smart cities

MDPI

Review

Cyber Resilience and Incident Response in Smart Cities: A Systematic Literature Review

Gabriela Ahmadi-Assalemi [1], Haider Al-Khateeb [1,*], Gregory Epiphaniou [2] and Carsten Maple [2]

[1] Wolverhampton Cyber Research Institute (WCRI), School of Mathematics and Computer Science, University of Wolverhampton, West Midlands WV1 1LY, UK; G.Ahmadi-Assalemi@wlv.ac.uk
[2] Warwick Manufacturing Group (WMG), University of Warwick, International Manufacturing Centre, Coventry CV4 7AL, UK; Gregory.Epiphaniou@warwick.ac.uk (G.E.); CM@warwick.ac.uk (C.M.)
* Correspondence: H.Al-Khateeb@wlv.ac.uk

Received: 11 July 2020; Accepted: 9 August 2020; Published: 13 August 2020

Abstract: The world is experiencing a rapid growth of smart cities accelerated by Industry 4.0, including the Internet of Things (IoT), and enhanced by the application of emerging innovative technologies which in turn create highly fragile and complex cyber–physical–natural ecosystems. This paper systematically identifies peer-reviewed literature and explicitly investigates empirical primary studies that address cyber resilience and digital forensic incident response (DFIR) aspects of cyber–physical systems (CPSs) in smart cities. Our findings show that CPSs addressing cyber resilience and support for modern DFIR are a recent paradigm. Most of the primary studies are focused on a subset of the incident response process, the "detection and analysis" phase whilst attempts to address other parts of the DFIR process remain limited. Further analysis shows that research focused on smart healthcare and smart citizen were addressed only by a small number of primary studies. Additionally, our findings identify a lack of available real CPS-generated datasets limiting the experiments to mostly testbed type environments or in some cases authors relied on simulation software. Therefore, contributing this systematic literature review (SLR), we used a search protocol providing an evidence-based summary of the key themes and main focus domains investigating cyber resilience and DFIR addressed by CPS frameworks and systems. This SLR also provides scientific evidence of the gaps in the literature for possible future directions for research within the CPS cybersecurity realm. In total, 600 papers were surveyed from which 52 primary studies were included and analysed.

Keywords: cyber–physical systems; mobility; critical national infrastructure; digital citizens; smart homes; healthcare; energy

1. Introduction

Industry 4.0, synonymously known as cyber–physical production systems (CPPSs), is a concept formed in 2011 at the Hannover Fair to describe how cyber–physical systems (CPSs) can be applied within production and manufacturing industries with enabled automation [1–4]. From the inception of the visionary notion specifically for factories and large-scale enterprises, CPSs' reach have extended beyond production enterprises linking the Industry 4.0 concept with aspects of smart city initiatives [3,4]. Smart cities have evolved and transformed over the past two decades becoming deeply integrated within the society facilitating an interconnected digital environment [3–5]. The estimated growth of the urban population is estimated to reach 5 billion by 2030 globally [6]. A variety of definitions for the term "smart city" [7–12], its sectors and components [3,13–17], the variants [8] and concepts of the term "smart" [6,14,18–21] have been suggested. The description of smart cities is heterogeneous

and commonly agreed facets converge sustainability, ICT-based technology and community needs. Therefore, in this study, we consider the smart city as an urban space using technology and resources innovatively, intelligently and securely to improve the lives of its citizens focusing on the spectrum of attributes that improve the cyber resilience of smart cities.

A key component of smart cities, CPSs can be described as smart, embedded and networked systems within production systems [22]; a tangible element that is not completely controlled by an automated system and a cyber element that focuses on the digital information form CPS entities capable of autonomous interaction regardless of human supervision [23]. Furthermore, these complex and growing networks of connected objects incorporate human-users and form complex cyber–physical–natural (CPN) ecosystems interrelating systems, software, people and services. As such, a problem within this complex cyberspace, including cybersecurity challenges, can have a cascading effect on the entirety of the ecosystem [24,25].

The motivation and tactics of the cyber threats landscape shifted from individuals hobby hacking to gain kudos amongst their peers toward well-organised cybercrime [26–28]. The motivations are often intensified by the possibilities to gain sensitive information, which can be used in subsequent attacks including cyberattacks against industrial control systems (ICSs) or critical national infrastructure (CNI). Verizon reported in their 2016 Data Breach Investigation Report the outcome of the investigation of 500 cybersecurity incidents in over 40 countries. In 89% of the cases, the key motives reported were described as "financial" and "espionage" fixated on targets including manufacturing, healthcare, utilities and public services by organised crime and state-affiliated groups. Many of these attacks had a secondary motive to aid an intrusion of another target [29,30]. This class of attacks known as advanced persistent threats (APTs) characterise a well-resourced group of attackers that carry out multi-stage and often multi-year persistent targeted campaigns. Traditional incident response (IR) methods fail in mitigating APTs because they assume successful intrusion before IR takes place. A kill chain model enables one to map such campaigns, identify patterns linking individual intrusions and through an iterative intelligence gathering enables the development of a resilient intelligence-driven mitigation approach [31]. In 2018, although the key motives remained largely unchanged, the most noteworthy attack vectors reported by the European Union Agency for Network and Information Security (ENISA) included malicious attachments, URLs in emails targeting the human element, web browser-based malicious scripts, malvertising, exploit kits and password reuse or weak service credentials in Internet exposed assets [26]. In 2019, law enforcement agencies responded to more attacks on CNI than we ever saw before; this trend was highlighted as a key emerging threat by Europol [32]. CNI such as smart energy, water or transport are complex, large-scale interconnected CPSs converging physical and cyber domains and utilise geographically dispersed ubiquitous distribution networks, which extend beyond the boundary of a smart city, often across national borders and legal jurisdictions.

