Advances in Knowledge-Based Systems, Data Science, and Cybersecurity Received 19-07-24; Accepted 25-09-2024; Published 03-10-2024

Cyber vs. Physical Attacks: An Analysis of Technical Discriminant Criteria, and Their Consideration From a Legal Perspective

Stéphane Paul stephane.paul@thalesgroup.com
Thales Research & Technology
1 avenue Augustin Fresnel, 91767 Palaiseau, France

Tamara Hadjina tamara.hadjina@koncar.hr
KONČAR-Digital Ltd.
Fallerovo šetalište 22, 10000 Zagreb, Croatia

Bengi Zeybek b.zeybek@uva.nl
Institute for Information Law
University of Amsterdam
Nieuwe Achtergracht 166, 1018 WV Amsterdam, Netherlands

Emmanuel Gureghian emmanuel.gureghian@thalesgroup.com
Thales Research & Technology
1 avenue Augustin Fresnel, 91767 Palaiseau, France

Corresponding Author: Tamara Hadjina

Abstract

Security threats on critical infrastructures are evolving and increasingly consist of a combination of physical and cyber-attacks. In practice, a common approach to characterise physical and cyber-attacks is lacking, which may cause security gaps. This article proposes a set of technical criteria to characterise attacks. It evaluates these criteria based on attack scenarios to assess their efficacy. This study is situated against the background of the EU policy and regulation to highlight the regulatory relevance of the distinction between physical and cyber threats for critical infrastructure protection. The article concludes that, based on the currently applicable criteria, it is not technically possible to distinguish systematically cyber from physical attacks. This calls for a security management approach that acknowledges the convergence of physical and cyber threats. From a legal perspective, authors conclude there is no harmonised guidance as to how physical and cyber threats may be addressed in protecting critical infrastructure. The multidisciplinary approach of this article aims to inform decision making in terms of security governance and management.

Keywords: Cyber Attack, Physical Attack, Taxonomy, Risk Assessment, EU Cybersecurity Regulation, Critical Infrastructure Protection

Citation: S. Paul, T. Hadjina, B. Zeybek, E. Gureghian. Cyber vs. Physical Attacks: An Analysis of Technical Discriminant Criteria, and Their Consideration From a Legal Perspective. Advances in Knowledge-Based Systems, Data Science, and Cybersecurity. Research 2024;1(1):1. Pages: 1-37

1. INTRODUCTION

Most of us consider the split between cyber and physical attacks as obvious. Typically, lock picking a door is, without any doubt, a physical attack. Conversely, a distributed denial-of-service attack on a web service is obviously a cyber attack. More generally, one would intuitively state that the main difference between cyber and physical attacks is that cyber attacks are typically carried out remotely and target computer systems, whilst physical attacks involve a direct physical attack on a facility or equipment. In other words, the target type is the main discriminant criterion, complemented by the location of the attacker with respect to its target, and the method used. However, using these common sense criteria, some attacks are much more difficult to classify. For example, is the plugging on a server of a USB key containing a malware a cyber or a physical attack? If the malware enciphers sensitive data, would you definitely classify it as a cyber attack? Conversely, if the malware opens wide the valves of a damp, drowning the village below, would you change your mind and classify it as a physical attack?

When the situation becomes fuzzy, community calls them cyber-physical attacks, without further thought about which parts of the attack are cyber, and which parts are physical. This article addresses three question. First, is it *useful* for an organisation to classify clearly an attack as being a cyber or a physical attack*?* One of the motivations that we analyse is the necessity to clearly distinguish the governing responsibilities over cyber and physical attacks inside the organisations (cf. section §2, and criteria n°8 in section §4.2). Having accepted the difficulty and need of characterizing some attacks as being cyber or physical (cf. section §2), we analyse some existing taxonomies of attacks and / or security in the literature (cf. section §3). Second question: is it possible to decide formally that an attack is cyber or physical? Based on the state of the art, we propose our own taxonomy of technical criteria (cf. section §4) that can be used to discriminate cyber and physical attacks. The taxonomy is tested against a use-case derived from the PRAETORIAN project (cf. section §5). Last question: how does the EU cybersecurity and critical infrastructure (CI) protection legislation deal with cyber and physical attacks? The legal section of this article (cf. section §6) focuses on internal market-based EU laws. National security aspects of CI protection are not dealt with in this article. Finally, the main results are provided and discussed (cf. section §7).

2. CONTEXT

The aforementioned questions (cf. §1) were initially raised in the scope of the PRAETORIAN European project [1] for very practical, technical and organisational reasons. However, these questions are also applicable to industry in general, in particular for their internal organisation and security governance. They are also of legal relevance.

The PRAETORIAN project aimed at increasing the security and resilience of European CIs, and facilitating the coordinated protection of interrelated CIs against combined physical and cyber threats. To that end, the project provided a toolset comprising the following main components: i) a Cyber Situation Awareness (CSA) system, to deal with suspicious cybersecurity events; ii) a Physical Situation Awareness (PSA) system, to deal with suspicious physical events; iii) a Hybrid Situation Awareness (HSA) system, to provide a holistic view and identify cascading effects; iv) a Coordinated Response (CR) system, to integrate seamlessly First Responders (FRs) with CI managers and

Counter Unmanned Autonomous Vehicle (C-UAV) systems. During the project, when modelling realistic attack scenarios on CIs for validation purposes, it was not always obvious whether the attack detection, analysis and response should be handled by the CSA or the PSA. Long discussions took place to clarify the situation, resulting in a weak consensus. This article pushes the analysis further.

More generally, with respect to internal security governance and management in industry, the responsibility over cyber and physical risks is often split between a Chief Information Security Officer (CISO) and a Chief Security Officer (CSO), or a Physical Security Officer (PSO). If the frontier between both scopes is blurry, then vulnerabilities on assets at this frontier may go unpatched, and / or attacks on these assets may go undetected. For example, consider the following set-up. A penetration-tester is mandated by an organisation to hack its enterprise Information Technology (IT) system. The penetration-tester discovers that the default password of the Uninterruptible Power Supply (UPS) system has not been changed. After taking control of the UPS, he leverages the logical interfaces between the UPS and the IT, to take control of the complete IT system. In this enterprise, the UPS was under the responsibility of the CSO, whilst the IT was under the responsibility of the CISO. The frontier between CISO and CSO responsibilities made this attack possible and easy.

With a frontier between cyber and physical security, organisations may also find it difficult allocating the responsibility for the procurement of a platform, dealing with both cyber and physical security. A Cybersecurity & Infrastructure Security Agency (CISA) white paper [2] presents other examples of risks associated with security functions in silos, together with several case studies of attacks on such siloed organisations.

With respect to insurance, it is noteworthy that cybersecurity risk insurance has recently become a significant concern in industry. The cybersecurity risk insurance market was worth $10bn in 2022. This is relatively a small figure compared to natural catastrophe-related claims (approx. $100bn), but the market is expected to rise to $40bn in 2025 [3]. It is reported that cyber was the risk to watch, since cyber-risk is becoming uninsurable [4]. Indeed, the claims-to-premium ratio has changed from 84% in 2019 to 167% in 2020 [5], making it a highly unprofitable business for the insurance companies. This inevitably leads to multiple exemptions written into policies, e.g., war-like actions or state-backed attacks [6], as well as significant increases in the requested premiums, such as 100% increases form one year to the next. These exemptions make it very difficult for companies to know exactly what they are insuring for such a high costs. This situation calls for companies to define exactly, what impacts they want covered with respect to cyber-attacks. To this end, Airbus has created its own method, called Scenario Planning for the Identification of Cyber Exposure (SPICE) [7] to identify black swan cyber risks [8] and evaluate their impacts in monetary terms. In the same vein, a small number of large European companies has created a Mutual Insurance and Reinsurance for Information Systems (MIRIS) [9]. These two actions show the extent to which companies will go in order to better characterise cybersecurity risks and / or save themselves from negotiating settlements with their insurance when a cybersecurity incident occurs.

The popularity of cybersecurity insurance is hardly surprising. IT has become integral to CIs' operations and their operational technology, which makes them more vulnerable to cybersecurity risks resulting in damages and (legal) compensation costs. At the same time, national and European cybersecurity and privacy laws, such as the currently applicable Network and Information Services (NIS) Directive [10], and the security provisions of the General Data Protection Regulation (GDPR) [11], foresee high administrative fines for failing to ensure the security of network and information

systems and personal data, which can result in legal costs [12]. Growth in the cyber risks insurance market can be considered in the light of these technological changes to the operation of CIs, and the fines and penalties for failing to ensure the security of information services and personal data.

Another context that calls for attention to addressing cyber and physical attacks relates to law and policy.EU's Cybersecurity Strategy for the Digital Decade [13], part of the EU Security Union [14]. The EU Security Union Strategy[14] recognises the convergence of cyber and physical threats, including with regard to the protection of critical infrastructures, requiring appropriate countermeasures [15]. Two new legislations stand out in that regard: the Network and Information Services 2 Directive (NIS2)[16] which aims to increase cybersecurity capabilities across the Union, and mitigate threats to network and information systems operating in essential sectors in the EU, and the Critical Entities Resilience Directive (CERD) [17] [18], which is main legal instrument on the protection of CIs.

Overall, in this section, we have shown that poorly classifying attacks as cyber or physical attacks creates technical implementation issues when developing intrusion prevention and detection tools, and management difficulties for organisations wanting to buy those tools and / or insuring themselves against such combined attacks. We also showed that the current blurry situation might create security gaps, possibly implying legal compliance issues. We will therefore look at the state of the art of security definitions and taxonomies (cf. §3), and then propose (cf. §4) and test (cf. §5) our own taxonomy, to see if the situation can be improved technically. These discussions are complemented with a brief primer on cyber vs physical attacks under the Network and Information Services 2 Directive (NIS2) [17] and the Critical Entities Resilience Directive (CERD). (cf. §6).

