **2020**, *10*, 2363. [CrossRef]
57. Varshney, G.; Misra, M.; Atrey, P.K. A survey and classification of web phishing detection schemes. *Secur. Commun. Netw.* **2016**, *9*, 6266–6284. [CrossRef]

58. Adeka, M.I. Cryptography and Computer Communications Security. Extending the Human Security Perimeter through a Web of Trust. Ph.D. Thesis, University of Bradford, Bradford, UK, 2015.
59. Colwill, C. Human factors in information security: The insider threat–Who can you trust these days? *Inf. Secur. Tech. Rep.* **2009**, *14*, 186–196. [CrossRef]
60. Ani, U.D.; He, H.; Tiwari, A. Human factor security: Evaluating the cybersecurity capacity of the industrial workforce. *J. Syst. Inf. Technol.* **2019**, *21*, 2–35. [CrossRef]
61. Gozon, F.Z.; Vaczi, D.; Toth-Laufer, E. Fuzzy-based Human Factor Centered Cybersecurity Risk Assessment. In Proceedings of the 2021 IEEE 19th International Symposium on Intelligent Systems and Informatics (SISY), Subotica, Serbia, 16–18 September 2021; pp. 83–88.
62. Van Vuuren, I.E. IT security trust model-securing the human perimeter. *Int. J. Soc. Sci. Humanit.* **2016**, *6*, 852. [CrossRef]
63. Astakhova, L.; Medvedev, I. An Information Tool for Increasing the Resistance of Employees of an Organization to Social Engineering Attacks. *Sci. Tech. Inf. Process.* **2021**, *48*, 15–20. [CrossRef]
64. Subramanian, R.K.; Kumar Kattumannil, D. ERRM Gap Analysis & Identification. In *Event-and Data-Centric Enterprise Risk-Adjusted Return Management*; Springer: Berlin/Heidelberg, Germany, 2022; pp. 205–283.
65. Bullee, J.W.; Montoya, L.; Junger, M.; Hartel, P. Spear phishing in organisations explained. *Inf. Comput. Secur.* **2017**, *25*, 593–613. [CrossRef]
66. Rendall, K.; Nisioti, A.; Mylonas, A. Towards a multi-layered phishing detection. *Sensors* **2020**, *20*, 4540. [CrossRef]
67. Parmar, B. Protecting against spear-phishing. *Comput. Fraud Secur.* **2012**, *2012*, 8–11. [CrossRef]
68. *Threat Landscape for Supply Chain Attacks*; Technical Report; European Union Agency for Cybersecurity (ENISA): Athens, Greece, 2021.
69. Collier, Z.A.; Sarkis, J. The zero trust supply chain: Managing supply chain risk in the absence of trust. *Int. J. Prod. Res.* **2021**, *59*, 3430–3445. [CrossRef]
70. Al-Amin, S.; Sharkar, S.R.; Kaiser, M.S.; Biswas, M. Towards a blockchain-based supply chain management for e-agro business system. In Proceedings of the International Conference on Trends in Computational and Cognitive Engineering, Online, 21–22 October 2021; pp. 329–339.
71. Latif, M.N.A.; Aziz, N.A.A.; Hussin, N.S.N.; Aziz, Z.A. Cyber security in supply chain management: A systematic review. *LogForum* **2021**, *17*, 49–57. [CrossRef]
72. Novoszel, L.; Wakolbinger, T. Meta-analysis of Supply Chain Disruption Research. In *Proceedings of the Operations Research Forum*; Springer: Berlin/Heidelberg, Germany; Volume 3, pp. 1–25.
73. Peisert, S.; Schneier, B.; Okhravi, H.; Massacci, F.; Benzel, T.; Landwehr, C.; Mannan, M.; Mirkovic, J.; Prakash, A.; Michael, J.B. Perspectives on the SolarWinds incident. *IEEE Secur. Priv.* **2021**, *19*, 7–13. [CrossRef]
74. Ohm, M.; Plate, H.; Sykosch, A.; Meier, M. Backstabber's knife collection: A review of open source software supply chain attacks. In Proceedings of the International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment, Lisbon, Portugal, 24–26 June 2020; pp. 23–43.
75. Halak, B. Cist: A threat modelling approach for hardware supply chain security. In *Hardware Supply Chain Security*; Springer: Berlin/Heidelberg, Germany, 2021; pp. 3–65.
76. Halak, B. *Hardware Supply Chain Security: Threat Modelling, Emerging Attacks and Countermeasures*; Springer Nature: Berlin/Heidelberg, Germany, 2021.
77. Harrison, J.; Asadizanjani, N.; Tehranipoor, M. On malicious implants in PCBs throughout the supply chain. *Integration* **2021**, *79*, 12–22. [CrossRef]
78. Arquilla, J.; Guzdial, M. The SolarWinds hack, and a grand challenge for CS education. *Commun. ACM* **2021**, *64*, 6–7. [CrossRef]
79. Analytica, O. *Kaseya Ransomware Attack Underlines Supply Chain Risks*; Technical Report oxan-es; Oxford Analytica: Oxford, UK, 2021.
80. Hope, A. North Korean Lazarus Hacking Group Leverages Supply Chain Attacks to Distribute Malware for Cyber Espionage. *CPO Magazine*, 5 November 2021.
81. Chinchani, R.; Iyer, A.; Ngo, H.Q.; Upadhyaya, S. Towards a theory of insider threat assessment. In Proceedings of the 2005 International Conference on Dependable Systems and Networks (DSN'05), Yokohama, Japan, 28 June–1 July 2005; pp. 108–117.