The rise of cybercrime has been greatly facilitated by the proliferation of modern advanced electronic communication technologies and the integration of IoT with physical systems [17,28,33]. High profile cyberattacks on ICSs have been well reported for some years, such as the Stuxnet malware targeting the Iranian nuclear plant [34], the attack on the Ukrainian power grid [35] or Norsk Hydro, a renewable energy supplier and the world's largest aluminium producer, which was compromised by the LockerGoga ransomware [32]. In case of a successful cyberattack, the disruption of power, water or fuel supplies to these facilities could have a potentially serious socio-economic impact including civilian unrest; however, consequences could be more profound. For example, in the widely reported Kemuri Water Company attack, the mixture of chemicals used to treat a water plant was altered. In this attack, the sensors responsible for monitoring the water treatment plants were compromised [29]. Due to the distributed nature and heterogeneity of CPSs, human interactions and the omnipresence of the underpinning technologies create hugely diverse attack vectors which increase the threat of cyberattacks on critical systems.

Comparatively, smart cities, smart healthcare and smart homes are in the earlier stages of development with several evolving projects including initiatives to improve the wellbeing of elderly

people through early changes detection [36] or application of digital forensics as a service in the context of smart homes [37]. Furthermore, connected appliances and app-based utility management will become the norm in connected homes [38] whilst automated congestion control, smart traffic lights or parking [39,40] will be part of smart cities' digitalization projects [14]. The cyber challenges in these smart sectors differ but the effect could be just as profound. For example, the ransomware attack against the San Francisco Municipal Transportation Agency's transport service only resulted in financial impact [41]. Accidents caused by cyberattacks including GPS ghosting, hijacking command and control systems, ransomware or attacks targeted at sensors, actuators or controllers could result in serious accidents and increase the pressure on healthcare systems. Digital transformation utilising mobile and emerging technologies such as artificial-intelligence (AI)-enabled networked medical devices or wearable health sensors are identified as enablers for healthcare organisations. However, healthcare does not escape cyberattacks as learnt from the WannaCry incident in May 2017 affecting over 300,000 computers, some of which belonged to 80 National Health Service (NHS) Trusts across the UK [26,32,42].

Due to the attacks becoming more sophisticated and targeted, the countermeasures also need consistency and coordination [5,26,28,32]. Therefore, a new paradigm must address cyber threats and cybercrime. Formulating cyber resilience to counter cybersecurity threats is required to resist cyberattacks and continue to function effectively under adverse conditions [43]. Accepting that not all cyberattacks are avoidable and computer-related crime is on the increase, the IR becomes an important component of CPS security management [32] including the need for digital evidence (DE). Forensic DE gathering must be carried out without compromising the integrity and authenticity of the DE to ensure admissibility in a court of law [44]. Therefore, the cybersecurity paradigm needs to shift to withstand cyberattacks, to function effectively under adverse conditions and support digital forensic investigations by producing DE that is admissible in the court of law. Collaborative practice and interdisciplinary approaches across smart sectors based on threat information sharing could increase situational awareness and help deal with potential threats or incidents more effectively.

Although CPS-related research is an active area, there seems to be substantially less empirical research available on frameworks and systems that address CPS in smart cities. For example, the following study [45] defines its framework as a risk-based approach to reducing cybersecurity risk consisting of three tiers: core, profile and implementation. Another study [46] defines a CPS framework as activities and outputs that support CPS engineering, which provides not a one-size-fits-all approach but a flexible way to address cybersecurity across the physical, cyber and people dimensions. Therefore, to make a meaningful contribution, we use a broad definition for frameworks as a common carefully designed organising structure of multiple approaches [47–49]. Furthermore, systems described by the National Institute of Standards and Technology (NIST) as a combined set of complex and coherent elements that constitute a use-case [46] can operate in different smart city sectors creating highly complex systems of systems. Systems can be represented by scientific modelling to describe hypothetical behaviour of phenomena that are challenging to observe directly. To help discover contributions in the literature of the specific research area we include systems to gain a deeper understanding of addressing support for cyber resilience across the physical, cyber and people dimensions in cross-sector applications within smart cities [50,51].

Specifically, concerning frameworks and systems that address cyber resilience and modern digital forensics and incident response (DFIR), there appears to be lack of available systematic literature review (SLR) based on recognised methodology, comprehensive protocols and quality assessment. For instance, to identify how CPS-related frameworks and systems support cyber resilience and to determine the support for modern DFIR in smart cities it is important to conclude what research has been published and systematically review relevant and available studies. Therefore, one of the key objectives of this study is to identify the current gaps in this research area. Overarchingly, the focus of this paper is on reported empirical evidence in existing literature concerning cyber resilience and DFIR support in CPSs across smart city sectors. Traditionally, "resilience" in a mechanical context was

the materials' resistance to shock, in the conventional networking context resilience focused on fault tolerance; however, the scope of this term extends to the cybersecurity discipline. In this study, we consider cyber resilience as the ability of the frameworks addressing smart cities to resist cyberattacks across the physical and digital domains regardless of an external or insider attack [43,52–54].

A small number of SLR studies in the realm of CPS have been published. These are outlined to examine the difference between the authors' focus on topics and our research. The author of [55] performed an SLR focusing on smart grid and related cybersecurity. In this study, the author presents results aimed at addressing cybersecurity by identifying all standards which define cybersecurity requirements for smart grids and reviews applicable standards and guidelines. In reference [56], the authors provide analysis to address cybersecurity issues in an Industry 4.0 context and focus on the physical Internet-connected systems. The authors concentrated on four areas, the definition of concepts relevant to Industry 4.0 and cybersecurity, the industrial focus, the characterization of cybersecurity and the management of the cybersecurity issues. Authors in reference [57] presented their SLR findings concerning smart cities focusing on instrumented, interconnected and intelligent systems investigating four areas including security. One of the authors' conclusions was that little was mentioned in the newly emerging security and privacy challenges. Although the studies into this growing area of research provide valuable knowledge consolidation, they answer questions about the wider use of CPS and related cybersecurity. No other SLR on this research topic was found by the authors during the preparation of the study. The focus of our SLR remains specifically on CPS-related cyber resilience and modern DFIR informed by cyber threat intelligence (CTI) to strengthen and accelerate the cyber defence in smart cities.