3. STATE OF THE ART

There are multiple taxonomies of attacks that may be used to characterise them as cyber or physical attacks. In addition to analysing the existing cyber and physical attack taxonomies, this section also looks into the developed taxonomies for cyber-physical attacks and hybrid attacks.

In the context of cyberattacks, Igure and Williams[19] recommend that attack taxonomies should be layered or hierarchical, and propose the following four levels: attack impacts, system-specific attack types, targeted system components, and system features at the source of the exploited vulnerabilities. On the other hand, Derbyshire et al. [20] highlight Common Attack Pattern Enumeration and Classification (CAPEC) [21] as the one outperforming all the other taxonomies.

The IEC 62351 standard [22] considers cybersecurity to be a synonym of information security[1]. IEC 62443 [23] standard regards assets to be holistic, without specifically placing them in a cyber category [2]. Similarly, the glossary of the NERC reliability standards [24] provides a definition [3] which recognizes the strong dependency of cyber assets and physical equipment in the power system domain. All these definitions and taxonomies are cyber related, and do not raise the question of cyber versus physical attacks.

[1] Cybersecurity is the protection of information against unauthorized disclosure, transfer, modification, or destruction, whether accidental or intentional

[2] Assets are physical or logical object owned or under the custodial duties of an organization, which possess a perceived or real value to the organization.

[3] Cyber assets are programmable electronic devices, including the hardware, software, and data in those devices.

In the context of physical attacks, Wikipedia's [25] definition of physical security is quite vague[4]. The Knowww [26] characterises physical attacks by three features related to the target objective, the means used and the effectiveness of the attack [5]. The Colorado Governor's Office of Information Technology (CISP) Supplemental Guidance [27] gives a definition[6] based on which physical security is exclusively defined by the physical nature of the attacked target. All of the mentioned taxonomies related to physical security do not raise the question of cyber versus physical attacks. By contrast, some definitions of physical attacks are set in the context of digital security. Lemke and Paar [28] recall that the term *physical attacks* has two different meanings in the field of cryptographic implementations. The first one describes mechanisms to penetrate physically a given perimeter; the second encompasses all attacks based on physical means against cryptographic devices. This definition could be extended from to the field of Information Technology (IT) / Operational Technology (OT) security in general, using only the attack means as a key differentiating criterion. This contradicts the requirement for three features expressed in the Knowww [26].

In the context of cyber-physical attacks the IRMI glossary [29] gives a definition of cyber-physical attack as that does not address the case of a security breach in the physical environment that affects the cyber space[7]. Yampolskiy et al. [30] introduce a taxonomy of cyber-physical attack based on three top-level abstractions: targets, effects, and attacks[8]. The same authors formalised the taxonomy through a Cyber-Physical Attack Description Language [31]. Humayer et al. [32] define cyber-physical systems as systems used to monitor and control the physical world. Using the attack taxonomy defined by Yampolskiy et al. [33] they distinguish between cyber, cyber-physical, and physical attacks on cyber-physical systems based on the location of the damages[9][10]. Depoy et al. [34] describe a risk assessment method that addresses the risk of combined physical and cyber attacks against CI facilities. The authors distinguish four types of attacks: physical-only, cyber-only, cyber-enabled physical and physical-enabled cyber attacks [11]. The discriminant criteria used to distinguish cyber and physical attacks is the relative location of the attack with respect to the targeted asset, i.e., local or remote. MITRE ATT&CK base, based on real-world observations, differentiates between Enterprise and Industrial Control Systems (ICS) domains [35]. Analysing

[4] Security measures that are designed to deny unauthorized access to facilities, equipment and resources and to protect personnel and property from damage or harm.

[5] i) Attack is against physical entities, e.g., buildings, persons, computers; ii) Attack is done using physical or chemical process, e.g., physical movement of the person or drone, kinetic energy of bullet, explosion, fire, ... and iii) Attack has damaged, disturbed, changed, compromised some physical entity.

[6] Physical security is the protection of people, property and physical assets from actions and events that could cause damage or loss

[7] Cyber-physical attack is a security breach in cyber space that impacts on the physical environment.

[8] The target is composed of the influenced elements, i.e., the attacked object, and the influence, i.e., the change directly performed by the attack on the object. The effect is composed of the victim element, and the impact on the victim. Finally, the attack is composed of the attack means and the preconditions, i.e., the attack prerequisites. Based on the domains of elements, the authors define four attack categories: (i) cyber-to-cyber (C2C); (ii) cyber-to-physical (C2P); (iii) physical-to-physical (P2P); and (iv) physical-to-cyber (P2C).

[9] Attacks that do not reach physical sensors / actuators are considered purely cyber, while attacks that directly affect physical components are physical. Attacks that indirectly affect physical components, through cyber components, are cyber-physical.

[10] Unintuitively, based on this sole damage location criterion, the Zotob worm attack on DaimlerChrysler [33], or the key fob relay attacks on smart cars [68] are considered pure physical attacks by Humayer et al. Indeed, even though the worm is clearly cyber, the intention of the authors is to highlight the physical impact of the attack.

[11] Physical attacks are defined as the attacks in which the attacker gains physical access to the asset under attack in order to damage or disable it. Physical attacks can be physical-only or cyber-enabled physical attacks.In both types of physical attacks, asset failure is induced by actions taken at the asset location. Cyber attacks are defined as the attacks in which the attacker induces failure without gaining physical access to the asset. Cyber attacks can be cyber-only or physical-enabled cyber attacks.

the Tactics, Techniques and Procedures (TTPs) for ICS [36] and mapping it to the taxonomy defined by Yampolskiy et al. [30], results with all the ICS attacks in the category of cyber-physical[12].

Hybrid threats first came to mention as part of hybrid warfare theory of military strategy by Hoffman [37] [13]. The author predicts that one of the implications of evolving hybrid conflicts will be an increased need to secure the national CI from man-made attacks. The North Atlantic Treaty Organization (NATO) definition of hybrid threats is a more elaborated version of the aforementioned definition[14] [38]. In the EU, the definitions of hybrid threats remain flexible and capture the mixture of coercive and subversive activity, conventional and unconventional methods, which can be used in a coordinated manner by state or non-state actors to achieve specific objectives (while remaining below the threshold of formally declared warfare) [39]. The three definitions do not differentiate and clearly name tools and methods used as part of a hybrid attack, and thus do not contribute to the effort of characterising an attack as cyber or physical. Hybrid threats recently entered military strategy discussion and political discourse in the EU [40] [41] but a common legal framework at the EU level does not exist.

There seems to be no authoritative definition of cyber attacks and physical attacks in the state of the art, and thereof no unanimously accepted discriminant criteria to split cyber attacks from physical attacks, or to split cybersecurity from physical security.

4. ANALYSIS OF ATTACK CHARACTERISTICS TO SUPPORT THE SPLIT DECISION BETWEEN CYBER AND PHYSICAL ATTACKS

Based on the above state of the art, we have defined our own taxonomy of attacks with the end goal of supporting the split decision between cyber and physical attacks. The analysis of the attack characteristics can be done as seen (i.e., enacted) from the attacker side, or as seen (i.e., detected) from the defender side (cf. Figure 1). From the attacker side, the characteristics are closely related to facts, corresponding to the threat source, its target objectives, its actions and the consequences of these actions. This is a theoretical standpoint, as it is often difficult, or worst, impossible to know these facts, unless you are the attacker yourself. From the defender side, the characteristics are dependent on the detectability of those facts, which covers both the used sensors / probes, and the detected observables themselves.

In this section, we will analyse the characteristics of an attack from the viewpoint of the attacker (cf. section §4.1) and from the viewpoint of the defender (cf. section §4.2).

[12] If we consider individual adversary tactics as simple *sub-attacks*, we can indeed argue that tactics named: (i) *inhibit response function*, (ii) *impair process control* and (iii) *impact* are in the cyber-physical category. By contrast, all other tactics inside the ICS matrix are, according to the same taxonomy, cyber-cyber.

[13] Hybrid wars incorporate a range of different modes of warfare, including conventional capabilities, irregular tactics and formations, terrorist acts including indiscriminate violence and coercion, and criminal disorder.

[14] Hybrid threats combine military and non-military as well as covert and overt means, including disinformation, cyber attacks, economic pressure, deployment of irregular armed groups and use of regular forces

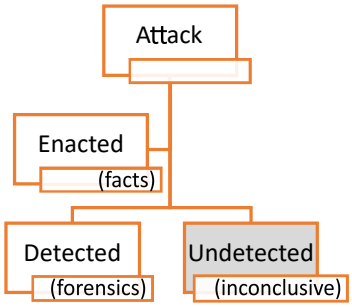

Figure 1: Two points of view on an attack.

4.1 Taxonomy of Enacted Attacks

As illustrated in Figure 2, from the attacker viewpoint, we have identified six main features that could be used as criteria to decide on the cyber or physical nature of the attack. These include: (i) the threat actor; (ii) the attacker's target objective, a.k.a. attack goal; (iii) the attacked object, in which we include the exploited vulnerabilities and / or necessary preconditions; (iv) the means used to perform the attack, covering the used tools and / or the changes performed; (v) the location from where the attack is launched versus the location of the target; and (vi) the consequences of the attack, in terms of effects and side effects.

