




Review

CNA Tactics and Techniques: A Structure Proposal

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: Destructive and control operations are today a major threat for cyber physical systems. These operations, known as Computer Network Attack (CNA), and usually linked to state-sponsored actors, are much less analyzed than Computer Network Exploitation activities (CNE), those related to intelligence gathering. While in CNE operations the main tactics and techniques are defined and well structured, in CNA there is a lack of such consensuated approaches. This situation hinders the modeling of threat actors, which prevents an accurate definition of control to identify and to neutralize malicious activities. In this paper, we propose the first global approach for CNA operations that can be used to map real-world activities. The proposal significantly reduces the amount of effort need to identify, analyze, and neutralize advanced threat actors targeting cyber physical systems. It follows a logical structure that can be easy to expand and adapt.

Keywords: computer network attack; CNA; information operations; IO; tactics; techniques; TTP; cyber attack



Citation: Villalón-Huerta, A.; Ripoll-Ripoll, I.; Marco-Gisbert, H. CNA Tactics and Techniques: A Structure Proposal. *J. Sens. Actuator Netw.* **2021**, *10*, 14. <https://doi.org/10.3390/jsan10010014>

Received: 14 January 2021

Accepted: 4 February 2021

Published: 10 February 2021

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Copyright: © 2021 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

An important threat against cyber physical systems is operations focused on its disruption or control. Although these activities can be directed against pure IT environments, the impact they can produce in a cyber physical system is usually much bigger, as it exceeds the cyberspace and materialize into the real-world, thus causing, for example, human losses. These activities are identified as Computer Network Attack (CNA), operations taken via computer networks to disrupt, deny, degrade, or destroy the information within computers and computer networks and/or the computers/networks themselves, as we will define later, and are performed by advanced threat actors, specially state-sponsored ones. Please note that when we refer to an *attack*, we are referring to disruption or manipulation operations, not just to any kind of attack (or cyber attack); this is an important point, as in many works the authors consider *attack* any operation against a technological infrastructure, no matter the objective of the attacker is.

CNA operations are much less analyzed than Computer Network Exploitation ones, or CNE, those related to cyber espionage; as an example, the main de facto standard to identify tactics and techniques—and to link them to advanced threat actors—MITRE ATT&CK, focuses mainly on CNE tactics and techniques, leaving CNA ones as a secondary aspect. This is due to the prevalence of CNE activities among advanced threat actors, which is a confirmation of the lack of studies to structure those attacks and its modus operandi. Although CNA operations are not as usual as those related to intelligence gathering, their importance is increasing with the expansion of cyber physical systems. An operation targeting these environments to destroy or to control them can cause damage not only to a specific industrial process, but to the society on the whole.

This work provides a structure of tactics and techniques for CNA operations and actors aligned with ATT&CK, thus complementing the effort that MITRE has done in this framework and helping to improve it. We have followed the MITRE ATT&CK structure

as the reference to develop those tactics and techniques, as it is the main public effort to establish a classification of Tactics, Techniques, and Procedures (TTP) used by threat actors, and we also propose an initial mapping for our approach to this classification. The tactics—and its associated techniques—linked to CNA activities will be submitted to MITRE to be included in the *Enterprise Tactics* section at MITRE ATT&CK. It is important to note that this work is the first proposal towards a global approach for CNA operations that can be used for establish a definitive taxonomy of TTP in those operations that nowadays have become a major threat for cyber physical systems. Moreover, a key point is that our proposal is not linked to specific components of a cyber physical system (for example, to improve specific detection mechanisms, those usually based on attack signatures in an expert system), but provides an upper approach to model and categorize threat activities against infrastructures.

One of the most important tactics is the manipulation one, as its effects are usually not noticed immediately, and so the damage on the cyber physical system can be larger; apart from that, it is the less analyzed tactic until now. In this tactic, we have identified a new research line that has to do with the identification of subcategories for manipulation families that are stated here, in order to refine the taxonomy and to cover all the relevant particular techniques; for example, inside the falsification family we could mention spoofing, a family of techniques in which an actor successfully masquerades as another by falsifying data, thereby gaining an illegitimate advantage [1].

The contributions of this paper are as follows.

- Identify the tactics linked to CNA operations.
- Discuss and establish techniques for each of the tactics identified.
- Define a structure for CNA tactics and techniques compatible with standards accepted among the community and suitable for its improvement.
- Identify a key research line for the structure and analysis of the manipulation tactic.

The rest of the paper is organized as follows. The background Section 2 provides a brief introduction to Information Operations—where CNA is located—and to the MITRE ATT&CK framework, as the main reference for the development of tactics and techniques. In Section 3, we assess the problem of the lack of a unified structure for CNA tactics and techniques, and its importance for the modeling of advanced threat actors. Section 4 analyzes the prior work in this field, stating that little research has been done, specially for the manipulation tactic. In Section 5, we propose a novel taxonomy for CNA tactics in which we identify four specific ones, and for each one of them we establish a classification for its associated techniques. In Section 6, we discuss the results of our work, comparing them with other approaches and identifying improvements. Finally, Section 7 summarizes the outcome of the overall work and identify future research lines.

2. Background

2.1. Computer Network Attack

Information Operations (IO) is defined as the integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own [2]. One of the core capabilities inside IO is Computer Network Operations (CNO), which can be described 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 [3]: (1) Computer Network Attack (CNA), (2) Computer Network Defense (CND), defensive measures to protect and defend information, computers, and networks from disruption, denial, degradation, or destruction [4], and (3) Computer Network Exploitation (CNE). While CND is about computer and network protection, whereas CNE is focused on information gathering, that is, in espionage (or cyber espionage).

CNA operations are [2] *those taken via computer networks to disrupt, deny, degrade, or destroy the information within computers and computer networks and/or the computers/networks*

themselves. As we can see from its definition, CNA has been usually linked to the so-called 4D: disrupt, deny, degrade, and destroy [5], referring to destructive—with more or less impact—actions performed through computer networks. This one, *through computer networks*, is a key point: a missile launched against a data center is not CNA, despite the fact that it shall destroy computers and networks.

The CNA concept is currently under revision and may be soon replaced by a more generic one: Cyberspace Attack (CA), a capability inside Cyberspace Operations (CO) [6], defined as [7] *the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace*. In this context, CA is a broader term than CNA: in fact, an interesting point in [7] is the relationship between CO and Electronic Warfare (EW). CA includes not only the 4D, but also manipulation, for example, in operations associated with deception, corruption, or usurpation. A compilation of these doctrine and terminology (and its use and history) can be found in [8,9]. Every threat actor that performs CNE or CNA activities develops Tactics, Techniques, and Procedures (TTP) to achieve its goals [10]. Table 1 briefly describes the TTP definitions.

Table 1. Tactics, Techniques, and Procedures (TTP) definitions.

Definition	Description
Tactics	The employment and ordered arrangement of forces in relation to each other.
Techniques	Non-prescriptive ways or methods used to perform missions, functions, or tasks.
Procedures	Standard, detailed steps that prescribe how to perform specific tasks.

Tactics specify what a threat actor is doing, at the highest level of description, to accomplish a certain mission, and techniques specify how tactics are implemented and procedures—outside of the scope of this work—describe a particular implementation. These Tactics, Techniques, and Procedures represent the behavior of the actor, very similar to what we usually call its *modus operandi*, from the highest level description (tactic) to the lowest level one (procedure) [11].

2.2. 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 worldwide, 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. An excellent description of the framework and the work done can be found at [12].

MITRE ATT&CK framework is today’s de facto standard to structure tactics and techniques of advanced threat actors. As of March 2019, ATT&CK had defined 11 enterprise tactics—those related to the activities of an attacker into its victim—and 223 enterprise techniques associated with those tactics. Apart from that, ATT&CK defines 15 pre-attack tactics—related to the activities of an attacker before compromising its victim—and 174 pre-attack techniques linked to them, as well as 13 mobile tactics—related to the compromise of mobile devices—and 66 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.

MITRE ATT&CK also links Advanced Persistent Threat groups (APT) to tactics, techniques, and software. With 78 identified groups at the time of this writing, everyone of them is named, aliased, described, and linked to specific techniques (including pre-attack and mobile) and software. In this way, an analyst can establish relations between those entities to model an adversary and its activities against a target and, most important, to establish defense mechanisms to prevent, detect and respond to a threat.

Without any doubt, ATT&CK is 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 to counter them. It constitutes a framework that, as usual, has to be improved with continuous work and contributions; in this sense, we miss in ATT&CK a deeper approach to the tactics, the techniques, and even to the software related to CNA activities.

Until 2019 MITRE ATT&CK was focused on CNE rather than in destructive operations or threat actors. In April 2019, a new enterprise tactic called “Impact” was added, where they specify the techniques whose primary objective is to reduce the availability or integrity of a system, service, or network, including manipulation of data to impact a business or operational process. This Impact tactic is directly related to CNA activities, and includes fourteen techniques, such as defacements, data manipulation, or data destruction. Although this tactic from MITRE ATT&CK is a good starting point, it is mandatory to develop it in depth.

3. The Issue

The impact of CNA operations in cyber physical systems has been largely discussed [13], especially since the discovery of Stuxnet [14]. This malware, Stuxnet, is a key piece in one of the best known manipulation operations. Although it was not the first one or the most noxious, it was the most reported [3]. Stuxnet is a cyber weapon, probably developed by United States and Israel, that compromised industrial systems to manipulate the centrifuges that enriched Uranium, so slowing down the Iranian nuclear program and directly impacting on a critical cyber physical system [15].