82. Bishop, M.; Gates, C. Defining the insider threat. In Proceedings of the 4th Annual Workshop on Cyber Security and Information Intelligence Research: Developing Strategies to Meet the Cyber Security and Information Intelligence Challenges Ahead, Oak Ridge, TN, USA, 12–14 May 2008; pp. 1–3.
83. Probst, C.W.; Hunker, J.; Gollmann, D.; Bishop, M. Aspects of insider threats. In *Insider Threats in Cyber Security*; Springer: Berlin/Heidelberg, Germany, 2010; pp. 1–15.
84. Hunker, J.; Probst, C.W. Insiders and Insider Threats-An Overview of Definitions and Mitigation Techniques. *J. Wirel. Mob. Netw. Ubiquitous Comput. Dependable Appl.* **2011**, *2*, 4–27.
85. Georgiadou, A.; Mouzakitis, S.; Askounis, D. Detecting Insider Threat via a Cyber-Security Culture Framework. *J. Comput. Inf. Syst.* **2021**, 1–11. [CrossRef]
86. Wei, Y.; Chow, K.P.; Yiu, S.M. Insider threat prediction based on unsupervised anomaly detection scheme for proactive forensic investigation. *Forensic Sci. Int. Digit. Investig.* **2021**, *38*, 301126. [CrossRef]
87. Miller, J.F. *Supply Chain Attack Framework and Attack Patterns*; Technical Report; MITRE Corp: Mclean, VA, USA, 2013.

88. Yeboah-Ofori, A.; Islam, S. Cyber security threat modeling for supply chain organizational environments. *Future Internet* **2019**, *11*, 63. [CrossRef]
89. Yeboah-Ofori, A.; Mouratidis, H.; Ismai, U.; Islam, S.; Papastergiou, S. Cyber Supply Chain Threat Analysis and Prediction Using Machine Learning and Ontology. In Proceedings of the IFIP International Conference on Artificial Intelligence Applications and Innovations, Crete, Greece, 25–27 June 2021; pp. 518–530.
90. Saxena, N.; Hayes, E.; Bertino, E.; Ojo, P.; Choo, K.K.R.; Burnap, P. Impact and key challenges of insider threats on organizations and critical businesses. *Electronics* **2020**, *9*, 1460. [CrossRef]
91. Liu, L.; De Vel, O.; Han, Q.L.; Zhang, J.; Xiang, Y. Detecting and preventing cyber insider threats: A survey. *IEEE Commun. Surv. Tutor.* **2018**, *20*, 1397–1417. [CrossRef]
92. Badhwar, R. Commentary on Insider Threat. In *The CISO's Next Frontier*; Springer: Berlin/Heidelberg, Germany, 2021; pp. 345–351.
93. Wang, J.H.; Tavoosi, J.; Mohammadzadeh, A.; Mobayen, S.; Asad, J.H.; Assawinchaichote, W.; Vu, M.T.; Skruch, P. Non-Singleton Type-3 Fuzzy Approach for Flowmeter Fault Detection: Experimental Study in a Gas Industry. *Sensors* **2021**, *21*, 7419. [CrossRef]
94. Qin, S.; Zhang, C.; Zhao, T.; Tong, W.; Bao, Q.; Mao, Y. Dynamic High-Type Interval Type-2 Fuzzy Logic Control for Photoelectric Tracking System. *Processes* **2022**, *10*, 562. [CrossRef]
95. Amanlou, A.; Suratgar, A.A.; Tavoosi, J.; Mohammadzadeh, A.; Mosavi, A. Single-Image Reflection Removal Using Deep Learning: A Systematic Review. *IEEE Access* **2022**, *10*, 29937–29953. [CrossRef]
96. Inac, H.; Oztemel, E. An assessment framework for the transformation of mobility 4.0 in smart cities. *Systems* **2021**, *10*, 1. [CrossRef]
97. Oladipo, I.D.; AbdulRaheem, M.; Awotunde, J.B.; Bhoi, A.K.; Adeniyi, E.A.; Abiodun, M.K. Machine Learning and Deep Learning Algorithms for Smart Cities: A Start-of-the-Art Review. In *IoT IoE Driven Smart Cities*; Springer: Cham, Switzerland, 2022; pp. 143–162. [CrossRef]
98. Wang, L.; Zhang, Y. Linear approximation fuzzy model for fault detection in cyber-physical system for supply chain management. *Enterp. Inf. Syst.* **2021**, *15*, 966–983. [CrossRef]
99. Alshurideh, M.T.; Al Kurdi, B.; Alzoubi, H.M.; Ghazal, T.M.; Said, R.A.; AlHamad, A.Q.; Hamadneh, S.; Sahawneh, N.; Al-kassem, A.H. Fuzzy assisted human resource management for supply chain management issues. *Ann. Oper. Res.* **2022**, 1–19. [CrossRef]
100. Bukowski, L.; Feliks, J. Fuzzy logic expert system for supply chain resilience modelling and simulation. *J. Pol. Saf. Reliab. Assoc.* **2015**, *6*, 31–38.
101. Kumar, S.; Anbanandam, R. An integrated Delphi–fuzzy logic approach for measuring supply chain resilience: An illustrative case from manufacturing industry. *Meas. Bus. Excell.* **2019**, *23*, 350–375. [CrossRef]
102. Gallab, M.; Bouloiz, H.; Alaoui, Y.L.; Tkiouat, M. Risk assessment of maintenance activities using fuzzy logic. *Procedia Comput. Sci.* **2019**, *148*, 226–235. [CrossRef]
103. Díaz-Curbelo, A.; Espin Andrade, R.A.; Gento Municio, Á.M. The role of fuzzy logic to dealing with epistemic uncertainty in supply chain risk assessment: Review standpoints. *Int. J. Fuzzy Syst.* **2020**, *22*, 2769–2791. [CrossRef]