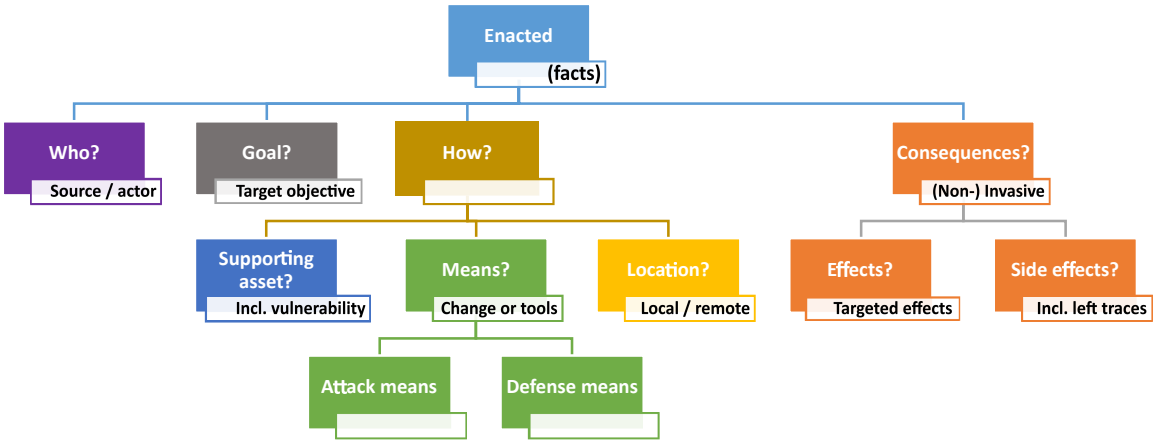

Figure 2: Taxonomy of enacted attacks.

The first feature at play in our taxonomy is the threat source / threat actor. According to the obsolete HMG IA Standard 1 & 2 [42], a *threat source* is a person or organisation that desires to breach security and ultimately will benefit from it. Based on this definition, a threat source is always *social* (i.e., human or organisational) in nature, and the actions of a threat source are always considered as intentional and malevolent. A threat source is capable of cyber, physical, social and/or hybrid attacks. Thereof, the sole knowledge of the threat source is inconclusive for the determination of the type of attack. By contrast, still according to [42], a *threat actor* is an entity who actually performs an attack or, in the case of accidents, will cause the accident. Based on this definition, the threat actor can be of social nature (i.e., person or organisation), or of cyber nature (e.g., malware, hardware

failure), or of physical nature (e.g., bomb, earthquake). When a threat actor is cyber by nature (e.g., targeted malware, stray virus, software bug), we could possibly decide for a cyber attack. When the threat actor is physical by nature (e.g., time-triggered bomb, fire), we could possibly decide for a physical attack. Thus, the cyber or physical nature of the threat actor seems to be a correct discriminant criterion to decide on the cyber or physical nature of an attack. However, as for a threat source, the threat actor can be social, in which case we cannot decide on the nature of the attack. Overall, we conclude that cyber versus physical attack determination based on the knowledge of the threat actor is a correct but incomplete criterion.

The second feature at play in our taxonomy is the *target objective* of the attacker. In line with [43], we define the target objective as the end purpose (a.k.a. end goal) targeted by a threat source. Our target objective is identical to the *Victim Element* and the *Impact on the Victim* in the Yampolskiy et al. [30] taxonomy (cf. section §3). Attackers may target valuable tangible assets, e.g., a petrol tank, an individual person, or a high-value computer, typically to steal or damage them. Alternatively, the attacker may also target cyber (a.k.a., digital or intangible) assets, e.g., an active directory, a sensitive database, or a web site. A priori, the cyber or physical nature of the target objective seems to be a strong discriminant criterion to decide on the cyber or physical nature of an attack. However, nowadays, many critical assets are cyber-physical by nature, e.g., Supervisory Control and Data Acquisition (SCADA) system, drone, radar, modern car, smart grid, etc. This implies that the target objective cannot be qualified as either cyber or physical, but as cyber-physical. Moreover, attackers' target objectives are often of a different nature altogether and / or completely abstract, e.g., an organisation's key business process, enterprise reputation, Intellectual Property Rights (IPRs), strategic prepositioning, etc. In this case, the criterion is also inconclusive. Overall, we conclude that cyber versus physical attack determination based on the knowledge of the target objective is a correct but incomplete criterion.

The third feature at play in our taxonomy is the actual asset that is attacked in order for the attacker to reach his target objective, e.g., cut power supply cable (asset) to stop the factory production (target objective – as discussed above). This attacked asset is often known as *supporting asset* [43]. A supporting asset is always physical in nature, in the sense that it exists in the physical world and thereof has vulnerabilities. The attacked *Physical Entity* is one of the three features used by Knowww [26] to characterise a physical attack (section §3), the authors consider it as a necessary feature to define a physical attack. The supporting asset is also called *Influenced Element* by Yampolskiy et al. [30], and used to discriminate the type of attack. Some people define supporting assets as tangible assets. This is often the case; however, it is a gross approximation, as many supporting assets are intangible, e.g., file stored on a hard-drive, message sent via WiFi, colour of a pixel on a screen, intensity of a sound, etc. In fact, the intangible versus tangible nature of the attacked supporting asset can be used to decide on the cyber or physical nature of an attack, even though the supporting asset is always physical. Typically, erasing *intangible* data on a hard-drive is a cyber attack, whereas breaking a *tangible* hard-drive is a physical attack. This brings us back to the true definition of cyber, i.e., the processing of information, which is by nature intangible, even though it exists in the physical world. Overall, we conclude that cyber versus physical attack determination based on the knowledge of the intangible versus tangible nature of the attacked supporting asset is a correct and complete criterion. To push further, one may consider the vulnerabilities that are exploited on this supporting asset. This criterion would be similar to the *Preconditions* of Yampolskiy et al. [30] or the *System Features* of Igure and Williams [20].

However, the list of cybersecurity related vulnerabilities is continuously evolving and growing, making the use of this vulnerability criterion impractical.

The fourth feature at play relates to the *means* used to perform and / or defend from the attack.

Attack means may be physical, e.g., camera, hammer, lock pick, bomb, etc. Alternatively, attack means may be essentially cyber, though supported by a combination of computers / Internet of Things (IoT), networks and software code. At this stage, we must acknowledge that cyber-attack means are always supported by physical means, e.g., computer with keyboard to type a malicious script or email, electro-magnetic signal to communicate via a network, etc. The attack means is one of the features used by Knowww [26] and by Lemke and Paar [28] to characterise a physical attack (cf. section §3); it is also one of the dimensions used in the taxonomy defined by Yampolskiy et al. [30]. A priori, the cyber or physical nature of the attack means seems to be a strong discriminant criterion to decide on the cyber or physical nature of an attack. However, the attack means may also be of a different nature altogether, e.g., social engineering, legal action, denunciation to a regulation authority, etc. According to the hybrid attacks definitions by NATO or EU (cf. section §3), a variety of different means can be used as part of a single hybrid attack. Thus, the nature of the attack means may be considered as a correct but incomplete criterion. When the attack means are cyber or physical, we may conclude on the nature of the attack, but when the attack means are of a different nature, the criterion is inconclusive.

Likewise, defence means may be cyber (e.g., anti-malware software, virtual local area networks, virtual firewall) or physical (e.g., closed door, air gap, firewall equipment). Defence means may also be social or procedural, e.g., awareness training on social engineering, or guidelines on what to post or not post on social networks. As such, the conclusions for defence means are identical to attack means: the criterion is correct but incomplete.

Our fifth feature at play relates to the *location* of the attacker with respect to the location of its target. An attack can be performed locally with respect to the attack target, e.g., hacking a computer using its own keyboard, setting fire to a car. Alternatively, an attack can be performed remotely with respect to the target, e.g., implanting malware through phishing, shooting a missile on a nuclear plant. Thus, by contrast with Depoy et al. [34], we believe that the location of the attacker with respect to the location of its target, i.e., local or remote, is orthogonal to the cyber or physical nature of the attack, and thereof irrelevant. It is also to be noted that our relative location criterion differs from the *location* used in Humayer et al. [32], as the latter only considers the absolute location of the damages to decide on the nature of the attack (cf. section §3). In our taxonomy, Humayer's *location* is close to our supporting asset.

The sixth feature at play relates to the consequences of the attack. This is a complex feature. First, we need to differentiate between *effects* and *side effects*. Effects relate to target objectives (a.k.a. attack goals), exclusively at the target's location. The term effects is used here with the same semantics as *Impact on Victim* in Yampolskiy et al. [30]. Side effects relate to (unwanted) traces left by the attack, both at the attacker and target location sides.

Effects are often classified as invasive (a.k.a. active) or non-invasive (a.k.a. passive) attacks [44] [45]. Invasive attacks are those with direct physical effects, both tangible and intangible, on the target. They include displacing, tampering or destroying a physical object, but also all breaches on the availability and integrity of data, e.g., Row Hammer [46], CLKscrew [47], the infamous

Lockbit ransomware, the simple deletion of a file, or the use of a Focused Ion Beam (FIB) to alter the behaviour of a processor. Non-invasive attacks are those without direct physical effects on the target[15]. They include voice recording, taking a photo of an object or its blueprint, filming, and more generally, all breaches on the confidentiality of information, e.g., DRAMA [48], Meltdown [49] or simply the reading of a file. Thus, using the effects criterion we can effectively characterise invasive attacks as physical. However, it would be somehow counter-intuitive to qualify non-invasive attacks as cyber attacks. Typically, threatening a maintenance operator with a hammer, without actually hitting him, has no physical effect, even though the attack may be effective in reaching the attacker's goal, e.g., obtaining the system credentials from the frightened maintenance operator. This action would therefore not be classified as a physical attack. It is certainly not either a cyber attack. The main issue with this *effects* criterion is that it defines physical attacks, but that it does not define cyber attacks. Thus, the use of the invasive or non-invasive nature of the effects of an attack may be considered as a correct but incomplete and unintuitive criterion.