As stated before, CNA operations, those destructive—in more or less grade—or control-oriented, are much less analyzed than CNE ones; although many of a threat actor’s TTP are common to CNE and CNA operations, in some cases, especially when dealing with actions on the target—or, depending of the tactic used, with actions against the target—they differ. As TTP are critical to identify and model threat actors, much work has been done to structure tactics and techniques, but most of the efforts in this sense are related to CNE activities. This focus on CNE may be due to two main facts:

- Many threat actors are engaged in intelligence gathering more than in destructive attack campaigns.
- Most of CNA activities require a previous CNE operation to know the attacked target, so CNE is almost always present.

During the last years, CNA operations that are publicly known are arising and we can face different threat actors engaged in both CNE and CNA operations; a good example is APT28, a group linked to the GRU, the Russian Military Intelligence Service, working not only in cyber espionage, but also in destructive campaigns against its targets. This is an important threat not only to pure IT environments but also to OT ones, where their impact exceeds the cyberspace by causing denial effects on cyber physical infrastructures, especially on critical ones. In fact, it is considered the fastest growing threat for cyber physical systems [16].

In this work, we address an issue that has not been largely approached and whose importance is increasing during the last years. Threat modeling, including the modeling of specific cyber attacks, has been largely discussed and many approaches exist nowadays to face the problem. However, when dealing with tactics and techniques for CNA operations no global view has been defined, a situation that hinders the modeling of advanced threat actors. Most of the work regarding the structure of tactics and techniques for these actors have been focused on CNE operations, while CNA ones are not so structured. This situation has an obvious reason: as stated before, CNE is much common, and all advanced CNA operations require a previous CNE one. However, destruction and manipulation operations have increased during the last decade, as well as the actors performing them. They have become a major threat to cyber physical systems, especially against critical infrastructures,

where the damage exceeds the cyber world and can impact in the real one, including a potential loss of life.

Therefore, we are facing an increasing problem, and the lack of a structure suitable for the modeling of these actors and its operations causes a weak protection against them. Without accurate capabilities to model CNA operations, starting with a structured view of its tactics and techniques as key elements, infrastructures are not well protected, especially cyber physical systems.

4. Approaches and Limitations

Some works have established a taxonomy for computer network attacks; the authors of [17] provide an ontology whose goal is to automate the classification of a network attack during its early stages. In this ontology, the “Attack goal class” refers to the purpose of the attack, which could be considered equivalent to the tactic. The authors identify five goals in CNA operations: to change data, to destroy data, to disrupt data, to steal data, and a springboard to other goals. While this last goal cannot be considered a tactic itself and the theft of information is not inside CNA but inside CNE operations (although as stated before all CNA serious operations require a previous CNE one), the change, destruction, and manipulation of data are all considered in the taxonomy we propose; not only referring to data, but referring to all pieces of a cyber physical systems that can impact in the process they support.

As stated before, when dealing with CNA we usually refer to 4D: disrupt, deny, degrade, or destroy the information or the systems or networks themselves; this initial set of actions, expressed in many works since the 1990s [18–21] has been superseded by two approaches: to consider denial as an umbrella term for the other 3D and to include manipulation as a form of attack, beside the denial tactics.

The first of these approaches considers denial as the actions to prevent access to, operation of, or availability of a target function by a specified level for a specified time [6]; in other words, denial is not a tactic, but an effect that can be achieved by degradation, disruption, or destruction. This approach is used in many works, and seems specially consolidated in modern doctrines [7,22,23], thus considering denial as a goal, but not as a tactic itself.

Apart from denial tactics, inside CNA operations we must consider a tactic called manipulation [6,7], whose goal is to control or change the target’s information, information systems, and/or networks in a manner that supports the attacker’s objectives. Those objectives, in CNA operations, are clear: to cause denial effects against access or operation, goals that can be achieved by tactics such as degradation, disruption, destruction, and manipulation. However, following this approach, what is the difference between a manipulation that achieves a degradation or a direct degradation as a tactic? It is a very subtle one: mainly, manipulation refers to a manner that is not immediate apparent or detected: a DDoS (degradation or disruption) or a ransomware attack (destruction) are immediately identified by the victim. If the tactic was manipulation, the attack would not have been immediately detected, and would extend in time, so impact would have been higher in advance.

It is important to differentiate CNA from Electronic Attack (EA), a branch of Electronic Warfare (EW), another IO core capability. EA relies on the use of electromagnetic spectrum, while CNA relies on the data stream to execute the attack [24], although both capabilities are converging inside the cyber field; a good reference to identify EW and CNO relationships can be found in [25]. However, EA tactics and techniques could be equivalent to CNA ones in some cases, so we must consider them in our work.

Attack modeling methodologies have been largely discussed. A summary and analysis of some of these methodologies can be found in [26,27] and of course in [28], in which it is still one of the main references in the topic. Particular approaches to model an attack have been developed:

- The Cyber Kill Chain[®], developed by Lockheed Martin, is part of the Intelligence-Driven Defense[®] model for identification and prevention of cyber intrusions activity, specifying what a threat actor must complete in order to achieve their objective. This model represents an industry accepted methodology for understanding how an attacker will conduct the activities necessary to cause harm to the organizations and has been largely discussed [29].
- The Diamond Model of Intrusion Analysis (DMIA) [30] establishes a formal method applying scientific principles to intrusion analysis, providing a simple, formal, and comprehensive method of activity documentation, synthesis, and correlation. The model represents an *adversary* deploying a *capability* over some *infrastructure* against a *victim*; these activities, called *events*, are the atomic features of the model, and they define one step in a series that a threat actor must execute to achieve its goal.
- MITRE ATT&CK, previously discussed in this work.
- The Detection Maturity Level (DML) [31] is a model to assess the maturity of an organization to detect cyber attacks in terms of its capabilities to consume and act upon given threat information. The DML model is composed of nine levels of maturity, from the most technical ones—level 0 represents no information about the threat—to the highest level ones—goals and strategy of the attacker. This hierarchical model and its improvements [32,33] can give an approach not only to evaluate the detection capabilities of an organization, but also to the semantic modeling of an advanced threat actor: from a group to specific indicators left after an operation, thus helping the analysts to model the interests and behavior of the actor and its modus operandi in specific operations.

With the exception of MITRE ATT&CK, none of these approaches focuses on the tactics and techniques of an attacker. The Cyber Kill Chain[®] tries to specify the steps an attacker has to perform to achieve its objectives, without discussing how these steps can be performed (a work that is done in MITRE ATT&CK). The Diamond Model provides a framework to identify adversary operations and to discover new capabilities, infrastructure, and victims, but once again it does not focus on what and how a threat actor works. An adversarial approach like DML does refer to tactics, techniques, and procedures of an actor, but not in depth.

As tactics and techniques are not widely discussed in threat models, and the only approach focused on these aspects (MITRE ATT&CK) does not cover CNA techniques in a structured way, it is mandatory to consider particular approaches for specific techniques and to contextualize them in a global structure, as well as to analyze other kind of attacks related to cyber activities (this is, EA), trying to provide a global, common structure for CNA operations.

The work in [34] states that EA tactics are disruption, delaying, deviation, and denial, and refers to techniques such as deception, jamming, masking, and directed energy, in no particular structure. The work in [35] considers degradation, disruption, and deception as techniques to accomplish the denial tactic, together with destruction. At this point deception emerges, being unclear in literature review where is located in a tactics and techniques structure. Apart from the “4D” (deny, degrade, disrupt, and destruct) linked to CNA, some authors [7,36] directly advocate the existence of a fifth “D” while dealing with EA tactics, referring to deception. In this work, we will consider deception as a particular manipulation with two possible goals: dissimulation, to hide the real, or simulation, to show the false; later we will discuss the role of equivalence between deception and manipulation.

Most of the literature reviewed is focused on degradation techniques, and inside them, in two main directions: the first one is the characterization of electronic attacks against WiFi networks; for example, in [37,38] the authors propose a classification of DoS attacks in wireless infrastructures, based on the network layer in which the attack is performed, from the physical layer to the application one. As stated before, this kind of techniques is outside of the scope of this paper because they are closer to EA than to CNA.

The other research field has been DDoS attacks taxonomies, that is, taxonomies of attacks engaging multiple hostile actors to degrade or disrupt a victim through a network connection. In spite of the fact that some authors state that there is not a DDoS classification model [39] and try to define a general and simple scheme that differentiates between attacks on bandwidth, host resources, and weaknesses, other studies try to define a taxonomy for DDoS attacks; for example, early works like [40,41] established a classification for DDoS attacks that has been improved during those years [42]. In this model, the authors distinguish between active and passive attacks (in this case, the only established category is packet dropping). While referring to active attacks, the second difference is based on the depleted object: bandwidth or an object mandatory to access the targeted system. First, bandwidth can be depleted by flood attacks (those that require a bandwidth usage larger in the attacker than in the target) or by amplification attacks, in which a simple request is amplified in the target system thus degrading its performance when many requests are made; a typical example of an amplification attack is DNS amplification. Related to resource depletion, it can be accomplished by exploiting flaws in network protocols or by malformed packets that fool those protocol's implementation.

As seen, depletion is a key technique inside degradation; some approaches try to establish a taxonomy based on the depleted resource. The authors of [40,41] identify bandwidth depletion and resource depletion; they defend that the first one can be achieved by flooding and amplification techniques, while the second one, resource depletion, can be achieved by techniques based on exploiting vulnerabilities. Our approach is different in the sense that we do not differentiate between bandwidth or resource depletion—at the end, bandwidth is just a resource to be depleted, just like CPU or storage, joining all the techniques above depletion: for example, an application can be flooded by legit queries—not exploiting—to deplete CPU.