Narrative reviews were found to focus on various Internet of Things (IoT) aspects and applications addressing challenges, threats and solutions. For example, the authors in reference [58] provided a brief review of IoT concepts and models. The paper focused on the IoT network model and related modelling challenges from the interconnections' perspective and briefly discussed the concept of interdependent infrastructure resilience. Another recent study investigated the autonomy, integration and level of intelligence in emerging applications related to CPSs across a range of application domains in smart cities [59] including big data challenges and data and communication security. Further, the authors explored the intelligence and interconnectivity of systems into a shared environment from a simulation perspective. Interestingly, the study concluded that the security of collected data and distributed systems are a persistent challenge that must be continually addressed. They expressed the need to design systems with agility to react to the changing security landscape. A study focusing on the IoT from the edge computing perspective was published in reference [60]. The focus of this study was on improving IoT networks' performance utilising edge computing exploring the relevant confidentiality, integrity and availability strategies. Another survey [61] examined the integration of the IoT and fog/edge computing. The paper clarified the difference between CPSs and the IoT and investigated the relationships and issues affecting the IoT and fog/edge computing; however, the paper's approach remained high-level and general. All the previous studies address broader aspects related to the IoT, but do not specifically investigate CPSs with a focus on improving cyber resilience, the value of CTI- or CPS-specific DFIR support in smart cities. The field of research related to CPSs is still emerging, but the advancement is accelerating. Therefore, a comprehensive SLR is required focusing on ways that current CPSs deal with cyber resilience and DFIR to guide future research.

This paper's main aim is to provide a systematic literature review (SLR) that consolidates primary studies' research investigating what empirical evidence has been reported for existing frameworks and systems that address CPS cyber resilience in smart cities. Second, we investigate how current CPS applications address modern DFIR. Finally, we explore existing integration proposals or applications that leverage CPSs across smart city sectors to improve digital forensics. We critically examine existing research and use the insights to conclude with suggestions for future research. The remainder of this paper covers our methodology in Section 2 which also discusses the research questions and the protocol including the data extraction strategy. Section 3 contains the results, analysis and key findings

from the included primary studies followed by a discussion in Section 4. Finally, the conclusion and future research suggestions are in Section 5.

2. Materials and Methods

The aim of this study was achieved with an evidence-based systematic literature review (SLR) as the means to objectively address our research questions. The protocol is based on the SLR guidelines for the computer engineering discipline proposed by Kitchenham and Charters [62]. These guidelines, which aim to present a rigorous and credible methodology, are based on three key phases: planning, conducting and reporting, as demonstrated in Figure 1. We demonstrate the discreet activities in each phase in the subsequent sections to allow replication of findings. Summarily, the core aspects of the systematic review protocol, the key contributions and the research questions are identified within the planning phase. The conducting phase consists of identifying the search strategy including the selection criteria for the primary studies, selection procedure, the search strings and the quality assessment criteria. This phase involves the development of the data extraction strategy, data synthesis and critical analysis. Finally, the information dissemination strategy is considered in the reporting phase. Each phase of the SLR is conducted iteratively to ensure a comprehensive evaluation. To maintain objectivity and mitigate bias, each phase was subject to a review and an approval process between the team before moving onto the next phase.

Figure 1. Phases conducted in this systematic literature review (SLR).

2.1. Research Questions and Rationale

The main aim of this research is to identify and present scientific evidence of gaps in current research and help inform the direction for further research. The aim can be achieved by answering the following three research questions (RQs):

RQ1: How do existing frameworks and systems that address CPSs in smart cities support cyber resilience and what empirical evidence has been reported? Use cases and application of CPSs have diversified, and complexities of these ecosystems have evolved. In addition to frameworks, we investigate how complex systems support cyber resilience identifying commonalities. Within the many diverse definitions used in existing studies addressing smart cities [7–12] and the numerous terminologies used in literature to describe frameworks and systems [51,52,63–65], providing an answer to RQ1 helps us conclude a list of all existing and relevant frameworks and systems that address CPSs in smart cities supporting cyber resilience as defined by the scope of this SLR.

RQ2: How do the identified frameworks and systems in smart cities address modern digital forensics and incident response (DFIR)? Application of DFIR in the context of a smart city is a new field of study [37]. Whilst the research focuses on the applications of IoT-enabled CPSs, smart cities are found to be vulnerable to cyberattacks [40]. It is acknowledged that DFIR methodologies are lacking in smart city sectors [17,66] and research suggests that DFIR faces more challenges in smart cities than other forms of digital breach investigations [67]. However, apart from the complexity to the cyberspace, the IoT enabled CPSs to create opportunities to facilitate modern DFIR [44]. RQ2 investigates how the components of the CPS frameworks help address modern DFIR.

RQ3: What are the current cross-sector proposals or applications in smart cities that attempt to utilise interactions in CPSs for the purpose of improving DFIR? This RQ explores the transferable solutions and cross-sector interactions between smart buildings, smart homes, smart healthcare, smart energy and others as illustrated in Figure 2. Despite digitalisation in smart cities, information security strategies are limited to the sector boundary with little evidence of cross-sector information security practice sharing [28]. We draw on the use of the term of cross-sector partnerships in reference [68] as intensive and long-term interactions between organisations from at least two sectors such as business and healthcare. Throughout this study, cross-sector collaborations are used as interactions to adopt, share or coordinate cyber defence practice between at least two different smart city sectors. To address the existing and emerging cyberattacks, transferable and innovative solutions should emerge from individual sectors within a smart environment to support modern digital forensics [28,68]. RQ1, RQ2 and RQ3 help uncover key themes and gaps in current literature and suggestions for future research direction.