In forensic science, Locard's principle [50] holds that the perpetrator of a crime will bring something into the crime scene and leave with something from it, and that both can be used as forensic evidence. This *something*, which we previously named *side effects*, can be physical, e.g., dust, hair, fingerprints, or cyber. Indeed, Locard's principle also holds in computer forensics, where committing cyber crime will result in cyber traces being left behind, typically cybersecurity logs or the creation of *tmp* files. In some attacks, the attacker could leave both cyber and physical traces, in which case the attack would be qualified as cyber-physical. As such, the cyber and/or physical nature of the traces may be considered as a correct and complete criterion towards differentiating a cyber attack from a physical attack.

Overall, the nature of supporting asset (i.e., tangible or intangible criterion) and the side effect criterion seem to be the only correct and complete criteria towards formally differentiating a cyber attack from a physical attack. However, all the above criteria are somehow theoretical, as it is often difficult, if not impossible, to acquire the knowledge of their values. Let us now study the criteria from the defender's side. These criteria are more practical, but they will often suffer of incompleteness due to the technical and practical limitations in their collection.

4.2 Taxonomy of Detected Attacks

As illustrated in Figure 3, from the defender and forensics a posteriori viewpoint, we have identified only two features that could be used as criteria to decide on the cyber or physical nature of the attack. They are: (i) the type of detected traces left by the attack; (ii) the actor who responded to the attack.

The type of traces left by the attack and detected by the defender, i.e., cyber or physical, is close to the effects and side effects criteria, as discussed in section §4.1. The minor difference is that the effects and side effects encompass all consequences, whereas the criterion discussed here relates only to the traces that are effectively detected. Some attack side effects may indeed remain undetected, either by lack of adequate means to detect them, or because of their accidental or automated destruction before anyone even tries to salvage them. It is also presumable that, in the event of a remote attack, all traces left at the attacker's location, or more generally in the ecosystem, may be out of reach

[15] Note that some non-invasive attacks may have side effects on the target or its direct environment. These side-effects are discussed below.

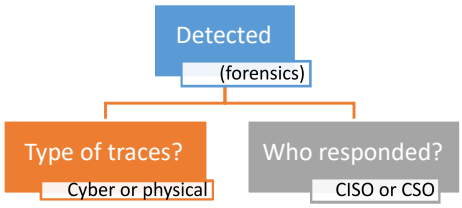

Figure 3: Taxonomy of detected attacks

of the forensics investigations. As such, the type of traces left by the attack and detected by the defender may be considered as a correct but incomplete criterion.

The second criterion at play is the actor who is responsible and / or who actually responded to the attack, and possibly contributed to the system recovery. Typically[16], a CISO is generally in charge of managing and coordinating cyber attacks, whereas CSO or PSO is generally in charge of managing and coordinating physical attacks. This criterion encompasses a very large scope of an organisation's policies and procedures. It reflects both the governance policies of the attacked organisation in terms of allocation of responsibilities and resources to respond to an attack, but also the actual response procedures and practices. Typically, in case of a cyber-physical attack, if both the CISO and CSO/PSO are on a war footing, it is possible to compare a posteriori the contributions of each of the actors in the response to and recovery from the attack, and thereof qualify the attack as mainly cyber, mainly physical, or cyber-physical. In some cases, it might be interesting to assess if the *officially* responsible officer is the one that really performed the job, or if the policies required some significant adaptations during the crisis management. As a drawback, this criterion can only be used in a post-mortem analysis. It would be both correct and complete.

4.3 Summary

Table 1 provides a summary of the conclusions for each of our taxonomy's criteria, as discussed in sections §4.2 and §4.2. It can be seen that five criteria are correct but incomplete (i.e., they are inconclusive in some cases), whilst three criteria are both correct and complete. Two of them are irrelevant, as it is impossible to decide on the cyber or physical nature of the attack based on these sole criteria. In the next section, we will evaluate each of these criteria on an attack scenario.

5. APPLICATION OF THE PROPOSED TAXONOMY

In the PRAETORIAN European project [1], we have defined four pilot scenarios to validate cyber, physical and hybrid situation awareness tools: two Austro-Croatian pilots, one Spanish pilot and one French pilot. The full description of these pilots [51] is EU Restricted, so herein we will provide a high-level overview of half of the French pilot scenario. The attack scenario is assessed in relation to all criteria discussed in previous section. This includes the criteria which were deemed irrelevant. The case study serves as illustration of our conclusions.

[16] This statement is based on the sole authors' knowledge of the organisation of some major CI industries. Variations in organisation may significantly affect the conclusions related to this actor criterion.

Attack characteristics	**Efficacy**
Criterion n°1a: type of threat source, i.e., social	Irrelevant
Criterion n°1b: type of threat actor, i.e., social, cyber or physical	Correct but incomplete
Criterion n°2: type of attacker's target objective, i.e., physical entity, data, function or service, business or operational process, social entity or social concern	Correct but incomplete
Criterion n°3: nature of supporting asset, i.e., tangible or intangible	Correct and complete
Criterion n°4a: type of attack means or tools, i.e., cyber, physical or social	Correct but incomplete
Criterion n°4b: type of defence means or tools, i.e., cyber, physical or social	Correct but incomplete
Criterion n°5: relative location of the attacker with respect to the location of its target, i.e., local or remote	Irrelevant
Criterion n°6a: type of intended attack effects on the target, i.e., invasive or non-invasive	Correct, but incomplete and unintuitive
Criterion n°6b: type of attack side effects, i.e., physical or cyber	Correct and complete
Post-mortem characteristics	**Efficacy**
Criterion n°7: Type of traces, i.e., physical or cyber	Correct but incomplete
Criterion n° 8: Responsible or responding actor, i.e., CSO/PSO or CISO	Correct and complete

Table 1: Efficacy of attack characteristics towards deciding on physical vs. cyber attack

The attack scenario is decomposed in 17 elementary steps which are analysed independently. However, two of our criteria are global for the overall attack: the threat source and the target objective. The analysis of these two criteria is performed prior to the decomposition.

Overall attack: terrorists blow up a power plant, creating hundreds of casualties

In the PRAETORIAN project [1], the French scenario involves a coordinated attack on two CIs: a power plant and a port. Herein, we will analyse only the part of the attack dealing with the power plant. In short, some terrorists want to blow up an electricity power plant, create havoc, and kill as many people as possible in the operation. The attack can be characterised as follows, cf. Table 2.

Criteria	**Value**	**Characterisation**
Threat source (n°1a)	Terrorist organisation	Inconclusive
Target objective / goal (n°2)	Blow up power plant, create power shortage in the region, kill as many people as possible	Physical

Table 2: Characterisation of the overall attack

As discussed in section §4, the knowledge of the threat source is irrelevant to decide on the cyber or physical nature of the attack. By contrast, the target objective criterion was said to be correct but incomplete. Here, it is possible to conclude on the physical nature of the attack, based on the physical nature of the target objective.

The attack scenario is now decomposed in 17 elementary steps, which will support the analysis of all the other criteria.

Step n°1: a terrorist organization corrupts a power plant physical security employee
A terrorist organization gives and promises significant amounts of money in cash to a legitimate power plant employee, working in the field of the power plant's physical security, in exchange of two services to render. First, the employee must create and deliver to the terrorist organisation five real company badges, which give full legitimate physical access to the most restricted areas of the power plant. Secondly, the employee must plug a USB stick in the Physical Access Control System (PACS) server, and schedule an application provided on the USB stick. The employee takes the money, no questions asked. Based on the taxonomy defined in section §4, this step of the attack is enacted, but cannot be detected without violating the employee's privacy. Thus, it can be characterised as follows, cf. Table 3.

Criteria	Value	Characterisation
Threat actor (n°1b)	Terrorist organisation	Inconclusive
Supporting assets (n°3)	Power plant employee	Physical
Attack means (n°4a)	Social engineering / corruption	Inconclusive
Defence means (n°4b)	None	Inconclusive
Location (n°5)	Public area, e.g., bar	Inconclusive
Effects (n°6a)	Malicious internal employee	Inconclusive
Side effects (n°6b)	Money transfer, USB stick transfer, malware transfer	Cyber-physical

Table 3: Characterisation of step n°1 of the attack (enacted, undetected): gain an insider to the cause

In section §4, we presented the threat actor, supporting assets, means and effects criteria as being correct but incomplete. Here, all the criteria values are social, and therefore the cyber versus physical characterisation of the attack is inconclusive. The side-effects criterion was presented as being correct and complete. However, the side effects cover both cyber and physical elements. Based on this criterion, the attack is characterised as cyber-physical. Overall, the above characterisation shows that this step of the attack is essentially social, with some cyber-physical side effects.

Note: in the following attack steps, we will not analyse each criterion as we have done above for the overall attack and for step n°1. The results of the characterisation will be provided in tables.

Step n°2: the corrupted employee enters the room containing the PACS
The corrupted employee is legitimate to enter the room containing the PACS, as part of his normal job activities. His entrance is allowed and logged by the PACS. Based on the taxonomy defined in section §4, this step of the attack can be characterised as follows, cf. Table 4 and Table 5.

The above characterisation shows that this step of the attack is mainly physical, with however an essential cyber part to the attack. Indeed, the employee entrance is allowed through a digital authorisation delivered by the PACS, and the PACS logs are the only traces that may be analysed post-mortem. By contrast, lock picking or breaking down the door would have characterised a purely physical attack. As such, step n°2 of the attack should be classified as cyber-physical.