The less-studied tactic we are addressing deals with the manipulation of cyber physical systems; we are facing a complex and novel task, because there are no works on the subject, and the few literatures we found are confusing. Although there are many taxonomies and ontologies for attacks [43–45] (a good summary can be found in [46]), none of them focus on techniques, but most on the complete modeling of an attack (and mainly understanding attack not only as a denial or manipulation operation). Even a good work on terminology and concepts referred below [6] includes deception, decoying, conditioning, spoofing, and falsification as examples of techniques to perform the manipulation tactic; after analyzing literature and practical cases, we cannot agree with these examples: apart from the fact that this relation is not exhaustive, it mixes techniques that should be considered as particular instances of an umbrella category (spoofing is just a family of techniques linked to falsification). Other, less doctrinal studies [47], identify data modification and infrastructure manipulation as the tactics related to what we—and other references—have called manipulation and that should be considered as a single tactic.

Other relevant work on manipulation is CAPEC (*Common Attack Pattern Enumeration and Classification*), from MITRE, which defines different mechanisms of attack that include infrastructure manipulation, file manipulation, configuration or environment manipulation, software integrity attack, modification during manufacture, manipulation during distribution, hardware integrity attack, malicious logic insertion, resource contamination, and obstruction; as its name implies, this resource focuses on attack patterns, not on techniques performed to accomplish manipulation. For example, a pattern like file manipulation can be performed by many techniques but techniques define how, no matter if it is applied to configuration, file, infrastructure, or manipulation.

As we can see, there is no global approach to define a structure for CNA tactics and techniques. Network attack is a common problem to face nowadays, and some approaches have been developed to classify them from different (objectives, mechanisms. . .). However, when dealing with TTP only partial approaches have been addressed, mainly focused on degradation techniques (and inside them, particularly inside DDoS techniques). These partial approaches do not cover the full spectrum of CNA activities and they are neither

aligned with today key references. Even MITRE, which has developed standards such as CAPEC (focusing on patterns of attack, not in TTP) and, specially, ATT&CK, do not cover the full range of CNA operations in a suitable manner.

As far as we know, our work is the first global approach for CNA operations TTP structure; all work done can be considered partial, focused on specific techniques like some DDoS types, and without a common framework where to structure CNA TTP. The lack of an unified, well-accepted taxonomy of CNA tactics and techniques impacts in the security of cyber physical systems, which nowadays are one of the main targets of state-sponsored threat actors. We propose a novel approach for a structure suitable for the modeling of such actors and its activities, that can be used to prevent, identify, and neutralize operations against technological infrastructures. We cannot compare our approach against existing ones, because as we have stated, all the reviewed research focuses on particular techniques without a common framework for CNA tactic and techniques. Our approach follows MITRE ATT&CK structure, so it can be easily used in real world scenarios and can improve MITRE's effort to maintain a global shared knowledge about threat actors' modus operandi.

5. Proposed Approach: A Novel CNA Tactics Taxonomy

In this section, we present a novel structure for tactics and techniques linked to destructive and manipulative operations against cyber physical systems. Our approach includes manipulation as a tactic in CNA operations, but we will not consider denial as a tactic itself but a goal or a meta tactic that can be performed by degradation, disruption, and destruction—in fact, also by manipulation. Furthermore, it is not differentiated degradation from disruption techniques: disruption is a particular case of degradation where degradation level is 100%, so all of the techniques families expressed in degradation directly apply to the disruption tactic. Therefore, although we can face four main tactics for CNA operations (degradation, disruption, destruction, and manipulation) as Table 2 shows, only for three of them (all but disruption, seen as a particular case of degradation) are we going to define categories and subcategories, where applicable, in order to classify specific techniques in each of them.

Table 2. CNA tactics.

Name	Description
Degradation	Degradation consists [6] of techniques used to deny access to, or operation of, a target to a level represented as a percentage of capacity; if this percentage is 100%, we refer to disruption.
Disruption	Disruption consists of techniques used to completely but temporarily deny access to, or operation of, a target for a period of time; it is a degradation whose level is 100%.
Destruction	Destruction consists of techniques used to completely and irreparably deny access to, or operation of, a target.
Manipulation	Manipulation consists of techniques used to control or change the target's information, information systems, and/or networks in a manner that supports the attacker's objectives.

Our criteria for the proposed structure of TTP are based primarily (tactics) on what an attacker is trying to achieve against its target to accomplish its objectives: that is, on the effects of the operation or attack. In this way, CNA operations try to degrade, disrupt, destruct, or manipulate. Once the tactics are stated, inside each of them we identify the different techniques the attacker can develop to get the desired effect (as stated before, techniques refer to *how* a tactic is accomplished). Here, we identify some techniques that can be seen similar to others (for example, alteration vs. modification or deletion vs. cancellation); the key difference between them is the tactic they are linked to, which reflects what the attacker is trying to achieve. At this point, it is also important to note that the same

technique can be used to perform different tactics: for example, manipulation techniques can also be executed both to degrade or to destroy a target, depending on the particular assets attacked in the target or on the particular kind of the manipulation performed. When we consider deletion or encryption, linked to destruction, we are not seeing the destruction of particular files of a cyber physical environment, but the destruction of its functionality.

The different tactics identified and analyzed in this work can also be classified from an impact point of view. In this sense, although it is hard to establish a global classification, and the final impact will depend on many factors (as on the complexity of a particular campaign, or on the early detection of an operation in a target), the manipulation tactic can be considered by far the most dangerous for cyber physical processes. For advanced threat actors, manipulation implies not only knowledge about particular industrial processes, but also a high control level of the targeted infrastructure. Following manipulation, destruction attacks are the most impactful ones for the target, as they imply an irreversible damage for cyber physical systems, that can only be restored by entirely rebuilding them. Disruption, as a fully degradation level, and degradation tactics can be considered the ones with less impact on the target, as the normal behavior of the affected cyber physical systems is usually recovered once the degradation operation is contained and the affected environments are turned again to a stable status. Please note that, in spite of its impact level, all CNA tactics can lead to fatal consequences, especially when the target is a cyber physical system for a critical infrastructure.

5.1. Degradation

Degradation is a tactic whose goal is to reduce the effectiveness or efficiency of command and control systems and information collections efforts or means [7], and can be implemented using various techniques, including what we usually call Denial of Service (DoS), an explicit attempt to avoid legitimate users of a service make use of it [48], or Distributed DoS (DDoS), depending on the number of attackers.

We propose a classification for degradation techniques based not only on depletion attacks, but considering other techniques to accomplish the tactic; we differentiate between depletion, interference, and alteration approaches, and identify techniques in all of them as shown in Figure 1. This proposal includes all the main techniques and its subtechniques, dealing with all the different mechanisms an attacker can use to degrade a cyber physical system, thus providing a full coverage of the degradation tactic.

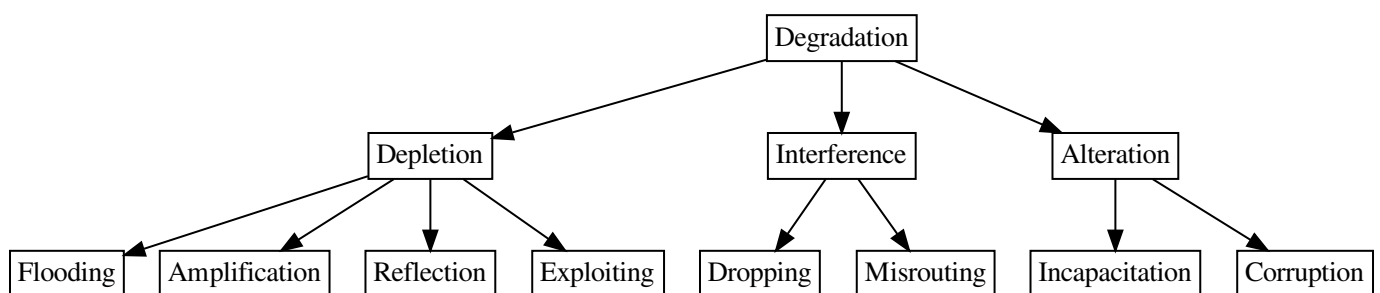


Figure 1. Degradation techniques classification.

5.1.1. Depletion

While dealing with degradation, the family of most studied techniques are those based on depletion—the degradation of an element whose work is mandatory to provide a service; depletion can be performed in any point between the target system and its legitimate users: the typically attacked points are the system itself or network devices whose degradation impacts in most users (usually, an attacker will want to maximize impact thus denying service to as many users as possible). In the special case of cyber physical systems, depletion attacks can also target physical elements of an infrastructure, although if its impact is not immediately noticed then we are facing not a degradation, but

a manipulation tactic. Depletion can be achieved through different mechanisms, presented in this section.

Flooding techniques aim to degrade services by sending vast amounts of valid service requests, trying to degrade a key resource for the provision of the service: it may be the target system itself or an intermediate infrastructure mandatory to provide service to legit users, typically a network device. Usually, flooding is performed as an N-to-1 attack, where a lot of zombies send valid requests to a destination thus achieving a service degradation—known as Distributed Denial of Service (DDoS); it is a simple and cheap attack.

Amplification techniques are those that benefit from sending small requests to services that produce responses orders of magnitude larger in size, in such a way that with a reduced number of queries an attacker can exhaust the service; inside amplification we find techniques such like DNS or NTP amplification.

A third commonly accepted technique nowadays [49] is reflection; reflection techniques are those in which the hostile actor sends requests, spoofing its source address pretending to be the victim, to a reflector server. This reflector, unable to distinguish legitimate from spoofed requests, replies directly to the victim [50,51]; launching a reflection attack from a botnet against a particular target will cause the target to be answered, thus degrading at least its bandwidth.