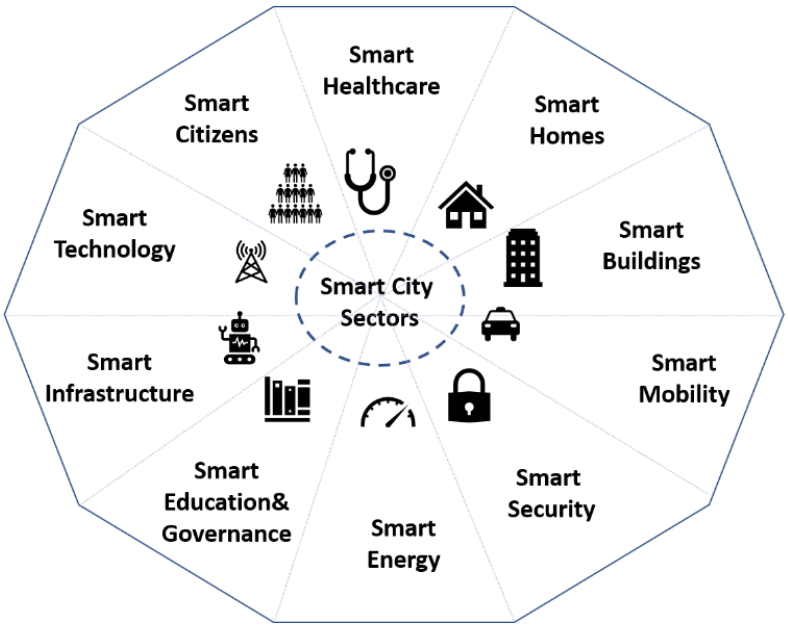

Figure 2. Core smart city sectors.

The PICOC (population, intervention, comparison, outcomes, context) criteria as demonstrated in Table 1 is used from an engineering point of view, as proposed by Kitchenham and Charters [62] to frame the research questions effectively.

Table 1. Application of PICOC criteria [59] to the research questions (RQs).

PICOC Criteria	Criteria Description
Population	Frameworks addressing smart cities
Intervention	Digital forensic incident response (DFIR) frameworks that support cyber resilience
Comparison	Frameworks addressing cyber resilience
Outcomes	Scope, technique, security application and sector of the studies analysed
Context	Academic research

2.2. Primary Studies' Data Sources and the Search Strategy

Digital library (DL) sources for computer science research publications were used. To help answer the RQs, keywords representative of the research topic were pre-defined and a search string was constructed using Boolean operators, key terms and synonyms to fetch all relevant studies. The Boolean operators were limited to AND and OR. The following search string was used:

('Cyber Physical Systems' OR 'Cyber-Physical Systems' OR 'CPS' OR 'Cyber Physical Object' OR 'CPO' OR 'smart device' OR 'IoT device') AND ('cybersecurity' OR 'cybersecurity' OR 'cyber-resilience' OR 'resilience') AND ('smart cities' OR 'smart city') AND ('model' OR 'modeling' OR 'technique' OR 'framework' OR 'information modeling' OR 'modeling technique' OR 'analytical modeling' OR 'reference architecture' OR 'reference model' OR 'Security Solutions' OR 'IoT Architecture').

The DLs used in this SLR were the Institute of Electrical and Electronics Engineers (IEEE), Association of Computing Machinery Digital Library (ACM DL), Science Direct, Web of Knowledge and Scopus. The search string was aligned to the built-in options within the DLs' search engines to filter the results. Where possible, searches were performed to match the search string from the title, abstract, keywords, and the full text. The search of the specified DLs concluded by 5 April 2019 taking into consideration all studies returned by the defined search string published to that date. In addition to the set of studies produced through the search of the DLs, we applied a snowballing approach in our search strategy, as outlined by Wohlin [69], which produced a further set of relevant studies. This was a manual process applied to the studies collected by the pre-identified search criteria until no further studies met the inclusion criteria. Subsequent to identifying studies from the specific data sources using the defined search string, the rest of the protocol outlined in Sections 2.3–2.7 was applied to the studies identified by the initial search.

2.3. Selection Criteria

Rigorous inclusion and exclusion criteria, as defined in Table 2, were applied to the produced set of studies from the DLs to ascertain that only relevant studies are retained in response to the research questions.

Table 2. Inclusion and exclusion criteria for the primary studies.

Inclusion Criteria (IC)	Exclusion Criteria (EC)
IC1: Must be a peer-reviewed, English language primary study. **IC2:** Must contain cyber–physical system (CPS)-specific information related to cyber resilience, modern DFIR or frameworks. **IC3:** Must include empirical evidence related to the cyber resilience security application and use of CPSs.	**EC1:** Duplicate studies. **EC2:** Study is not a framework that supports cyber resilience or DFIR.

Included studies must satisfy all inclusion criteria. I.e., they must be primary, peer-reviewed, written in English and contain appropriate information on new applications or development of an existing mechanism for cyber resilience, modern DFIR or framework in CPSs, providing empirical findings.

2.4. Selection Process

The selection process consisted of three key phases as demonstrated in Figure 3. The authors have critically reviewed this.