Criteria	Value	Characterisation
Threat actor (n°1b)	Corrupted employee	Inconclusive
Supporting assets (n°3)	PACS	Cyber-physical
Attack means (n°4a)	Legitimate employee, legitimate employee badge, PACS (incl. badge reader at entrance of restricted area)	Social and cyber-physical
Defence means (n°4b)	PACS	Cyber-physical
Location (n°5)	Power plant	Inconclusive
Effects (n°6a)	Malicious employee in restricted area	Physical
Side effects (n°6b)	Entrance logs	Cyber

Table 4: Characterisation of step n°2 of the attack (enacted): enter restricted area

Criteria	Value	Characterisation
Type of traces	Entrance logs	Cyber
Responsible / responding actor	PSO	Physical

Table 5: Characterisation of step n°2 of the attack (detected, forensics): entrance within restricted area

Step n°3: the corrupted employee logs into the PACS

The corrupted employee uses his legitimate credentials to log into the PACS. In our PRAETORIAN system implementation, this login is undetected. Based on the taxonomy defined in section §4, this step of the attack can be characterised as follows, cf. Table 6.

Criteria	Value	Characterisation
Threat actor (n°1b)	Corrupted employee	Inconclusive
Supporting assets (n°3)	PACS	Cyber-physical
Attack means (n°4a)	PACS human-machine interface (incl. software, screen and keyboard), employee credentials	Social and cyber
Defence means (n°4b)	PACS credentials	Cyber
Location (n°5)	PACS restricted area	Inconclusive
Effects (n°6a)	Attacker logged in PACS	Cyber
Side effects (n°6b)	PACS state, possible fingerprints on keyboard	Cyber (potentially cyber-physical)

Table 6: Characterisation of step n°3 of the attack (enacted, undetected): log into PACS

The above characterisation shows that this step of the attack is essentially cyber, with some minor physical side effects, because the action is performed on premise.

Step n°4: the corrupted employee plugs the USB key provided by the terrorists

The corrupted employee plugs the USB stick provided by the terrorists in a USB connector of the

PACS server. This plugging is detected by the operating system. Based on the taxonomy defined in section §4, this step of the attack can be characterised as follows, cf. Table 7 and Table 8.

Criteria	Value	Characterisation
Threat actor (n°1b)	Corrupted employee	Inconclusive
Supporting assets (n°3)	PACS	Cyber-physical
Attack means (n°4a)	USB stick, USB connector on PACS server	Physical
Defence means (n°4b)	Logging of OS events	Cyber
Location (n°5)	PACS restricted area	Inconclusive
Effects (n°6a)	Illegitimate mobile storage media physically connected to PACS	Physical
Side effects (n°6b)	OS logs, possible fingerprints on USB stick (if the USB stick is not removed)	Cyber (potentially cyber-physical)

Table 7: Characterisation of step n°4 of the attack (enacted): plug USB stick on PACS

Criteria	Value	Characterisation
Type of traces	OS logs, possible fingerprints on USB stick (if the USB stick is not removed)	Cyber (potentially cyber-physical)
Responsible / responding actor	CISO	Cyber

Table 8: Characterisation of step n°4 of the attack (detected, forensics): mobile media plugged on PACS

Based on the goal, means and effects criteria, the above characterisation shows that this step of the attack is essentially and intuitively physical, but with significant cyber aspects to it. Indeed, the responsible actor here would generally be the CISO, and the key traces for forensics are purely cyber. Overall, this elementary step of the attack can only be classified as cyber-physical.

Step n°5: the corrupted employee copies a file from the USB stick

The corrupted employee copies a file from the USB stick to the PACS Solid State Drive (SSD). A file creation event is detected and logged by the Windows operating system, but the source of the file remains unknown from a forensics viewpoint. Based on the taxonomy defined in section §4, this step of the attack can be characterised as follows, cf. Table 9 and Table 10.

Intuitively, a file copy is purely cyber. This is confirmed by all criteria, except the supporting assets and side effects criterion, because the attack is performed locally on a cyber-physical target. Overall, this step of the attack can only be classified as cyber-physical.

Step n°6: the corrupted employee schedules the malware to run at a defined time

The corrupted employee opens the Windows Task Scheduler, and schedules a task to run the copied malware at the date and time that was specified by the terrorists. In our PRAETORIAN monitoring system implementation, the opening of the Task Scheduler is undetected, but the scheduling of a new task is detected. Based on the taxonomy defined in section §4, this step of the attack can be characterised as follows, cf. Table 11 and Table 12.

Criteria	Value	Characterisation
Threat actor (n°1b)	Corrupted employee	Inconclusive
Supporting assets (n°3)	PACS	Cyber-physical
Attack means (n°4a)	PACS human-machine interface (incl. software, screen and keyboard), storage media, malware file	Cyber
Defence means (n°4b)	Logging of OS events	Cyber
Location (n°5)	PACS restricted area	Inconclusive
Effects (n°6a)	Installed malware	Cyber
Side effects (n°6b)	OS logs, possible fingerprints on keyboard	Cyber (potentially cyber-physical)

Table 9: Characterisation of step n°5 of the attack (enacted): install malware

Criteria	Value	Characterisation
Type of traces	OS logs, possible fingerprints on keyboard	Cyber (potentially cyber-physical)
Responsible / responding actor	CISO	Cyber

Table 10: Characterisation of step n°5 of the attack (detected, forensics): malware installed

Criteria	Value	Characterisation
Threat actor (n°1b)	Corrupted employee	Inconclusive
Supporting assets (n°3)	PACS	Cyber-physical
Attack means (n°4a)	PACS human-machine interface (incl. software, screen and keyboard), Ms. Task Scheduler, malware file	Cyber
Defence means (n°4b)	Logging of OS events	Cyber
Location (n°5)	PACS restricted area	Inconclusive
Effects (n°6a)	Scheduled task	Cyber
Side effects (n°6b)	OS logs, possible fingerprints on keyboard	Cyber (potentially cyber-physical)

Table 11: Characterisation of step n°6 of the attack (undetected): schedule malware

Intuitively, one would expect that malware scheduling is a purely cyber attack. However, as for step n°5 (see above), the supporting asset is cyber-physical, and side effects may also be assessed as cyber-physical. Thus, overall, this step of the attack can only be classified as cyber-physical.

Step n°7: the corrupted employee creates the five requested badges

The corrupted employee creates a new badge, and assigns it high physical access privileges. He repeats this operation five times. These badge creations are detected and logged by our monitoring

Criteria	Value	Characterisation
Type of traces	New task scheduled, OS logs, possible fingerprints on keyboard	Cyber (potentially cyber-physical)
Responsible / responding actor	CISO	Cyber

Table 12: Characterisation of step n°6 of the attack (detected, forensics): scheduled malware

system. Based on the taxonomy defined in section §4, this step of the attack can be characterised as follows, cf. Table 13 and Table 14.

Criteria	Value	Characterisation
Threat actor (n°1b)	Corrupted employee	Inconclusive
Supporting assets (n°3)	PACS	Cyber-physical
Attack means (n°4a)	Virgin badges, PACS human-machine interface (incl. software, screen and keyboard), badge printer	Cyber-physical
Defence means (n°4b)	Logging of OS and PACS events	Cyber
Location (n°5)	PACS restricted area	Inconclusive
Effects (n°6a)	Five new badges with high access privileges	Cyber-physical
Side effects (n°6b)	OS logs, PACS logs, possible fingerprints on keyboard, badge printer and badges	Cyber (potentially cyber-physical)

Table 13: Characterisation of step n°7 of the attack (enacted): create 5 high-privilege badges

Criteria	Value	Characterisation
Type of traces	New rights opened for 5 new people, OS logs, PACS logs, 5 newly printed badges, fingerprints on keyboard, badge printer and badges	Cyber-physical
Responsible / responding actor	PSO	Physical

Table 14: Characterisation of step n°7 of the attack (detected, forensics): 5 high-privilege badges created

Intuitively, one would expect that the creation of *true-false* badges is a physical attack. This is confirmed by having the PSO as responsible actor. However, since the attack is performed using cyber-physical means and requires the modification of the PACS Data Base (DB) to store the authorisations of the new badges, the above characterisation shows that this elementary step of the attack may better be classified as cyber-physical. In particular, this attack would certainly be easier to detect by the CISO than by the PSO.

Step n°8: the corrupted employee exits the PACS restricted area

The corrupted employee is legitimate to exit the room containing the PACS, as part of his normal

job activities. This exit is allowed and logged by the PACS. This step is similar to step n°2 (see above), so it is not detailed herein. As for step n°2, this attack step is classified as cyber-physical, based on the taxonomy defined in section §4.

Step n°9: the corrupted employee delivers the badges to the terrorists

The corrupted employee delivers the five requested badges to the terrorists, and reports on the good execution of the malware scheduling. This step is similar to step n°1 of this attack chain, so it is not detailed herein. As for step n°1, this attack step is undetected and social.

Step n°10: the terrorists enter the transformer station area

Later in the evening, five terrorists, dressed as maintenance operators, enter the power plant and reach the restricted transformer station area, using their *true-false* badges. This step is similar to step n°2 (see above), so it is not detailed herein. As for step n°2, this attack step classified as cyber-physical, based on the taxonomy defined in section §4.

Step n°11: the terrorists place bombs

The terrorists place timed-triggered bombs at strategic locations of the Transformer Station (TS) to cause the most damage. There is no sensor (e.g., camera) in our implementation to detect such actions; thereof, the action remains undetected. Based on the taxonomy defined in section §4, this step of the attack can be characterised as follows, cf. Table 15.

Criteria	Value	Characterisation
Threat actor (n°1b)	Terrorists	Inconclusive
Supporting assets (n°3)	Transformer station	Physical
Attack means (n°4a)	Time-trigger bombs	Physical
Defence means (n°4b)	None	Inconclusive
Location (n°5)	Transformer station restricted area	Inconclusive
Effects (n°6a)	Bombs deposit	Physical
Side effects (n°6b)	-	Inconclusive

Table 15: Characterisation of step n°11 of the attack (enacted, undetected): blow up TS

The above characterisation shows that this step of the attack is clearly physical.