Finally, inside depletion, we can discuss exploiting techniques, those which are based on the exploitation of one or more flaws in a policy or in the mechanism that enforces the policy, or a bug in the software that implements the target system, and aims to consume excessive amount of resources of the target by sending it a few carefully crafted requests [52]. Inside exploiting we can consider techniques related to protocol exploiting or violation—including all layers, from infrastructure to application level—and also techniques related to application exploiting: malicious queries to a web application with a poor database structure can lead to CPU depletion on the web or database server, for example.

5.1.2. Interference

Interference attacks in CNA activities work by intentionally inducing noise or injecting false data into the target, thus degrading its service. While regarding these techniques, it is mandatory to mention jamming, a subset of denial of service attacks in which malicious nodes block legitimate communication by causing intentional interference in networks [53] and which is a key threat to cyber physical systems [54–57]; while jamming could be included inside an interference category for degradation or disruption operations, especially in WiFi sensor networks, we cannot consider jamming inside CNA techniques as it is related to Electronic Warfare. Anyway, interference techniques exist in CNA operations, with most well-known instances of this category relying upon features of the TCP protocol [58]; inside this category we can include packet dropping [59,60], an attack whose goal is to make the source and the destination perceive disconnection or degradation of path quality. Of course, while referring to degradation not all packets are to be dropped—as it could be easily detected, and will fall into the disruption tactic—but only a subset of the packets is dropped, thereby making it more difficult to detect [59]. Although packet dropping is usually performed in wireless networks by EA techniques, it can also be used in wired infrastructures, mainly in network devices (just as routers). As stated, this kind of attack can be seen as techniques inside interference, as well as routing attacks: those related to the modification of routes that interconnect source and destination of a communication, from poisoning to black holing.

5.1.3. Alteration

Another family of techniques inside degradation is alteration of system components. In this category, we can mention incapacitation, when the attacker disables one or more of key components, and change, when the attacker modifies key functions or data of the target (please note that the term “target” not only refers to a final infrastructure, but also to any point of the service delivery that can be attacked to degrade the service).

A particular tactic inside change techniques to achieve degradation is the corruption of system memory; it is a technique analyzed in many works [61–63]. Although it could be usually considered inside the destruction tactic—memory corruption attacks destroy the data, we identify it inside alteration techniques because it is performed against volatile memories and rebooting the system usually recovers its functionality (the goal of the attacker is not to destroy, but to degrade).

It is important to state that what we have called alteration differs from the manipulation tactic, although both imply the modification of key system components: in this context, alteration techniques must be seen inside the denial meta tactic, this is, they prevent access to, operation of, or availability of a target, while manipulation tactic tries to control or change information in a manner that supports the attacker’s objectives. For example, defacement can be seen as a technique inside alteration (change in particular): it directly denies the access to a legit resource, and although web defacement is usually a simple attack but it can be also performed by advanced actors—for example, for political purposes as we saw in Georgia 2008 attacks. Some authors distinguish between sophisticated and unsophisticated attacks (see in [20] for references).

5.2. Destruction

Although destruction can be performed through hardware, firmware, software, data, or network destruction, in most cases both logical and physical, while dealing with it in CNA operations targeting cyber physical systems we can identify techniques that delete firmware, software or data, that make them unusable—corruption—or that make them unusable unless a condition is met—encryption, unless the encryption key is known. All of them, when successfully used, damage its target in an irreversible manner: the target cannot perform any function or be restored to a usable condition without being entirely rebuilt [7]. Other destruction techniques, such as physical destruction, degaussing, or physical shredding, are considered outside CNA operations (some attacks, especially those against cyber physical systems, result in the physical destruction of one or more components of an infrastructure, but we will consider them inside the manipulation tactic: the attacker manipulates an industrial process, thus causing physical destruction), although they can also impact cyber physical systems.

Destruction techniques performed by advanced threat actors are usually executed against the components of the cyber physical system that most impact can cause (it is important to note that no destruction tactic can be executed without the destruction of one of these components); for example, file shredding would not be a regular technique because the file could be easily recovered from a backup, while disk wiping or cryptographic erasure are more common techniques in this context.

We propose three techniques to accomplish destruction, no matter which component they are performed against, as shown in Figure 2: deletion, the removal of key components; encryption, the encoding of those components thus rendering them or the system unusable; and corruption, the modification of key components with the same objective. In addition, the alteration techniques shown before can also be used to cause destruction of a target, although they can be included in the corruption family.

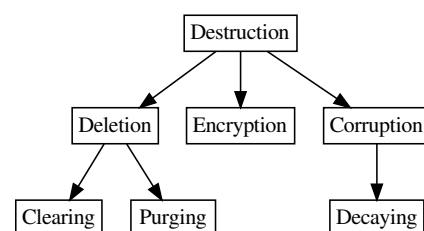


Figure 2. Destruction techniques classification.

5.2.1. Deletion

Deletion is the removal of files on a target's system in order to interrupt availability in its services. In its simplest form (clearing), it applies logical techniques to sanitize data in all user addressable storage locations [64], protecting against simple noninvasive data recovery techniques. Clearing is usually performed through system commands or methods that do not really destroy the information—it could be retrieved by a forensic analysis, but the references, in the form of file system pointers, to it.

Of course, advanced actors do not usually perform clearing techniques on CNA operations, but erasure or purging, the logical removal of data from a storage so that it can no longer be read using state of the art laboratory techniques. Unlike clearing, purging is a real deletion of data. If it is performed against a storage structure, such as a hard disk or a file system, it is usually called wiping, while if it is performed against individual files or folders, it is called shredding, which destroys data by overwriting the space used by the object with a random pattern.

5.2.2. Encryption

Encryption is a technique used to achieve destruction by encoding, in an irreversible way for the victim, data stored into a system. This non-reversible way implies that the victim does not have access to the decryption key; if access to this key is granted, data can be recovered. In some contexts, the use of this kind of cryptographic techniques when the decryption key has been destroyed is called cryptographic erasure and is an accepted technique for legit data sanitization [64]; if the decryption key does not even exist it shall be considered as corruption.

Although in some cases it has been possible for the analysts to recover the encrypted data, due to weaknesses on the encryption algorithm or in its implementation, this fact has been seen in some general, non-directed, ransomware, but no case linked to advanced actors in CNA operations is known.

5.2.3. Corruption

Finally, in the destruction context, corruption can be seen as the deliberate modification of information—firmware, software, or data—to render it unusable; of course, while considering corruption in CNA operations context, we are referring to intentional corruption, not to unintended changes to data caused by errors. A good example of corruption in computer network attacks, although not performed by advanced actors, is CIH virus, which in the late 1990s was able to replace boot-time code in particular BIOS with junk, rendering systems unusable until their BIOS was replaced.

A particular case inside corruption is decaying, techniques linked to a gradual corruption of data; although decaying is usually caused by failures in computer systems, with factors like media type, file systems design or preallocation strategies [65], it also can be considered a progressive, not easily detected, CNA technique.

5.3. Manipulation

Manipulation is an attack against integrity and, while in CNA, its goal is clear: to create denial effects [6]. Manipulation alters its target not to enable intelligence gathering—as in CNE operations—but to damage it in a manner that is not immediately apparent or detected and, in many cases, that manifests in physical domains [7]. This one, not to be immediately apparent, is a key concept in manipulation attacks; as opposite to other tactics inside CNA, manipulation degrades or destroys its target without being detected. While all CNA tactics have become an important threat to cyber physical systems, manipulation is perhaps the most dangerous one, as it extends over time, so its impact is usually higher than these of other CNA tactics. For example, Stuxnet, previously referred in this work, influenced the development of cyber weapons not only from a technical perspective, and marked a milestone on the security of cyber physical systems [66].

As previously stated, we are addressing a novel task when establishing a categorization for manipulation techniques; our position is to keep it as simple as possible, and following this approach, we can subdivide manipulation techniques into three families: fabrication, modification, and cancellation, as stated in [67,68]. These three families are capable of including different threats classification, for example, those presented in [69] against integrity, which refer to substitution, change (both considered inside modification), removal (cancellation), and addition (fabrication).

All of these types of attack can be applied against a target from the lower part of a cyber physical infrastructure [70,71] to the higher one, and can be performed during the transmission, storage, runtime, as well as during manufacturing or supply of information. In Figure 3, we show the structure for this simple manipulation techniques classification.

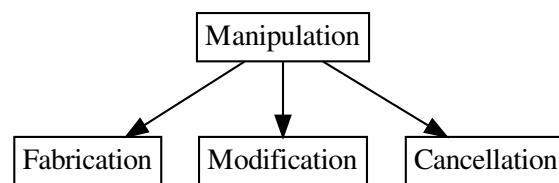


Figure 3. Manipulation techniques classification.

The definitions we could state for these techniques are obvious, as shown in Table 3, always remembering the goal of the tactic (denial) against cyber physical systems:

Fabrication techniques are those that include additional data into a system; these data can range from a single parameter in a configuration file to a piece of malware that causes an incorrect behavior of the target. Modification techniques alter existing legit data, changing it with logic, inputs, outputs, etc. that will cause a malfunction on the target. Finally, cancellation deals with the removal of certain data which is critical to the correct behavior of the target system; although cancellation is just a synonym for deletion, the techniques linked to destruction and those linked to manipulation are not similar: while in manipulation, we are referring to techniques that are not immediately detected, so their goal is not the destruction of data itself but a stealth removal of key elements in order to cause a malfunction of a process.

Table 3. Manipulation techniques.