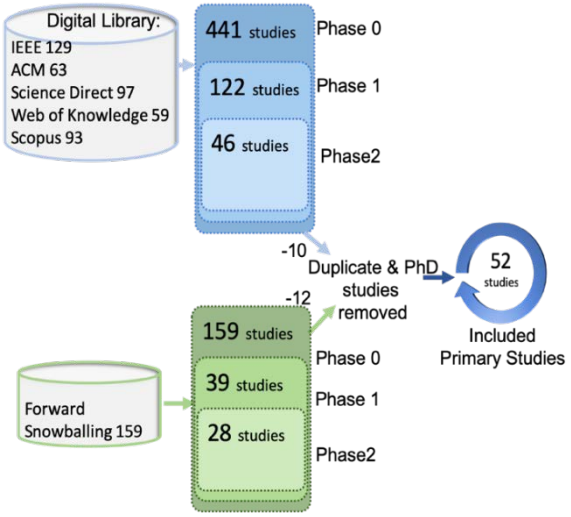

Figure 3. Primary studies selection process. IEEE—Institute of Electrical and Electronics Engineers; ACM—Association of Computing Machinery.

Phase 0—Keyword Filtering. During this phase, the identified search string was applied to each of the DLs utilised returning a combined result of 441 research studies. These studies were passed through to the next phase.

Phase 1—Title, Indexing Keywords, Abstract, and Conclusion Filtering. Following the initial keyword filtering, in phase 0, the titles, indexing keywords, abstracts and conclusion were scrutinised against the inclusion criteria. Studies showing relevance to the research topic were included in the next phase. In this phase, 319 studies were excluded and 122 were put through to the final phase.

Phase 2—Full-Text Filtering. The full texts of the 122 studies were read. After applying the selection criteria in this final phase, some studies were excluded for several reasons. For example, references [37,70,71] did not include an empirical study, references [72–74] at the time of review were not peer-reviewed publications, reference [75] is not an English language study, reference [76] is a poster, the focuses of references [77–79] were not specific to CPS cyber resilience or modern DFIR. Additionally, 10 studies were identified as duplicates and excluded from the final selection list. Snowballing identified an additional 159 studies. After applying the selection process, these studies were reduced to 19 after excluding nine duplicate studies and three PhD theses.

The final list of primary studies included in this SLR resulted in 52 articles, as shown in Figure 3.

2.5. Quality Assessment

Motivated by the guidance in reference [62], a checklist was developed according to references [80,81] to make sure all included studies satisfy quality assessment (QA) criteria. This evidence-based approach assesses the validity of experimental data and reduces bias. The following QA criteria were applied:

Phase 1: CPS. The study must be focused predominantly on CPS security or the application of the CPS framework to a specific cyber resilience problem and appropriately documented.

Phase 2: Context. The context of the study must be provided in sufficient detail to accurately interpret the research.

Phase 3: Detail. The framework details are critical to answering RQ1 and RQ2. Sufficient detail about the approach to build the framework and comparison with other approaches must be presented clearly in assisting to answer RQ3.

Phase 4: Data. Sufficient detail about the type of training and test data identified and how the data was acquired, measured and reported must be provided clearly to determine the accuracy of the results reported.

2.6. Validation Process

A random set of 30 primary studies from the pool of studies were selected and had the inclusion/exclusion criteria re-applied to validate the effectiveness and the objectivity of the process application. A further 30 random primary studies were selected from the pool of studies and had the QA criteria applied to validate the effectiveness and the application of the quality assessment process.

2.7. Data Extraction Strategy

The data extraction was applied to the final 52 primary studies. Initially, the process and format were trialled on a subset of studies before extending the process to all included studies. The data were categorized, stored in a spreadsheet and tabulated using the following characteristics.

Context: year of publication, type of article, application of the study, sector, model type and security approach.

Qualitative data: were recorded including the conclusion and future research directions provided by the authors.

Quantitative data: experiment observations were noted including the technique and dataset source.

To conclude, the protocol used in this SLR process, which is based on Kitchenham and Charters [62] guidelines, was rigorously applied and documented to objectively address the research questions. The resulting set of primary studies after applying the protocol are summarised in Figure 3. Therefore, this SLR consolidates previous research within the defined scope; however the methodology used can be applied iteratively to studies beyond this SLR's defined scope as an extension and update of literature reviews to further expand the scientific body of knowledge.

3. Results Analysis and Discussion

3.1. Primary Studies

Applying our protocol revealed that no primary studies were published before 2011, suggesting that cyber resilience and DFIR addressed by CPS frameworks and systems in smart cities is a recent paradigm. Nevertheless, as Figure 4 shows, there is an upward trend in CPS-related research within smart cities addressing cyber resilience and modern DFIR, which indicates that this has emerged into an active research area. This trend will likely continue as the first quarter (Q1) of 2019 is just over half of the studies published in 2018, as demonstrated in Table 3.

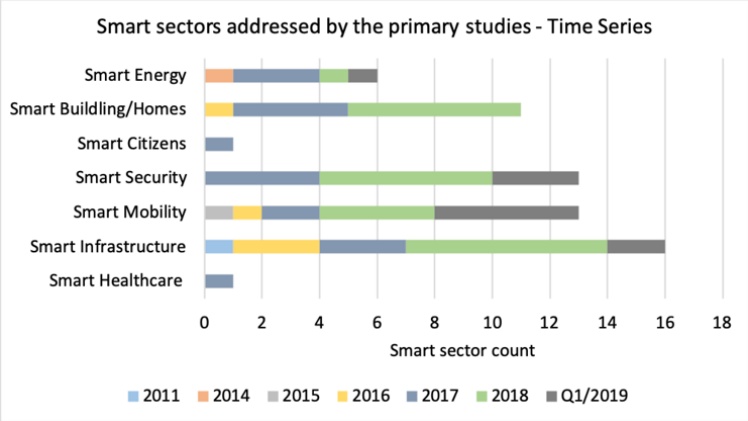

Figure 4. Smart sectors addressed by the primary studies time series.