Step n°12: the terrorists move to the turbine area

The five terrorists then move to the restricted turbine area, using their “true-false” badges. This step is similar to step n°2 (see above), so it is not detailed herein. As for step n°2, this attack step is classified as cyber-physical.

Step n°13: the terrorists intrude inside the Industrial Control Systems network

In the turbine area, the terrorists connect a maintenance PC to the electrical cabinet. The PC is equipped with a special modem needed to communicate with the electrical valves controlling the water flow. The connection does not require any authentication. In our PRAETORIAN system implementation, the PC connection to the maintenance cabinet is undetected. Based on the taxonomy defined in section §4, this step of the attack can be characterised as follows, cf. Table 16.

The above characterisation shows that this elementary step of the attack is clearly cyber-physical.

Criteria	Value	Characterisation
Threat actor (n°1b)	Terrorists	Inconclusive
Supporting assets (n°3)	Electrical cabinet, ICS network	Cyber-physical
Attack means (n°4a)	PC, with specific modem and maintenance software	Cyber-physical
Defence means (n°4b)	None	Inconclusive
Location (n°5)	Turbine restricted area	Inconclusive
Effects (n°6a)	Malicious device connected to the ICS network	Cyber-physical
Side effects (n°6b)	-	Inconclusive

Table 16: Characterisation of step n°13 of the attack (enacted, undetected): take control of ICS network

Step n°14: the terrorists tamper the water valves

The terrorists switch the valves control in manual mode and then send manual opening and closing commands to the valves. The rapid execution of these inconsistent commands leads to a breakdown of the valves, disrupting the overall industrial process. In our system implementation, the switch to manual mode is detected and logged, as well as all the subsequent commands sent to the electrical valves. Based on the taxonomy defined in section §4, this step of the attack can be characterised as follows, cf. Table 17 and Table 18.

Criteria	Value	Characterisation
Threat actor (n°1b)	Terrorists	Inconclusive
Supporting assets (n°3)	ICS network, electrical valves	Cyber-physical
Attack means (n°4a)	PC, with specific modem and maintenance software, and commands sent by maintenance PC	Cyber-physical
Defence means (n°4b)	Logging of commands sent by maintenance PC	Cyber
Location (n°5)	Turbine restricted area	Inconclusive
Effects (n°6a)	Valve breakdown	Physical
Side effects (n°6b)	Logs of commands sent by maintenance PC	Cyber

Table 17: Characterisation of step n°14 of the attack (enacted): sabotage electrical valves

Criteria	Value	Characterisation
Type of traces	Damaged electrical valves, logs of commands sent by maintenance PC	Physical and cyber
Responsible / responding actor	Industrial Control Systems (ICS) CISO	Cyber

Table 18: Characterisation of step n°14 of the attack (detected, forensics): electrical valves damaged

The above characterisation shows that this elementary step of the attack is once again cyber-physical, with an interesting mix of purely physical assessments (e.g., effects, traces), and purely cyber assessments (e.g., side-effects, traces and responsible actor criteria).

Step n°15: the terrorists exit the power plant

The five terrorists exit the power plant, using their *true-false* badges. This step is similar to step n°2, so it is not detailed herein. As for step n°2, this attack step is classified as cyber-physical.

Step n°16: the malware activates

The time-triggered dormant malware wakes up: it disables all the badges and the normal exit buttons. Some congestion is created near the doors, and the power-plant staff is confused. Based on the taxonomy defined in section §4, this step of the attack can be characterised as follows, cf. Table 19 and Table 20.

Criteria	Value	Characterisation
Threat actor (n°1b)	Malware	Cyber
Supporting assets (n°3)	PACS DB, all exit doors	Cyber and physical
Attack means (n°4a)	None[17]	-
Defence means (n°4b)	Logging of PACS and OS events	Cyber
Location (n°5)	PACS restricted area (threat actor location) versus overall power-plant (effects location)	Inconclusive
Effects (n°6a)	Erased PACS DB, disabled badges and power-plant emergency exits	Cyber-physical and social
Side effects (n°6b)	PACS logs indicating that all users are deleted from the access control DB, crowds gathering behind closed exit doors, panic	Cyber-physical and social

Table 19: Characterisation of step n°16 of the attack (enacted): prevent people from exiting the premises

Criteria	Value	Characterisation
Type of traces	PACS DB, PACS logs, OS logs, crowds gathering behind closed exit doors, panic	Cyber, physical and social
Responsible / responding actor	CISO	Cyber

Table 20: Characterisation of step n°16 of the attack (detected, forensics): evacuation procedure inoperative

Intuitively, one would expect that the activity of a malware would be characterised as a purely cyber attack. However, the above characterisation shows that multiple criteria (e.g., supporting assets, effects, side effects and traces) deliver a physical, social and / or cyber-physical classification.

Step n°17: the bombs detonate

The time-triggered bombs detonate one by one, causing fire in the transformer station, and triggering a general evacuation of the power plant. Employees push the emergency buttons located near the

doors to exit the power plant. Based on the taxonomy defined in section §4, this step of the attack can be characterised as follows, cf. Table 21 and Table 22.

Criteria	Value	Characterisation
Threat actor	Time-triggered bombs	Physical
Supporting assets	Transformer station	Physical
Attack means	None2	-
Defence means	Microphone (records the explosion sounds) and sound analysis (raises an alert when sound is uncommon)	Cyber-physical
Location	TS restricted area	Inconclusive
Effects	Explosion, destroyed TS	Physical
Side effects	Noise, panic	Physical, social

Table 21: Characterisation of step n°17 of the attack (enacted): destroy the TS

Criteria	Value	Characterisation
Type of traces	Destroyed TS, fire	Physical
Responsible / responding actor	PSO	Physical

Table 22: Characterisation of step n°17 of the attack (detected, forensics)

The above characterisation shows that this elementary step of the attack is essentially physical, but with some social side effects, and cyber-related automated detection.

Case study conclusions

The application of our taxonomy to the case study highlights the complexity of characterising an attack step as a cyber or a physical attack, even though the overall attack is broken down into 17 small steps. Many attack steps are indeed characterised as cyber-physical. Worst, some attack characterisations based on our taxonomy are counter intuitive, e.g., badge creation (step n°7), or malware installation (step n°5) and execution (step n°16). The issue is not related to the granularity of the attack steps. Breaking down the overall attack into smaller elementary actions will not allow for a clearer characterisation. Indeed, in our use case, it is not possible to break the simple plugging of a USB key on a server (step n°4) into smaller steps, and yet, this step is characterised as cyber-physical using our taxonomy.

Could we solve the issue by considering only a subset of our criteria? In section §3, we recalled that the Knowww [26] characterises physical attacks by combining three features, corresponding to the supporting assets, the attack means and the target objective in our taxonomy. In our attack example, this subset of criteria is inconclusive. Typically, the target objective is physical, but the supporting assets and the attacks means can be physical, cyber or cyber-physical, depending on the attack step. Likewise, a short analysis shows that the subset of all our correct and complete criteria (i.e., supporting assets, side effects and responsible actor) are also inconclusive, i.e., they carry internal contradictions between the conclusions of each criterion.

As such, we conclude that it is impossible to systematically and formally discriminate cyber attacks from physical attacks. For some cases, it will just be obvious, but in many other cases, different

criteria lead to different conclusions, leaving us with the simple *cyber-physical* label. It is an unfortunate fact that we did not solve our initial question of being able to discriminate cyber and physical attacks with our taxonomy. However, this may not have been the right question from the start. Instead of trying to discriminate attacks, the current panorama of attacks should more pragmatically push organisations to adopt a holistic approach to cyber and physical security. The legal frameworks are already moving in that direction (cf. §6) and more generally, we will conclude that there are some profound trends pushing towards holistic approaches (cf. §7).

6. A LEGAL PERSPECTIVE ON PHYSICAL VS. CYBER ATTACKS: the NIS2 and the CERD

Law and policy related to physical and cyber attacks are multiple, ranging from national laws to technical standards This section briefly deals with the EU-level regulations and policy background and general observations on cyber and physical threats on CIs based on the NIS2 Directive [16] and the CERD [17]. We focus on these two legislations because they provide the minimum standards of harmonisation, meaning that states can provide for stricter measures and they were dealt within the aforementioned PRAETORIAN project.

Traditionally, critical entities have always been vulnerable to so-called *conventional threats*, e.g., natural or man-made accidental disasters, caused by human errors or by natural or technological causes [52] But as CIs' dependency on each other, and their reliance on networks of connected devices significantly increase cyber and physical security become essential [53–55]. As such, physical and cyber security efforts merge, particularly in the context of CIs with cyber components [56]. This section explains how the NIS2 Directive and the CERD approach physical and cyber attacks.[18].

The NIS2 does not define cyber attacks or cyber threats, although it refers to them in a number of instances. It defines network and information systems and cyber incidents. These definitions, and the obligations set out in the NIS2, illustrate that the NIS2 is primarily concerned with safeguarding the target of attacks (e.g. data transmitted via network and information systems) against the effects of these attacks (e.g. adverse impacts on network and information systems). The NIS2 does not attach particular consequences to whether an attack is physical or cyber in nature. It leaves the governance of physical and cyber attacks to the industry and to sector specific laws.

The CERD does not explicitly limit its scope to physical security[19]. . National strategies and sector specific laws implementing the CERD can define the specific security entities are obligated to take, which may be directed at physical security. The Recitals of the CERD refer to threats of varying nature, such as "physical risk due to natural disasters and climate change" and "evolving hybrid and terrorist threats" [17]. Under the CERD, Member States are to put in place a strategy for enhancing the resilience of critical entities. National authorities are to carry out a risk assessments within their territory. Such risk assessment should provide a report of natural and man-made risks for such essential services. Notably, hybrid threats or other antagonistic threats are listed amongst the risks that should be considered when producing the risk assessment [17].

[18] The definition of cybersecurity and cyber threats is adopted from the Cybersecurity act [69].