Name	Description
Fabrication	Inclusion of spurious data into a key element (or elements) in order to cause a malfunction of the target system
Modification	Replacement of legitimate data with malicious one, also in order to achieve a malfunction
Cancellation	Removal of key data in the target, with the same proposal than previous techniques

Under this simple structure we can cover all techniques introduced in works cited before, like in [6], and it is also consistent with the techniques stated in MITRE ATT&CK for the Impact tactic regarding data manipulation (runtime, stored, and transmitted). In the same way, all CAPEC mechanisms for manipulation (data structures, system resources, and timing and state) can be linked to the proposed manipulation techniques structure.

5.4. Summary

In our proposal, we state that the tactics associated to CNA operations are degradation, disruption, destruction, and manipulation (we shall no longer mention 4D, as denial can be considered just a meta tactic); for all four tactics (“what”) we have structured techniques (“how”) families, with more or less detail, trying to define a common base to classify particular techniques in each of these families or categories. For example, a SYN Flooding

is considered a technique to achieve degradation or disruption, so obviously it should be classified inside these tactics; more specifically, and following our proposed structure, it should be classified inside the Depletion category and the Flooding subcategory.

The proposed structure that we have developed in this paper is summarized in Table 4. We summarize the different identified techniques for each CNA tactic and, if applicable, we also propose subtechniques inside techniques. This structure also follow MITRE ATT&CK that, as we have stated, is today’s de facto standard.

Table 4. CNA techniques structure proposal.

Tactic	Layer 1 Techniques	Layer 2 Techniques
Degradation and Disruption	Depletion	Flooding Amplification Reflection Exploiting
	Interference	Dropping Misrouting
	Alteration	Incapacitation Change
Destruction	Deletion	Clearing Purging
	Encryption	
	Corruption	Decaying
Manipulation	Fabrication Modification Cancellation	

5.5. 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 developed our approach following this standard, and as interesting exercise we propose a mapping of the MITRE ATT&CK “Impact” tactic (where the standard places the techniques oriented to manipulation and destruction) to our proposed structure.

At the time of this writing, MITRE ATT&CK “Impact” tactic (last modified on 25th July 2019), identified as TA0040, consists of techniques that adversaries use to disrupt availability or compromise integrity by manipulating business and operational processes. For this particular tactic, MITRE identifies the techniques shown in Table 5.

Table 5. MITRE ATT&CK Impact techniques.

Technique ID	Name	Sub Techniques
T1531	Account Access Removal	N/A
T1585	Data Destruction	N/A
T1486	Data Encrypted for Impact	N/A
T1486	Data Manipulation	Stored Data Manipulation Transmitted Data Manipulation Runtime Data Manipulation
T1491	Defacement	Internal Defacement External Defacement
T1561	Disk Wipe	Disk Content Wipe Disk Structure Wipe

Table 5. *Cont.*

Technique ID	Name	Sub Techniques
T1499	Endpoint Denial of Service	OS Exhaustion Flood Service Exhaustion Flood Application Exhaustion Flood Application or System Exploitation
T1495	Firmware Corruption	N/A
T1490	Inhibit System Recovery	N/A
T1498	Network Denial of Service	Direct Network Flood Reflection Amplification
T1496	Resource Hijacking	N/A
T1489	Service Stop	N/A
T1529	System Shutdown/Reboot	N/A

As we can see, MITRE ATT&CK provides no structure for techniques inside the “Impact” tactic, but places all of them at the same level under the tactic. Although this approach is followed in all ATT&CK tactics and techniques, given the importance of CNA activities, and its trends during last years, we consider it is mandatory to provide a wider detail, at least by splitting “Impact” tactic into the three main targets we propose in this work.

T1531, Account Access Removal, refers to the inhibition of access to accounts utilized by legitimate users; this is obviously not any destruction, but a “Degradation” or disruption tactic, and it maps to the “Change” subtechnique in our approach, stated as modification of key functions or data of the target.

T1485, Data Destruction, refers to render stored data irrecoverable by forensic techniques; it is a technique inside the “Destruction” tactic, mapping directly to “Deletion” technique in our approach, and more specifically T1485 maps to the “Purging” subtechniques inside deletion.

T1486, Data Encrypted for Impact, refers to the non-recoverable encryption of systems data or information. Like T1485, it is linked to the “Destruction” tactic and it maps directly to the “Encryption” technique in our approach.

T1565, Data Manipulation, refers to the insertion, deletion, or manipulation of data in order to hide activities. This technique is considered a tactic in our approach, mapping obviously to “Manipulation”; depending on the type of manipulation performed in each case, it could be mapped to specific techniques (fabrication, modification, or cancellation). This example shows why MITRE ATT&CK “Impact” should be detailed more in depth, as it is considering a whole tactic for CNA operations as a specific technique.

T1491, Defacement, refers to the modification of visual content; MITRE ATT&CK considers two types of defacement, internal and external, based on from where the modified content can be accessed. Following our approach, T1491 is considered inside “Degradation” tactic, particularly mapping to the “Change” subtechniques, inside the “Alteration” technique, as we have stated previously in our work.

T1561, Disk Wipe, refers to the destruction of data (from content to structure) stored in disks. Like T1485, it is linked to the “Destruction” tactic and maps to the “Purging” subtechniques, inside the “Deletion” technique. Unlike MITRE ATT&CK, in our approach we do not differentiate what type of data is purged, being in this way independent from specific approaches, close to particular technologies but not suitable for a high-level classification.

T1499, Endpoint Denial of Service, refers to the degradation or disruption of service to legitimate users. It is obviously linked to the “Degradation” (or disruption) tactic, more particularly mapped to the “Depletion” technique. Depending on how this Denial of Service is performed by the attacker, it can be mapped to particular subtechniques; MITRE ATT&CK establishes different subtechniques, where all the “Flood” ones can be

mapped to “Flooding” in our approach and “Exploitation” maps directly to the “Exploiting” subtechnique in our approach.

T1495, Firmware Corruption, refers to the corruption of firmware in devices attached to a system in order to render them inoperable. As the specific firmware is targeted in an irreversible manner, we map this technique directly to the “Corruption” technique inside the “Destruction” tactic.

T1490, Inhibit System Recovery, refers to the removing of built-in capabilities designed to aid in the recovery of a corrupted system. Depending on how this technique is performed, it can be mapped to different techniques in our approach. MITRE ATT&CK specifies two possible actions to impact on system recovery features: to disable or to delete them. In the first case, this technique would map to “Incapacitation”, a particular subtechnique of “Alteration” inside the “Degradation” tactic. In the second one, that referring to deletion, the technique maps obviously to the “Deletion” technique inside the “Destruction” tactic.

T1498, Network Denial of Service, refers to the degradation or disruption of the availability of targeted resources to legitimate users. As T1499, it is obviously linked to the “Degradation” (or disruption) tactic, more particularly mapped to the “Depletion” technique. Moreover, as in T1499, depending on how this Denial of Service is performed by the attacker, it can be mapped to particular subtechniques; in this case, MITRE ATT&CK establishes two subtechniques, the first one regarding a flooding approach and the second one regarding a mix of reflection and amplification techniques. Inside our proposal, these subtechniques can also be directly mapped to “Flooding”, “Reflection”, or “Amplification”. Please note that MITRE ATT&CK does not establish a subtechnique for “Exploitation”, as proposed in our work.

T1496, Resource Hijacking, refers to the leverage of resources impacting in availability. Although it could be considered a technique inside “Degradation”, a particular case of a Denial of Service (in MITRE ATT&CK approach, T1499, Endpoint DoS), we cannot consider it a valid technique in a CNA approach. Of course, it is an action could lead to the degradation or disruption of particular services (those hosted on the targeted system), what attackers are trying to achieve is not this tactic, but simply an economic benefit from the earning of cryptocurrencies (as MITRE ATT&CK) states as most common. In this case, degradation is just a secondary effect from the operation, not what the attacker is achieving; if degradation was the desired effect, inside our approach this one would be considered a “Depletion” technique in most cases.

T1489, Service Stop, refers to the stopping of services on a system to render them unavailable to legitimate users. As no destruction is considered, this technique is linked to the “Degradation” or “Disruption” tactic; more specifically T1489 is mapped to the “Incapacitation” subtechnique inside the “Alteration” technique.

Finally, T1529, System Shutdown/Reboot, as its name implies refers to the shutdown or reboot systems to interrupt access to, or aid in the destruction of, them. In this particular case, our approach would link this technique to the “Degradation” tactic, specifically to “Alteration” techniques, particularly to the “Change” subtechnique: the attacker is modifying key functions of its target. In no way would T1529 be linked to the “Destruction” tactic: in spite of the case a reboot can be used to aid in the destruction of a target, as MITRE ATT&CK states, it is not a destructive technique by itself but a support action.

All identified MITRE ATT&CK techniques for “Impact” tactic can be mapped to our proposed structure; apart from that, different techniques and subtechniques showed in our work do not appear in MITRE ATT&CK actual specification. In Table 6, we summarize the mapping of MITRE ATT&CK techniques to the structure we propose in our work.

At this point, it is important to note that we are using MITRE ATT&CK for references, not ATT&CK ICS. This one is a knowledge base useful for describing the actions an adversary may take while operating within cyber physical systems, but we consider it an ongoing effort focused on the goals of the attacker, not in its tactics and techniques. For example, the techniques identified in this knowledge base are not techniques (objectives)

from a pure point of view, but global goals of the attacker: a sample one, “Damage to property”, cannot be considered a technique but an impact the threat is trying to cause.

Table 6. MITRE ATT&CK techniques mapping.