Table 3. Primary studies' distribution by type. Journal—J or conference—C and publication year.

Year	11	14	15	16	17	18	Q1/19	Total Studies
%/year	2%	2%	2%	10%	23%	40%	21%	52
J			1			13	10	24
C	1	1		5	12	8	1	28

3.2. Keyword Analysis

To help establish common themes amongst the primary studies, a keyword analysis including all 52 primary studies was carried out. The frequency of specific keywords appearing in the primary studies is shown in Table 4. As the table captures, the second most frequently used keyword in the dataset is "System", closely followed by "Security", "Internet of Things" and "Cyber-Physical Systems" (CPSs). This shows an increasing research interest in the security of CPSs in the context of the IoT. Furthermore, the keyword "framework" indicates that it is an active but still emerging area of research interest in the context of CPS cyber resilience and support for DFIR. The dataset also demonstrates that there is a significant disparity in the research interests in "detection" compared to other aspects of CPS security. The keywords used in established investigation models and frameworks to define these investigation phases including "Response", "Recovery" or "Prevention" rank lowest in the dataset. In addition, "Forensics" and "Cyber Resilience" rank also low in the dataset indicating potential areas of further research requirement.

Table 4. Primary studies' keyword analysis.

Keyword	Occurrence	In Studies
Attacks	4165	50
System(s)	3650	52
Security	2272	51
Internet of Things/IoT	2024	36
Model(s)(ing)	2002	52
Cyber-Physical Systems	1857	52
Smart	1750	52
Device(s)	1610	50
Detection	1193	47
Approach(es)	589	50
Method(s)	579	49
Analysis	579	52
Framework(s)	491	44
Technique(s)	461	44
Cyber * resilience/resilience	251	26
Processing	242	38
Architecture	239	43
Forensic(s)	214	16
Cyber * security	179	37
Response	156	33
Incident(s)	41	15
Prevention	38	20
Recovery	32	10

The asterisk (*) in this table is used to represent the variants considered during the keyword search: space, dash or continuous word without any space i.e., 'cyber resilience', 'cyber-resilience', 'cyberresilience' and 'cyber security', 'cyber-security', 'cybersecurity'.

3.3. Key Themes

Our analysis of the primary studies shows several emerging themes and main focus domains, each of which is discussed within Sections 3.3.1–3.3.7.

3.3.1. Chronological Analysis of Key Events

The purpose of the chronological analysis is to examine the main determinants and the time correlation for the research distribution addressing CPS cyber resilience and modern DFIR in smart cities concerning the defined scope. To achieve this, the primary studies were organised in chronological order and classified depending on the year published and type of publication, as shown in Table 3. The trend shows that the first empirical study concerning this topic is dated from 2011 from a conference proceeding. It is not until 2016 that there is an 8% increase in research for this subject area through conference proceedings as the main outlet for the research publications. By 2017, the number of articles doubled and increased again in 2018. The differentiating factor was the high proportion of journal articles over publications from conference proceedings whilst by the first calendar quarter (Q1) of 2019 and the articles published in journals reached over 75% of studies published throughout the entire 2018.

Further investigating the results from the chronological analysis, the following key years were highlighted as a potential influencing factor concerning the investigated CPS-related research developments: 2011, 2016, 2018.

2011. This year was defined by the Hannover Messe Fair, where the term "Industry 4.0" was born to describe the next industrial revolution, a vision of three German engineers. Whilst the first industrial revolution dates back to the end of the 18th century introducing water and steam power, the second industrial revolution at the turn of the 20th century was centred around mass production using electricity and the third industrial revolution integrated IT and electronics into production systems, the

4th industrial revolution introduces digital processing and implementation of the IoT into production. In this context, the concept and the vision have been established for CPSs for production systems. Industry 4.0, a German origin of the Industry 4.0 term, is used synonymously with cyber–physical production systems [1,82]. In the post-recession output fall, the vision of Industry 4.0 elevated the German manufacturers and economy back into the spotlight [83,84].

2016. The creation of the UK's National Cyber Security Centre (NCSC) as the technical cybersecurity lead was a feature of this year. Furthermore, the investment and economic infrastructure plans announced in the National Infrastructure Delivery Plan in the UK [85] and the announcement of the significant cybersecurity fund as part of the USA's Cybersecurity National Action Plan also took place in 2016 [86]. The World Economic Forum (WEF) was also held in Davos. The WEF used the motto: "Mastering the Fourth Industrial Revolution" [87]. The event was attended by 2500 participants and 40 heads of states from 140 different countries discussing ideas to tackle global challenges sustainably with the aid of technology and the economic impact of Industry 4.0.

2018. In the USA, there was the notable creation of the Cybersecurity and Infrastructure Security Agency (CISA) responsible for national critical infrastructure from physical and cyber threats. Australia released an update for its cybersecurity sector competitiveness plan outlining Australia's significant economic opportunities to become a "global cybersecurity powerhouse" [88]. Despite Industry 4.0 being a global phenomenon, the acceleration of efforts by countries in the race of Industry 4.0 is local to lead the change and be the face of the new digital transformation. This era is characterized by high-capacity and low-latency 5G networks that will catapult digitalisation, which is predicted to create significant opportunities in many economic sectors. Furthermore, in terms of cybersecurity, the NCSC reported on the growing cybercrime threat, recording 34 significant cyberattacks that typically required cross-government responses over two years [42]. The government has explicitly acknowledged the need to improve the resilience of the UK's critical national infrastructure [89]. The consequence of the transformation not having peaked yet results in a continued increase in investment, grants and financial incentives; therefore, research efforts continue [90,91].