[19] CERD amended the Directive on the identification and designation of European Critical Infrastructures and the assessment of the need to improve their protection, ECI directive [70].

As such, the NIS2 and the CERD do not *per se* deal with cyber or physical security. They introduce measures to ensure the security of network and information systems and resilience of critical infrastructures. Their implementation can consist of measures to prevent or deal with cyber or physical attacks. The NIS2 and the CERD are meant to complement each other, with the former focusing on the security of network and information systems [16] and the latter on the resilience of critical entities [17]. The CERD and the NIS2 recognise that they are to be implemented in a complementary manner, "in light of the relationship between the physical security and cybersecurity of critical entities" [17]. Cybersecurity of critical entities will be subject to the NIS2. Measures to address the resilience of critical entities in respect of all hazards, whether natural or man-made, accidental or intentional will be defined by the Member State strategy adopted as part of the CERD.

6.1 Discussion: The NIS2 and the Cerd on Cyber vs. Physical Attacks

As mentioned above, in the context of CIs, the NIS2 and the CERD do not define or impose conditions for the assessment of cyber vs. physical attacks. How physical and cyber security are dealt with are left to sector specific legislation, Member State implementation of the NIS2 and the CERD, and to industry initiatives. For example, energy and transport sectors are already regulated by sector-specific Union legal acts [57]. Those legal acts contain provisions that relate only to certain aspects of resilience of entities operating in those sectors.

At the national level, there are national authorities that deal with cybersecurity and CI requirements in the CERD and the NIS2 in combination, which may result in considering physical and cyber security together, typically during audits and risk assessments. For example, in the electricity sector, the Danish Energy Agency is working towards an integrated implementation of NIS2 and CERD [58]. In practice, this means taking a holistic approach towards assessing risks related to both information technology and operational technology. This approach is currently applied by the Belgian Federal Public Service Mobility and Transport to implement the NIS and the ECI Directive, where audits look both into physical and cyber security [59]. One important motivation for this is the fact that cyber elements merge with operational infrastructure.

The NIS2 and the CERD foresee their complementary implementation to deal with both cybersecurity and CI protection, particularly because information technology elements are integrated into the operational infrastructure of critical entities. However, currently an EU level guidance on how the NIS2 and the CERD can be implemented in combination with respect to physical and cyber attacks is lacking. This lack of guidance results in enforcement and security gaps that may cause operational disruptions, safety incidents, as well as economic impacts [60]. This can lead to the disruption of critical operations, loss of sensitive data, and physical damage to equipment.

That being said, the NIS2 and CERD provide necessary tools to address the convergence of physical and cyber-attacks. Article 25 of the NIS2 and Article 16 of the CERD that encourage technical standards to ensure their convergent implementation can be used to set up common standards on the convergence between physical and cyber-attacks. In addition, ENISA can make use of its mandate under the Cybersecurity Act to set up and maintain the European cybersecurity certification framework on physical and cyber-attacks in relation to the NIS2 and the CERD by preparing the technical ground for specific certification schemes. Standardisation efforts should come with support from Member States, given the importance of ensuring continuity of the operation of critical entities and

the risk of cascading effects that can disrupt operation of critical infrastructures. Guidance can be useful for them to re-consider their design, governance and management of operational technology and information technology systems and to prevent security gaps in the future.

7. FINAL REMARKS

After analysing the available literature, we authors did not find any authoritative definition of cyber attacks and physical attacks and no unanimously accepted discriminant criteria to differentiate between cyber attacks and physical attacks. This state of fact motivated us to investigate possible criteria that could lead to a precise distinction between the two. In order to find a precise distinction between physical and cyber attacks, we approached the discrimination issue form both the attacker's and the defender's point of view. We identified eight main features that could be used as criteria to decide on the cyber or physical nature of the attack. These criteria were assessed for their efficacy by applying them on a real-life significant test case study taken from the EU PRAETORIAN project.

The application of the proposed taxonomy to the case study confirmed the complexity of characterising an attack step as a cyber or a physical attack. The approach of breaking down the overall attack into smaller elementary actions did not allow for a clearer characterisation and many attack steps remained characterised as cyber-physical. Our study showed that the technical split between cyber and physical attacks is not feasible. The frontiers between the two are blurred and approaching the issues from two completely separated silos lead to overlooking situations that cannot be characterised as purely cyber or purely physical. Enterprises should acknowledge this fact and reorganise their security governance to approach security in a holistic manner.

A significant testimony of the unification of cyber and physical threats is the evolution of the Incident Detection Message Exchange Format (IDMEF) [61]. IDMEF version 1 was cybersecurity oriented. IDMEF version 2 includes both cyber and physical incidents. This evolution was made in parallel with the change of the semantics of the 'I' in IDMEF. The 'I' of IDMEFv1 was for Intrusion, whereas it stands for Incident in IDMEFv2, which covers a larger scope, including intrusions. Also noteworthy, the standard uses the term Alert for the notification/message that a particular event/incident (or series of events/incidents) has occurred. The standard recalls that in physical incident detection systems, the term Alarm is often preferred, but that the two terms (i.e., Alert and Alarm) are sufficiently close to avoid misinterpretation.

Another significant testimony of the upcoming unification of cyber and physical threats lies with the H2020 EU-HYBNET project. One of the objectives of this project is to monitor developments in research and innovation activities applied to hybrid threats [62]. Scoping and analysing the selected innovation resulted in proposing the adoption of a Holistic Security Operation Centre (HSOC) in each CI [63]. This proposal relies on the conclusions of a paper by Mantzana et al. [64]. The authors analyse physical and cyber security related regulations and standards, operations, organisational and technical measures and, through the discussion on gaps and best practices identified, propose a global, cyber-physical security management and joint coordination approach through the establishment of a HSOC.

ENISA recently published a list of emerging cyber security threats for year 2030 [65]. The rise of advanced hybrid threats is one of the identified threats with the highest risk. ENISA predicts

that cyber attacks will become more sophisticated and match with physical attacks. ENISA concluded that it would lead to difficulties in detecting and defending against those attacks due to the complexity and the tendency to treat cyber and physical attacks individually. Once again, this conclusion acknowledges the necessity of merging cyber and physical. One of the biggest obstacles that could slow down such combined approach is the lack of skilled professionals who master both cyber and physical domains. In this regard, national competent authorities in some sectors oversee the implementation of the NIS2 and the CERD together, where audits are conducted to assess both cyber and physical risks [66]. In these cases, national competent authorities conduct audits with the presence of both physical security and cybersecurity experts.

According to the EU Military Vision and Strategy on Cyberspace as a Domain of Operations [66], cyberspace comprises the distinct but interrelated physical layer, logical layer and cognitive layer, which cannot be considered independently, but is one facet of the triad cyberspace, electromagnetic environment and cognitive environment. Pointing to the same direction, NATO's doctrine for cyberspace operations describes cyberspace in terms of three layers: physical, logical and cyber persona, where Cyberspace Operations (CO) always include the logical layer, but may also include activities or elements from the other two layers. According to [67], "previous national and EU initiatives have addressed the conceptualisation and development of technologies for the acquisition of situational awareness by focusing on the logical sub-layer of cyberspace (software, services, networks, interfaces, etc.) but there is a raising demand of military-focused solutions able to holistically understand the cyberspace as a whole, taking into account all the layers".

8. CONCLUSIONS

The main findings of this article are the following:

- Poorly classifying attacks as cyber or physical attacks creates technical implementation issues when developing intrusion prevention and detection tools, and governance difficulties for organisations wanting to buy tools and / or insure themselves against such attacks. The current blurry situation might also create security gaps, possibly implying legal compliance issues.
- There is no authoritative definition of cyber attacks and physical attacks in the state of the art, and thereof no unanimously accepted discriminant criteria to split cyber attacks from physical attacks, or to split cybersecurity from physical security.
- We proposed a fine-grained taxonomy to discriminate cyber attacks from physical attacks. This taxonomy includes eight main criteria with some sub-criteria, leading eleven criteria in total. These are: attack origin (1), including threat source (1a) and threat actor (1b); attack goal (2); nature of the attacked supporting asset, including its exploited vulnerabilities (3); means used (4), including attack means (4a) and defence means (4b); location of the attacker with respect to its target (5); consequences of the attack (6), in terms of direct effects (6a) and side-effects (6b); types of traces (7); defence responsible and/or responding actor (8). We analysed each criterion. We showed that five criteria are correct but incomplete (i.e., they are inconclusive in some cases), whilst three criteria (i.e., target objective, side effects and responsible actor) are both correct and complete. The last criteria (i.e., threat source and

location) are irrelevant, as it is impossible to decide on the cyber or physical nature of the attack based on these sole criteria.

- To strengthen our analysis, we tested the eleven criteria on a complex case study from the EU PRAETORIAN project. We concluded that it is impossible to systematically and formally discriminate cyber attacks from physical attacks. For some cases, it will just be obvious, but in many other cases, different criteria lead to different conclusions, leaving us with the simple *cyber-physical* label. It is an unfortunate fact that we did not solve our initial question of being able to discriminate cyber and physical attacks with our taxonomy. However, this may not have been the right question from the start. It is useless trying to discriminate attacks. We assert that the frontiers between cyber and physical attacks are blurred. Approaching the issues from two completely separated silos leads to overlooking situations that cannot be characterised as purely cyber or purely physical. Enterprises should acknowledge this fact and reorganise their security governance to approach security in a holistic manner.
- In parallel, we showed that the legal frameworks are also moving in the direction of holistic approaches, specifically at the national level, by considering the CERD and the NIS2 in combination. However, an EU level guidance on how the NIS2 and the CERD can be implemented in combination with respect to physical and cyber attacks is currently lacking. This lack of guidance may result in operational disruptions, safety incidents, as well as economic impacts. We assert that regulators should guide CIs operators and important and essential entities on the types of appropriate organisational measures, and on how these can be combined with technical measures to address the convergence between cyber and physical threats.