Tactic	Layer 1 Techniques	Layer 2 Techniques
Degradation and Disruption	Depletion (T1499, T1498)	Flooding
		Amplification
	Interference	Reflection
		Exploiting
		Dropping
	Alteration	Misrouting
		Incapacitation (T1490, T1489)
	Change (T1531, T1491, T1529)	
Destruction	Deletion (T1490)	Clearing
		Purging (T1485, T1561)
	Encryption (T1486)	
	Corruption (T1495)	Decaying
Manipulation (T1565)	Fabrication	
	Modification	
	Cancellation	

5.6. Practical Example

The specification and structuring of CNA tactics and techniques provide organizations a higher capability to identify and analyze threats and, most important, to map defensive controls to mitigate these threats. Our proposal does not focus on specific attack detection, but on the modeling of threats regarding its objectives. Using abstract models for threat modeling allows analysts to be independent of specific technologies or systems, thus facilitating a global definition of security requirements and the implementation of defense mechanisms [72].

Focusing on a specific example, we can consider the most common techniques for degradation and disruption: those related to pure Denial of Service (DoS). In the MITRE ATT&CK approach, they identify two techniques for performing DoS: those based on the endpoint and those based on the network. For Network DoS, MITRE ATT&CK defines two subtechniques, Direct Network Flood (0.001) and reflection and amplification (0.002), and for endpoint DoS they define four subtechniques, being three of them based on flooding of resources (OS, service and application, 0.001, 0.002, and 0.003) and the last one (0.004) on the exploitation of vulnerabilities in application or systems. For all of these techniques and subtechniques, MITRE ATT&CK identifies a single mitigation countermeasure: to filter network traffic.

By including endpoint and network, this approach identifies flooding, reflection and amplification, and exploitation; for all of them, as stated before, there is a single mitigation technique based on the filtering of network traffic. We cannot agree with this approach because it mixes different techniques and does not identify appropriate countermeasures in each case. Our proposal provides a more specific classification of tactics and techniques, so it can be used to identify more suitable countermeasures in each case.

In first place, amplification is not considered as a specific technique, in spite of the given name; amplification is not a subset neither a specific subtechnique inside reflection, because both techniques differ in how they are deployed, so they also differ in how they are mitigated. Countermeasures against amplification rely in many cases in the implementation

and configuration of specific applications, while the ones regarding reflection do not rely on these aspects. In this way, we cannot deal with protection against amplification the same way we deal with protection against reflection. By considering them at the same technique level, countermeasures against them will not be appropriate.

The approach followed by MITRE ATT&CK also considers network denial of service only by exhausting the network bandwidth services rely on, while endpoint DoS are considered those that denies the availability of a service without saturating the network used to provide access to the service. This simple approach does not cover the possibility of interference in the network, that degrades its performance not by a depletion technique, so a potential threat actor performing interference operations (as such seen on Electronic Warfare) would not be considered, so no countermeasures would be applied to mitigate those attacks. This is an interesting point: as shown in Table 6, interference is the only technique not even considered in the MITRE ATT&CK approach, once again reflecting the absence of a unified common structure for tactics and techniques in this field of operations.

Apart from this two simple examples relating the mapping of defensive controls to specific attack techniques, a valid, complete, structure for CNA tactics and techniques allows organizations to improve the identification of threat offensive capabilities in a threat modeling approach as well as the attribution of specific operations. For a threat actor who can execute encryption techniques for destruction, is easiest to perform corruption or deletion techniques than to perform manipulation ones, on a prior basis.

Finally, tactics specification in three main categories provides potential information about threats not only regarding their objectives (what they are trying to do) and intentions, but also about their capabilities; in general terms, tactics can be seen from less (degradation and disruption) to more complex (manipulation). Manipulation attacks usually require specific knowledge about the target, its processes and its technologies, while a degradation attack, for example, based on depletion techniques, does not require these skills.

6. Discussion

We have identified an absence of a suitable structure of the tactics and techniques commonly used by advanced threat actors; even MITRE ATT&CK, as a key reference in the subject, lacks an approach for disruptive and manipulative operations, and we can assess that it has not been defined until now. As the number and impact of these operations are increasing in the last years, until they have become a major, significant threat for cyber physical systems, we consider it mandatory to establish such an structure that allows the prevention, detection, and neutralization of these operations.

Our work states an initial classification for that structure, following commonly accepted frameworks such as MITRE ATT&CK, thus allowing the identification of operations and the early adoption of appropriate countermeasures. We identify the main tactics specific techniques linked to this structure; of course, we do not try to provide an exhaustive compendium of particular techniques, but to identify the most relevant ones and to classify them into the defined categories. This provides a novel approach to the problem of structuring CNA operations, a mandatory requirement for the modeling of advanced threat actors' activities.

Until now, there was no doctrine providing this base model, a fact that directly impacts on the security of cyber physical systems. Most of the previous research has been focused on the study of particular techniques, such as Denial of Service, or in the analysis of particular operations, such as Stuxnet. No global structure for CNA threat actors' activities or operations has been previously stated, a fact that hinders the knowledge of those activities and the modeling of the threat actors behind them. As we have shown in previous sections, this lack of a global approach can lead to improper countermeasures against threat actions, thus degrading the security of cyber physical systems.

To specify an initial approach in a field where no doctrine has been established is a complex task. In the case of CNA tactics and techniques, it has been mandatory to analyze other disciplines inside Information Operations, such as Electronic Attack, in order for us

to compare methods and concepts. In the evaluation of disruptive approaches has also been relevant for the less analyzed tactic, manipulation, where no previous work, neither partial, has been identified.

We provide the basis for the identification of techniques in CNA operations, generating a practical structure ready to be used in commonly accepted standards, such as MITRE ATT&CK. We have provided a proposal mapping to this standard, and it would be also interesting to expand and to improve the information provided by MITRE ATT&CK regarding particular techniques by identifying activities from advanced actors that perform them; for example, APT28, linked to Russian GRU, used this technique during 2017 attacks against Ukraine (NotPetya, BadRabbit), encrypting hard drives with a non-reversible algorithm and rendering them inoperable [73].

As we have previously stated, the manipulation tactic is the less studied and structured. We have proposed a taxonomy for techniques inside this particular tactic but, in every case, a future research line is to compare manipulation techniques as those stated while referring to deception in classic references like [74]. If we look at the definition we have stated in this paper, and we replace the technical aspects with cognitive ones we could consider that (technical) manipulation is just (human) deception; in fact, deceit is just an active manipulation of reality in order to manufacture it, alter it, or hide it [75]. A key reference, such as the work in [6], refers to some techniques directly linked to deception. Under this approach, manipulation (deception) techniques should include those to hide the real, or dissimulation, and those to show the false, or simulation [74,76,77]. Under dissimulation the authors identify masking (hiding the real by making it invisible), repackaging (hiding the real by disguising) and dazzling (hiding the real by confusion), and under simulation it is included mimicking (showing the false through imitation), inventing (showing the false by displaying a different reality) and decoying (showing the false by diverting attention) [78]. Although deception is considered a usual tactic in CND operations [79–81], their study from an offensive point of view is not as usual, so we consider it as a key research line.

Applying a valid up-to-date taxonomy may guarantee a significant advantage in terms of appropriateness and fitness for attack prevention; in [82], the authors present a taxonomy that is tested against the behavior of sensors modeled as agents. Other relevant attack taxonomies are those presented in [83,84], but none of them is based on TTP for those attacks. Such contextualization should provide a global framework for the prevention, identification, and neutralization of attacks against cyber physical systems.

Finally, the use of machine learning approaches to detect intrusions against cyber physical systems, and its contextualization in a taxonomy of CNA tactics and techniques may be also a relevant research line. In [85–87], the authors provide relevant approaches, while in [88] the authors provide approaches not only in the detection, but also in the classification of such attacks. Loukas et al. [89] provides a taxonomy focused not in tactics or techniques regarding attacks, but in intrusion detection systems characteristics and architectures designed for vehicles. Extending those approaches for general taxonomies relevant to cyber physical systems and aligning them with a suitable classification, as the one provided in this work, could be an interesting research line.

7. Conclusions

Destructive and manipulation activities against all kind of targets, but especially against cyber physical systems, have increased in the last years. A classification and structure for the tactics and techniques linked to these operations is a must in order to identify capabilities, to profile advanced actors and to implement security controls to counteract them. However, few researches have been done in this sense, so analysts have almost no references to establish capabilities, families, etc. For destructive or manipulation activities performed by advanced actors, not even military doctrine has been found with the required depth level.

In this work, we propose a novel approach to identify and structure the techniques followed to perform each of the tactics linked to CNA operations against cyber physical systems. We have identified the main tactics accepted nowadays (degradation, disruption, destruction, and manipulation) and, for each of them, we have discussed and proposed the different techniques suitable to accomplish each of the tactics. Where applicable, we have also identified subtechniques. The proposed structure is aligned with MITRE ATT&CK, the main effort and the de facto standard to identify and analyze tactics and techniques from advanced threat actors. This proposed novel structure of tactics and techniques significantly contributes to improve the threat model of CNA actors.

Tactics and techniques are one of the first key points to model those actors and to deploy capabilities in order to prevent, to detect and to neutralize them, thus increasing the security not only of cyber physical systems, but of all technological infrastructures. We consider our proposal as the first, and therefore the starting point towards a commonly accepted taxonomy that helps researches to better know hostile actors, especially advanced ones, performing CNA operations.

In future works, our proposal can be used as a fundamental basis for new and more refined approaches. In this sense, manipulation techniques are the less structured ones until now—in fact, manipulation is not always considered as a tactic inside CNA operations—so in this particular case we identify an important research line.

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.

Informed Consent Statement: Not applicable.