Relating the primary studies' trend with the key events, we identify a link between the technological and economic landscape and cyber-resilience-centric research that addresses CPSs in smart cities. From the primary studies, it emerges that the trend in the increase of papers has been influenced by a strategic focus on cybersecurity; improving the cybersecurity defence landscape, including the creation of NCSC and CISA; significant investment in improvements and strengthening of the national critical infrastructures. Coupled with efforts and initiatives exclusively focused on digital transformations to gain economic advantage could explain the surge in research studies published from 2016 onwards.

3.3.2. Cyber Resilience Analysis

To address the question of how existing frameworks and systems that address CPSs in smart cities support cyber resilience, we consider the scope of resilience within the cybersecurity discipline and the evidence reported in the primary studies. To achieve this, the primary studies were organised in order of the reported evidence of how the cyberattacks across the physical and digital domains were addressed and how the external or insider threats were approached.

Although cyber resilience is widely acknowledged by governments including the UK's National Cyber Security Strategy 2016–2021, which promotes the cyberspace resilience by shaping technical standards that govern emerging technologies, promoting best practices and security-by-design [5], the Joint Committee on National Security and Strategy in their report acknowledged that the UK Government must do more to improve the cyber resilience of the critical national infrastructure (CNI) [89]. Cyber resilience has been acknowledged as a challenge in the IoT; President Obama issued an Executive Order (EO) 13636 to strengthen the critical infrastructure cybersecurity resilience. Likewise, improving cyber resilience is at the forefront of the Australian Government [88].

Despite many efforts to define the term "resilience" and although CPS resilience is accepted as an important aspect by the scientific community, governments and industry, it is a multi-dimensional

and multi-disciplinary facet that has no clear and uniform definition or performance metrics [92,93]. The term resilience is described by the NIST as "[t]he ability to quickly adapt and recover from any known or unknown changes to the environment through a holistic implementation of risk management, contingency, and continuity planning" [94]. Furthermore, to evaluate CPS resilience, several areas of CPS resilience were studied including policy [95], correlation of resilience on probability and impact of performance under adverse conditions [96] and risk and resilience correlation [93].

The nature of CPSs is multi-dimensional, converging physical and cyber domains in a highly complex ecosystem integrating systems, software, people and services. In our approach to establishing how CPSs in smart cities support cyber resilience, we were able to investigate the primary studies according to specific layers within the TCP/IP model—a standard model used in computer networks, based on modern DFIR general-purpose frameworks—based on adversary type and by the smart sector covered by each study.

Layers were identified with reference to the TCP/IP model described in RFC 1122 [97]. The TCP/IP model consists of four layers which, from the lowest to the highest, are the link layer, the internet layer (network), the transport layer, and the application layer. The primary studies can be categorised into three layers: physical, communication (aligns to the Internet and transport layers of the TCP/IP model) and application. A similar categorization approach was taken by authors [92] to define CPS resilience. For example, the physical layer includes physical faults, component failure and the delivery of the attacks through access within the security perimeter including attacks on CPS controllers, sensors and actuators. The communication category includes communication-environment-based disruptions and attacks like denial of service (DoS), man-in-the-middle (MiM), the user to root type buffer overflow or remote to user ftp write. The application category included false data injection (FDI), malware and other services and cloud storage and web application-based attacks. Some incidents can fit into more than one category [98].

DFIR Support was investigated concerning the phases that form the basic foundation of an IR plan accordingly to general-purpose DFIR frameworks and standards such as the Digital Forensic Research Workshop (DFRWS), Abstract Digital Forensic Model (ADFM), NIST800-61 and ISO/IEC27050, from preparation to post-incident activities to identify how the primary studies address this process.

Adversary Type was identified within each layer, where the threat can be caused by external or internal factors. We consider an internal threat to be a threat by an adversary initiated inside the security perimeter. Such an entity is authorised to access the systems or resources within the security perimeter but acts in a way that is not authorised. Examples include malicious or disgruntled employees or contractors who have direct access and sufficient knowledge of the system or the resource. In contrast, an external threat is initiated by an adversary from outside the security perimeter. Such an entity is not authorised to access or use the systems or resources and gains access through unauthorised or illegitimate attack vectors. We investigate how the primary studies address this aspect; a similar emphasis on this approach was followed by reference [92].

Smart Sectors will leverage CPS performance and resilience differently. CPSs operate across different smart sectors, therefore we identify the smart sectors as reported in the primary studies.

Several studies specifically focus on the applicability of resilience in terms of the CPS's ability to withstand disruptions, recover from and adapt to known and unknown threats, as shown in Table 5. For example, in their approach, reference [40] argued that optimisation between smartness and cyber resilience in a CPS is required for a balance between functionality and cybersecurity without compromising the systems' resilience. In this study, the percolation theory was used as the basis of evaluating the stress caused by disruptions. The authors in reference [99] argued that the absence of common security standards and flexible methods to assess IoT security requires dedicated testbeds to systematically evaluate the devices' resilience under various conditions. The study developed a security testbed framework for the IoT. The testbed consists of standard security testing predominantly based on well-established vulnerability scans and penetration testing methodologies including port scanning, process enumeration, fuzzing and fingerprinting. The advanced testing capabilities of the

testbed are based on techniques and tools including machine learning (ML), traffic-based IoT device type identification, automatic anomaly detection and environment simulations. The number of test scenarios demonstrated the effectiveness of the testbed in detecting the IoT devices' resilience against attacks including denial of service (DoS). Another study [100] focused on CPS resilience mechanisms that can be applied during runtime to sustain resilience utilising self-healing structural adaptation. In the following study [101], the authors argued the importance of an interdisciplinary integrated approach between the cyber and physical layers. They asserted that cyber resilience-by-design must address two scopes to achieve overall resilience, the security controls, communication scope and the power engineers' scope to reinforce the weak points during the design. The study proposed an integrated cyber–physical sustainability metric framework to assess CPS cyber resilience.