9. ACKNOWLEDGEMENTS

This work has received funding from the European Union's Horizon 2020 Research and Innovation programme under Grant Agreement No 101021274 (PRAETORIAN).

10. REFERENCES

References

[1] https://praetorian-h2020.eu/.

[2] https://www.cisa.gov/resources-tools/resources/cybersecurity-and-physical-security-convergence-action-guide.

[3] https://www.linkedin.com/news/story/le-risque-cyber-devenu-inassurable-5101425/.

[4] https://www.ft.com/content/63ea94fa-c6fc-449f-b2b8-ea29cc83637d.

[5] https://www.usine-digitale.fr/article/il-est-urgent-de-trouver-une-solution-aux-problemes-d-assurance-cyber.N1779877.

[6] https://itegriti.com/2022/compliance/lloyds-will-exclude-catastrophic-state-sponsored-attacks-from-its-cyber-insurance-plans/.

[7] https://www.intelligentinsurer.com/article/understand-risk-why-it-s-time-to-spice-up-your-cyber.

[8] https://en.wikipedia.org/wiki/Black_swan_theory.

[9] https://www.miris-insurance.com/.

[10] Network and Information Systems Directive, "Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union," Official Journal of the European Union,2016.

[11] General Data Protection Regulation (GDPR), "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC," Official Journal of the European Union,2016.

[12] https://www.oecd.org/finance/insurance/The-Role-of-Public-Policy-and-Regulation-in-Encouraging-Clarity-in-Cyber-Insurance-Coverage.pdf.

[13] https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=JOIN:2020:18:FIN.

[14] https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1596452256370&uri=CELEX%3A52020DC0605.

[15] https://www.eeas.europa.eu/sites/default/files /joint_communication_increasing_resilience_and_bolstering_capabilities_to_address , _hybrid_threats.pdf.

[16] NIS 2 Directive, "Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (E," European Parliament and of the Council, 2022.

[17] https://eur-lex.europa.eu/eli/dir/2022/2557/oj.

[18] https://digital-strategy.ec.europa.eu/en/news/new-stronger-rules-start-apply-cyber-and-physical-resilience-critical-entities-and-networks.

[19] V. M. Igure and R. D. Williams, "Taxonomies of Attacks and Vulnerabilities in Computer Systems," IEEE Communications Surveys & Tutorials,2008;10:6-19.

[20] R. Derbyshire, B. Green, D. Prince, A. Mauthe and D. Hutchison, "An Analysis of Cyber Security Attack Taxonomies," in European Symposium on Security and Privacy Workshops (EuroS&PW),2018.

[21] https://capec.mitre.org/documents/schema/.

[22] IEC 62351, "Power Systems Management and Associated Information Exchange – Data and Communications Security," International Electrotechnical Commission, 2007.

[23] IEC 62443, “Industrial Communication Networks - Network and System Security,” Industrial Automation and Control System Security Committee of the ISA.

[24] https://www.nerc.com/ pa/Stand/Glossary%20of%20Terms/Glossary_of_Terms.pdf. [Accessed 27 2 2023].

[25] https://en.wikipedia.org/wiki/Physical_security. [Accessed 11 01 2023].

[26] https://knowww.eu/nodes/5bd5bfdd7bb7bca48fe42d18.

[27] Colorado Governor’s Office of Information Technology, “Supplemental Guidance Colorado Information Security Policies”.

[28] K. Lemke and C. Paar, Encyclopedia of Cryptography and Security, Boston, MA: Springer, 2015.

[29] https://www.irmi.com/term/insurance-definitions/cyber-physical-attack.

[30] M. Yampolskiy, P. Horvath, X. D. Koutsoukos, Y. Xue and J. Sztipanovits, “Taxonomy for Description of Cross-Domain Attacks on Cps,” in Second ACM International Conference on High Confidence Networked Systems, 2013.

[31] M. Yampolskiy, P. Horváth, X. D. Koutsoukos, Y. Xue and J. Sztipanovits, “Language for Describing Attacks on Cyber-Physical Systems,” International Journal of Critical Infrastructure Protection,2015:40-52, .

[32] A. Humayer, J. Lin, F. Li and B. Luo, “Cyber-Physical Systems Security - A Survey,” IEEE Internet of Things Journal,2017;4:1802-1831.

[33] P. F. Roberts, “Zotob, Pnp Worms Slam 13 Daimlerchrysler Plants,” eWeek,2005.

[34] J. Depoy, J. Phelan, P. Sholander, B. Smith, G. Varnado and G. Wyss, “Risk Assessment for Physical and Cyber Attacks on Critical Infrastructures,” in Military Communications Conference (MILCOM), 2005.

[35] https://attack.mitre.org/docs/ATTACK_for_ICS_ Philosophy_March_2020.pdf.

[36] https://attack.mitre.org/matrices/ics/.

[37] F. G. Hoffman, Conflict in the 21st Century: The Rise of Hybrid Wars, Arlilngton, Virginia: Potomac Institute for Policy Studies, 2007:1-72.

[38] https://www.nato.int/cps/en/natohq/topics_156338.htm.

[39] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016JC0018.

[40] E. Bajarūnas, «Addressing Hybrid Threats: Priorities for the EU in 2020 and Beyond,» European View, 2020;19,62–70, .

[41] European Commission, «Delivering on the European Agenda on Security to Fight Against Terrorism and Pave the Way Towards an Effective and Genuine Security Union. Communication, Com (2016) 230 Final,» European Commission, Brussels, 2016.

[42] Communications-Electronics Security Group (Cesg), "Hmg IA Standard Numbers 1 & 2, Information Risk Management," National Technical Authority for Information Assurance, Cheltenham, Gloucestershire, UK, 2012.

[43] Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), EBIOS Risk Manager, version 1.0 ed., Paris: ANSSI,2019:49.

[44] https://doi.org/10.1007/978-1-4419-5906-5_511.

[45] https://www.geeksforgeeks.org/
difference-between-active-attack-and-passive-attack/.

[46] https://googleprojectzero.
blogspot.com/2015/03/exploiting-dram-rowhammer-bug-to-gain.html.

[47] A. Tang, S. Sethumadhavan and S. Stolfo, "Clkscrew: Exposing the Perils of Security-Oblivious Energy Management," in 26th USENIX Security Symposium, Vancouver, BC, Canada, 2017:16–18.

[48] P. Pessl, D. Gruss, C. Maurice, M. Schwarz and S. Mangard, "Drama: Exploiting Dram Addressing for Cross-Cpu Attacks," in 25th Usenix Security Symposium, Austin, Texas, USA,2016.

[49] M. Lipp, M. Schwarz, D. Gruss, T. Prescher, W. Haas, A. Fogh, J. Horn, S. Mangard, P. Kocher, D. Genkin, Y. Yarom and M. Hamburg, "Meltdown: Reading Kernel Memory From User Space," Communications of the ACM, 2020;63:46-56.

[50] https://en.wikipedia.org/wiki/Locard%27s_exchange_principle.

[51] F. Bouzon, P. Carer, F. Guyomard and J. Ma, "Use Cases and Pilot Scenario Definition (d2.3)," Protection of Critical Infrastructures From Advanced Cyber-Physical Threats (PRAETORIAN project).

[52] P. Tessari and K. Muti, "Strategic or Critical Infrastructures, a Way to Interfere in Europe: State of Play and Recommendations," European Parliament Policy Department for External Relations, Brussels,2021.

[53] https://www.enisa.europa.eu/.

[54] https://www.enisa.europa.eu/publications/definition-of-cybersecurity. ,

[55] https://www.europarl.europa.eu/RegData
/etudes/BRIE/2019/642274/EPRS_BRI(2019)642274_EN.pdf.

[56] P. Tessari and K. Muti, "Strategic or Critical Infrastructures, a Way to Interfere in Europe: State of Play and Recommendations," European Parliament Policy Department for External Relations,2021.

[57] https://www.acer.europa.eu/Recommendations
/Revised%20Network%20Code%20on%20Cybersecurity%20(NCCS)_1.pdf.

[58] https://nisduc-cloud.list.lu/index.php/s/o6Y7g2PdM4yS9sY.

[59] https://nisduc-cloud.list.lu/index.php/s/WAk6Bixqpy7zY8Y.

[60] https://www.nisduc.eu/fileadmin/files/resources /D3.3-NISDUC_Lessons_learnt_vol.3.pdf.

[61] https://idmefv2.github.io/.

[62] https://euhybnet.eu/.

[63] EU-HYBNET, «First Report on Strategy for Innovation Uptake, Industrialisation and Research,» 2021.

[64] V. Mantzana, E. Georgiou, A. Gazi, I. Gkotsis, I. Chasiotis and G. Eftychidis, "Towards a Global Cis' Cyber-Physical Security Management and Joint Coordination Approach," Cyber-Physical Security for Critical Infrastructures Protection. CPS4CIP 2020. Lecture Notes in Computer Science, vol. 12618, 2021.

[65] https://www.enisa.europa .eu/publications/enisa-foresight-cybersecurity-threats-for-2030.

[66] https:// www.statewatch.org/media/2879/eu-eeas-military-vision-cyberspace-2021-706-rev4.pdf.

[67] https://defence-industry-space.ec.europa.eu/system/files /2023-03/C_2023_2296_EDF Financing Decision and Work Programme 2023 Part 2 (2).pdf.

[68] https://www.wired.com/2017/04/just-pair-11-radio-gadgets-can-steal-car/.

[69] Cybersecurity Act, "Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on Enisa and on Information and Communications Technology Cybersecurity Certification and Repealing Regulation (EU) No 52," 2019.

[70] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32008L0114.