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

References

1. El-sherif, S.H.; Abdel-kader, R.F.; Rizk, R.Y. Two-factor authentication scheme using one time password in cloud computing. In *International Conference on Advanced Intelligent Systems and Informatics*; Springer: Berlin/Heidelberg, Germany, 2018; pp. 425–434.
2. Joint Chiefs of Staff. *Joint Publication 3–13. Information Operations*; Department of Defense: Arlington, VA, USA, 2012.
3. Monte, M. *Network Attacks and Exploitation. A Framework*; John Wiley and Sons: Hoboken, NJ, USA, 2015.
4. Denning, D.E. *Assessing the Computer Network Operations Threat of Foreign Countries*; Technical Report; Naval Postgraduate School: Monterey, CA, USA, 2007.
5. Mazanec, B.M.; Thayer, B.A. *Deterring Cyber Warfare. Bolstering Strategic Stability in Cyberspace*; Palgrave Macmillan: London, UK, 2014.
6. Joint Chiefs of Staff. *Joint Publication 3–12. Cyberspace Operations*; Department of Defense: Arlington, VA, USA, 2018.
7. US Army. *Cyberspace and Electronic Warfare Operations*; Army Publishing Directorate: Fort Belvoir, VA, USA, 2017.
8. Warner, M. Notes on Military Doctrine for Cyberspace Operations in the United States, 1992–2014. *Cyber Def. Rev.* **2015**, *27*.
9. Cartwright, J.E.; James, W. Joint terminology for cyberspace operations. In *Joint Chiefs of Staff (JCS) Memorandum*; Department of Defense: Arlington, VA, USA, 2010.
10. Joint Chiefs of Staff. *Joint Publication 1-02. Department of Defense Dictionary of Military and Associated Terms*; Department of Defense: Fort Belvoir, VA, USA, 2010.
11. Johnson, C.; Badger, L.; Waltermire, D.; Snyder, L.; Skrorupka, C. *NIST SP 800-150. Guide to Cyber Threat Information Sharing*; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2016.
12. 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.
13. Rrushi, J.L. SCADA protocol vulnerabilities. In *Critical Infrastructure Protection*; Springer: Berlin/Heidelberg, Germany, 2012; pp. 150–176.
14. Langner, R. Stuxnet: Dissecting a cyberwarfare weapon. *IEEE Secur. Privacy* **2011**, *9*, 49–51. [[CrossRef](#)]
15. Moon, D.; Im, H.; Lee, J.D.; Park, J.H. MLDS: Multi-layer defense system for preventing advanced persistent threats. *Symmetry* **2014**, *6*, 997–1010. [[CrossRef](#)]
16. Merrick, K.; Hardhienata, M.; Shafi, K.; Hu, J. A survey of game theoretic approaches to modelling decision-making in information warfare scenarios. *Future Internet* **2016**, *8*, 34. [[CrossRef](#)]
17. Van Heerden, R.; Irwin, B.; Burke, I.D.; Leenen, L. A computer network attack taxonomy and ontology. *Int. J. Cyber Warf. Terror.* **2012**, *2*, 12–25. [[CrossRef](#)]

18. Tirenin, W.; Faatz, D. A concept for strategic cyber defense. In Proceedings of the MILCOM 1999 IEEE Military Communications, Conference Proceedings (Cat. No. 99CH36341), Piscataway, NJ, USA, 31 October–3 November 1999; Volume 1, pp. 458–463.
19. Grange, D.L. Asymmetric warfare: Old method, new concern. *Natl. Strategy Forum Rev.* **2000**, *9*, 1–6.
20. Siedler, R.E. Hard power in cyberspace: CNA as a political means. In Proceedings of the 2016 8th International Conference on Cyber Conflict (CyCon), Tallinn, Estonia, 31 May–3 June 2016; pp. 23–36.
21. Ionică, D.; Popescu, N.; Popescu, D.; Pop, F. Cyber Defence Capabilities in Complex Networks. In *Internet of Everything*; Springer: Berlin/Heidelberg, Germany, 2018; pp. 217–231.
22. UK Ministry of Defence. Joint Doctrine Note 1/18. In *Cyber and Electromagnetic Activities*; UK Ministry of Defence: Bicester, UK, 2018.
23. Bonner, E.L. *Defending Our Satellites: The Need for Electronic Warfare Education and Training*; Technical Report; Air Force Research Institute Maxwell AFB United States: Montgomery, AL, USA, 2015.
24. Wilson, C. *Information Operations, Electronic Warfare, and Cyberwar: Capabilities and Related Policy Issues*; Library of Congress Washington DC Congressional Research Service: Washington, DC, USA, 2007.
25. Smith, R.; Knight, S. Applying Electronic Warfare Solutions to Network Security. *Can. Mil. J.* **2005**, *6*, 49–58.
26. Mead, N.R.; Shull, F.; Vemuru, K.; Villadsen, O. *A Hybrid Threat Modeling Method*; Technical Report CMU/SEI-2018-TN-002; Software Engineering Institute, Carnegie Mellon University: Pittsburgh, PA, USA, 2018.
27. Shevchenko, N.; Chick, T.A.; O’riordan, P.; Scanlon, T.P.; Woody, C. *Threat Modeling: A Summary of Available Methods*; Carnegie Mellon University Software Engineering Institute Pittsburgh United States: Pittsburgh, PA, USA, 2018.
28. Shostack, A. *Threat Modeling: Designing for Security*; John Wiley & Sons: Hoboken, NJ, USA, 2014.
29. Myers, L. The practicality of the cyber kill chain approach to security. *CSO Online* **2013**. Available online: <https://www.cio.com/article/2381947/the-practicality-of-the-cyber-kill-chain-approach-to-security.html> (accessed on 12 January 2021).
30. Caltagirone, S.; Pendergast, A.; Betz, C. *The Diamond Model of Intrusion Analysis*; Technical Report; Center For Cyber Intelligence Analysis and Threat Research: Hanover, MD, USA, 2013.
31. Stillions, R. The DML Model. 2014. Available online: <http://ryanstillions.blogspot.com/2014/04/> (accessed on 14 December 2020).
32. Bromander, S.; Jøsang, A.; Eian, M. Semantic Cyberthreat Modelling. In *Semantic Technology for Intelligence, Defense and Security*; George Mason University: Fairfax, VA, USA, 2016; pp. 74–78.
33. Mavroeidis, V.; Bromander, S. Cyber threat intelligence model: An evaluation of taxonomies, sharing standards, and ontologies within cyber threat intelligence. In Proceedings of the 2017 European Intelligence and Security Informatics Conference (EISIC), Athens, Greece, 11–13 September 2017; pp. 91–98.
34. US Army. *FM 34-45 Tactics, Techniques, and Procedures Electronic Attack*; Department of the Army: Washington, DC, USA, 2000.
35. Joint Chiefs of Staff. *Joint Publication 3-13.1: Electronic Warfare*; Department of Defense: Arlington, VA, USA, 2007.
36. US Army Capabilities Integration Center. *The US Army Concept for Cyberspace and Electronic Warfare Operations*; Technical Report; Department of the Army HQ: Fort Eustis, VA, USA, 2018; pp. 2025–2040.
37. Sharma, K.; Ghose, M.; Kumar, D.; Singh, R.P.K.; Pandey, V.K. A comparative study of various security approaches used in wireless sensor networks. *Int. J. Adv. Sci. Technol.* **2010**, *17*, 31–44.
38. Gavric, Z.; Simic, D. Overview of DOS attacks on wireless sensor networks and experimental results for simulation of interference attacks. *Ing. Investig.* **2018**, *38*, 130–138. [CrossRef]
39. Bhaya, W.; Manaa, M.E. Review clustering mechanisms of distributed denial of service attacks. *J. Comput. Sci.* **2014**, *10*, 2037. [CrossRef]
40. Douligeris, C.; Mitrokotsa, A. DDoS attacks and defense mechanisms: A classification. In Proceedings of the 3rd IEEE International Symposium on Signal Processing and Information Technology (IEEE Cat. No. 03EX795), Ajman, United Arab Emirates, 9–11 December 2003; pp. 190–193.
41. Specht, S.; Lee, R. Distributed Denial of Service: Taxonomies of Attacks, Tools, and Countermeasures. In Proceedings of the International Workshop on Security in Parallel and Distributed Systems, San Francisco, CA, USA, 15–17 September 2004; pp. 543–550.
42. Chhabra, M.; Gupta, B.B.; Almomani, D. A Novel Solution to Handle DDOS Attack in MANET. *J. Inf. Secur.* **2013**, *4*, 165–179. [CrossRef]
43. Abrek, N. Attack taxonomies and ontologies. In *Seminar Future Internet SS2014, Network Architectures and Services*; Technical University of Munich: Munich, Germany, 2015. Available online: https://www.net.in.tum.de/fileadmin/TUM/NET/NET-2015-03-1/NET-2015-03-1_01.pdf (accessed on 12 January 2021).
44. van Heerden, R.P.; Irwin, B.; Burke, I. Classifying network attack scenarios using an ontology. In Proceedings of the 7th International Conference on Information-Warfare & Security (ICIW 2012), Seattle, WA, USA, 27 May–1 June 2012; pp. 311–324.
45. Simmonds, A.; Sandilands, P.; Van Ekert, L. An ontology for network security attacks. In *Asian Applied Computing Conference*; Springer: Berlin/Heidelberg, Germany, 2004; pp. 317–323.
46. Van Heerden, R.P. *A Formalised Ontology for Network Attack Classification*; Rhodes University: Grahamstown, South Africa, 2014.
47. Kenneth, G. Cyberspace and the Changing Nature of Warfare. In *White Paper Pre-Sented at the 2008 Black Hat Conference, 7.0*; 2008; Volume 27; Available online: <https://connections-qj.org/article/cyberspace-and-changing-nature-warfare-0> (accessed on 12 January 2021).

48. Prudente, L.; Aguirre, E.; Hdez, A.F.M.; García, R.J. DoS Attacks Flood Techniques. *Int. J. Comb. Optim. Probl. Inform.* **2012**, *3*, 3–13.
49. Geva, M.; Herzberg, A.; Gev, Y. Bandwidth distributed denial of service: Attacks and defenses. *IEEE Secur. Priv.* **2014**, *12*, 54–61. [[CrossRef](#)]
50. Booth, T.; Andersson, K. Network security of internet services: Eliminate DDoS reflection amplification attacks. *J. Internet Serv. Inf. Secur.* **2015**, *5*, 58–79.
51. Arukonda, S.; Sinha, S. The innocent perpetrators: Reflectors and reflection attacks. *Adv. Comput. Sci. Int. J.* **2015**, *4*, 94–98.
52. Abliz, M. *Internet Denial of Service Attacks and Defense Mechanisms*; Technical Report; Department of Computer Science, University of Pittsburgh: Pittsburgh, PA, USA, 2011; pp. 1–50.
53. Grover, K.; Lim, A.; Yang, Q. Jamming and anti-jamming techniques in wireless networks: A survey. *Int. J. Hoc Ubiquitous Comput.* **2014**, *17*, 197–215. [[CrossRef](#)]
54. Xu, W.; Ma, K.; Trappe, W.; Zhang, Y. Jamming sensor networks: Attack and defense strategies. *IEEE Netw.* **2006**, *20*, 41–47.
55. Li, X.; Dai, H.N.; Wang, H.; Xiao, H. On performance analysis of protective jamming schemes in wireless sensor networks. *Sensors* **2016**, *16*, 1987. [[CrossRef](#)]
56. Jaitly, S.; Malhotra, H.; Bhushan, B. Security vulnerabilities and countermeasures against jamming attacks in Wireless Sensor Networks: A survey. In Proceedings of the 2017 International Conference on Computer, Communications and Electronics (Comptelix), Jaipur, India, 1–2 July 2017; pp. 559–564.
57. Osanaiye, O.; Alfa, A.S.; Hancke, G.P. A statistical approach to detect jamming attacks in wireless sensor networks. *Sensors* **2018**, *18*, 1691. [[CrossRef](#)]
58. Barry, P.; Crowley, P. *Modern Embedded Computing. Designing Connected, Pervasive, Media-Rich Systems*; Elsevier: Amsterdam, The Netherlands, 2012.
59. Zhang, X.; Wu, S.F.; Fu, Z.; Wu, T.L. Malicious packet dropping: How it might impact the TCP performance and how we can detect it. In Proceedings of the 2000 International Conference on Network Protocols, Osaka, Japan, 14–17 November 2000; pp. 263–272.
60. Cetinkaya, A.; Ishii, H.; Hayakawa, T. An overview on denial-of-service attacks in control systems: Attack models and security analyses. *Entropy* **2019**, *21*, 210. [[CrossRef](#)]
61. Chen, S.; Xu, J.; Sezer, E.C.; Gauriar, P.; Iyer, R.K. Non-Control-Data Attacks Are Realistic Threats. In Proceedings of the USENIX Security Symposium, Baltimore, MD, USA, 1–5 August 2005; Volume 5.
62. Van der Veen, V.; Cavallaro, L.; Bos, H. Memory errors: The past, the present, and the future. In *International Workshop on Recent Advances in Intrusion Detection*; Springer: Berlin/Heidelberg, Germany, 2012; pp. 86–106.
63. Saito, T.; Watanabe, R.; Kondo, S.; Sugawara, S.; Yokoyama, M. A survey of prevention/mitigation against memory corruption attacks. In Proceedings of the 2016 19th International Conference on Network-Based Information Systems (NBIS), Ostrava, Czech Republic, 7–9 September 2016; pp. 500–505.
64. Kissel, R.; Regenscheid, A.; Scholl, M.; Stine, K. *Guidelines for Media Sanitization. NIST SP 800-88*; US Department of Commerce, National Institute of Standards and Technology: Washington, DC, USA, 2014.
65. Fairbanks, K.; Garfinkel, S. Column: Factors Affecting Data Decay. *J. Digit. Forensics Secur. Law* **2012**, *7*, 1. [[CrossRef](#)]
66. Denning, D.E. Stuxnet: What has changed? *Future Internet* **2012**, *4*, 672–687. [[CrossRef](#)]
67. Kamel, I.; Juma, H. A lightweight data integrity scheme for sensor networks. *Sensors* **2011**, *11*, 4118–4136. [[CrossRef](#)] [[PubMed](#)]
68. Pieterse, H.; Olivier, M.; van Heerden, R. Detecting Manipulated Smartphone Data on Android and iOS Devices. In *International Information Security Conference*; Springer: Berlin/Heidelberg, Germany, 2018; pp. 89–103.
69. Novokhrestov, A.; Konev, A.; Shelupanov, A. Model of Threats to Computer Network Software. *Symmetry* **2019**, *11*, 1506. [[CrossRef](#)]
70. Shakhov, V.; Koo, I. Depletion-of-battery attack: Specificity, modelling and analysis. *Sensors* **2018**, *18*, 1849. [[CrossRef](#)]
71. Desnitsky, V.; Kotenko, I.; Zakoldaev, D. Evaluation of Resource Exhaustion Attacks against Wireless Mobile Devices. *Electronics* **2019**, *8*, 500. [[CrossRef](#)]
72. Myagmar, S.; Lee, A.J.; Yurcik, W. Threat modeling as a basis for security requirements. In Proceedings of the Symposium on requirements engineering for information security (SREIS), Paris, France, 29 August 2005; Volume 2005, pp. 1–8.
73. NCSC. Reckless Campaign of Cyber Attacks by Russian Military Intelligence Service Exposed. 2018. Available online: <https://www.ncsc.gov.uk/news/reckless-campaign-cyber-attacks-russian-military-intelligence-service-exposed> (accessed on 14 March 2019).
74. Bell, J.B.; Whaley, B. *Cheating and Deception*; Library of Congress: Washington, DC, USA, 1991.
75. Jajodia, S.; Subrahmanian, V.; Swarup, V.; Wang, C. *Cyber Deception*; Springer: Berlin/Heidelberg, Germany, 2016.
76. Hutchinson, W.; Warren, M.J. The use of deception in systems. In Proceedings of the 1st International Conference on Systems Thinking in Management, Geelong, Australia, 8–10 November 2000.
77. Almeshekah, M.H.; Spafford, E.H. Planning and integrating deception into computer security defenses. In Proceedings of the 2014 New Security Paradigms Workshop, Victoria, BC, Canada, 15–18 September 2014; pp. 127–138.
78. Cohen, F.; Lambert, D.; Preston, C.; Berry, N.; Stewart, C.; Thomas, E. A framework for deception. In *National Security Issues in Science, Law, and Technology*, 1st ed.; CRC Press: Boca Raton, FL, USA, 2001.
79. Han, X.; Kheir, N.; Balzarotti, D. Deception Techniques in Computer Security: A Research Perspective. *ACM Comput. Surv.* **2018**, *51*, 80. [[CrossRef](#)]

80. Almeshekah, M.H. Using Deception to Enhance Security: A Taxonomy, Model, and Novel Uses. Ph.D. Thesis, Purdue University, West Lafayette, IN, USA, 2015.
81. Zuhri, F.A. *The Illusion of the Cyber Intelligence Era*; ZAHF.ME: Stockholm, Sweden, 2019.
82. Santacà, K.; Cristani, M.; Rocchetto, M.; Viganò, L. A topological categorization of agents for the definition of attack states in multi-agent systems. In *Multi-Agent Systems and Agreement Technologies*; Springer: Berlin/Heidelberg, Germany, 2016; pp. 261–276.
83. Hu, J.; Pota, H.R.; Guo, S. Taxonomy of attacks for agent-based smart grids. *IEEE Trans. Parallel Distrib. Syst.* **2013**, *25*, 1886–1895. [[CrossRef](#)]
84. Heartfield, R.; Loukas, G.; Budimir, S.; Bezemskij, A.; Fontaine, J.R.; Filippopolitis, A.; Roesch, E. A taxonomy of cyber-physical threats and impact in the smart home. *Comput. Secur.* **2018**, *78*, 398–428. [[CrossRef](#)]
85. Loukas, G.; Vuong, T.; Heartfield, R.; Sakellari, G.; Yoon, Y.; Gan, D. Cloud-based cyber-physical intrusion detection for vehicles using deep learning. *IEEE Access* **2017**, *6*, 3491–3508. [[CrossRef](#)]
86. Wu, M.; Song, Z.; Moon, Y.B. Detecting cyber-physical attacks in CyberManufacturing systems with machine learning methods. *J. Intell. Manuf.* **2019**, *30*, 1111–1123. [[CrossRef](#)]
87. Rouzbahani, H.M.; Karimipour, H.; Rahimnejad, A.; Dehghantanha, A.; Srivastava, G. Anomaly detection in cyber-physical systems using machine learning. In *Handbook of Big Data Privacy*; Springer: Berlin/Heidelberg, Germany, 2020; pp. 219–235.
88. Junejo, K.N.; Goh, J. Behaviour-based attack detection and classification in cyber physical systems using machine learning. In Proceedings of the 2nd ACM International Workshop on Cyber-Physical System Security, Xi'an, China, 30 May–3 June 2016; pp. 34–43.
89. Loukas, G.; Karapistoli, E.; Panaousis, E.; Sarigiannidis, P.; Bezemskij, A.; Vuong, T. A taxonomy and survey of cyber-physical intrusion detection approaches for vehicles. *Ad Hoc Netw.* **2019**, *84*, 124–147. [[CrossRef](#)]