Table 5. Primary studies focusing on aspects of cyber resilience(-by-design).

Year	Primary Study	Smart Sector
2011	[102]	Infrastructure
2012		
2013		
2014	[52]	Energy
2015	[103]	Mobility—Automotive
2016		
2017	[104]	Infrastructure
2018	[101,105]	Energy, Mobility—Aviation
Q1 2019	[40,99,100]	Security, Mobility—Aviation

Further analysis investigating possible correlations with the emerging key themes discussed in this paper shows no clear geographical correlation. The studies, categorised in Table 5, except for [101], acknowledged grant funding. Time correlation was observed with a continued trend in the increase of primary studies focusing on cyber resilience in 2018 and Q1 2019. This trend could indicate a response to the emergence of new and diverse types of security-related incidents that have the potential to be damaging and disruptive.

The author in reference [102] argued that the key difference between control and information technology (IT) systems is the control systems' interaction with the physical world and concludes that to withstand cyberattacks, systems should be resilient by design. The author asserts that the risk to control systems is higher due to the exposure and availability of vulnerabilities combined with the increasing motivations and capabilities of the attackers. The paper focuses on sensor attacks and addresses ways of prioritising sensors. Attack types were studied using the Tennessee-Eastman process control system (TE_PCS) model [106]. An automatic response mechanism was introduced based on various system states taking into consideration a false alarm response. The author's main conclusion was the strength of the TE-PCS's design resilience. Although the proposed principles and techniques could be applied to other physical processes and the false positive rate at 1000 simulation cycles was 0%, the automated response may not be appropriate for all control systems. The author cautions of a likely lack of resilience-by-design in large scale control systems which could remain vulnerable to several attack vectors. Further, the author in reference [104] defined a trustworthy service as one which secures against cyberattacks and operates normally despite faults or attacks. The authors proposed an IoT framework to integrate smart water systems (SWSs) with the IoT using a multilayer architecture trustworthy service and proposed that security issues should be addressed systematically by developers during the design and development of each IoT layer. Anomaly behaviour analysis (ABA) intrusion detection system (IDS) methodology was applied to protect the secure gateway from attacks utilising the Smart Water System Testbed. The secure gateway is part of the communication layer. The general detection rate of the ABA-IDS approach was over 90% for 600 packets/second intensity, with less than 3.5% recorded false alarm rate, with the fastest detection of 1 s and the slowest detection of a 4 s interval.

Other studies [52,101] focused on CNI such as power grids whilst urban systems were investigated by reference [40]. In reference [52], the resilience of five classical routing protocols applied in distributed large-scale networks was studied through simulation. Resilient techniques using route diversification were introduced to enhance the protocols' resilience against cyberattacks. The resilience was evaluated based on metrics consisting of five performance parameters which showed promising results. The communication layer was also the focus of [101] study, which proposed a new metric system framework to assess the reliability of large-scale distributed power systems. The author asserts the importance of combining the communication layer's cyber vulnerabilities with the physical layers' resilience for a meaningful assessment of the system sustainability. The following study [40] developed a network efficiency and resilience evaluation method for intelligent transportation systems (ITSs) in response to random and targeted attacks in urban areas. The author maintains that although the use of sensors is beneficial for automation, the infrastructure through their use becomes complex and liable to unknown and little understood vulnerabilities. The article concludes that the system's relative resilience was not sensitive to the levels of disruption. Integrity attacks were investigated by reference [105] proposing a global attack detection system for resilience against attacks on the railway traction systems. Resilience mechanisms that can be applied during runtime and are adaptable to the changing environment were studied by reference [99]. It is argued by reference [40] that the rate of integration of smartness in many systems proliferates at a greater rate than the ability to develop resilience whilst reference [100] identified resilience in the IoT as a significant challenge with research often focused only on one aspect or on a single attribute of resilience. Our results, as shown in Table 6, support this notion, for example, 46% of the primary studies considered the communication layer, whilst only 5% considered all three layers. We found that the communication layer had the most significant incremental trend in 2018, as presented in Figure 5, generally with an utmost focus across the smart industry and smart mobility sectors, Figure 6.

Table 6. Primary studies categorisation by the reference model layers.

Threat Layers	Primary Studies
Physical, Communication and Application	[48,105,107]
Physical and Communication	[2,38,39,51,63,65,101,103,104,108–114]
Physical	[36,37,67,84,85]
Communication	[33,37,40,52,99,100,115–131]
Application	[36,49,132–135]

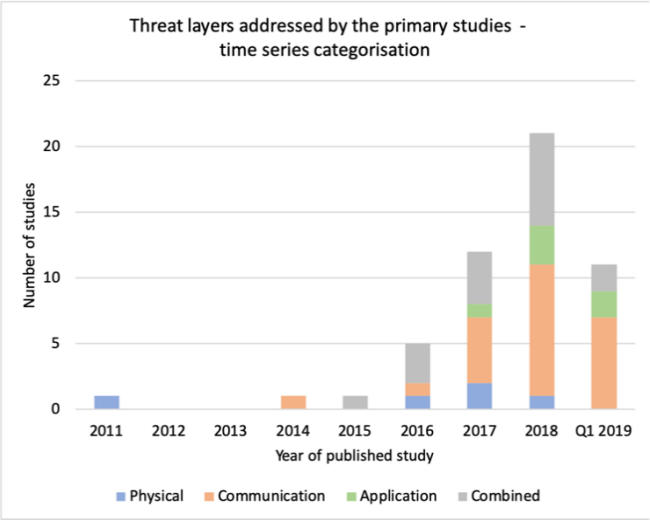

Figure 5. Time series categorization of the threat layers addressed by the primary studies.

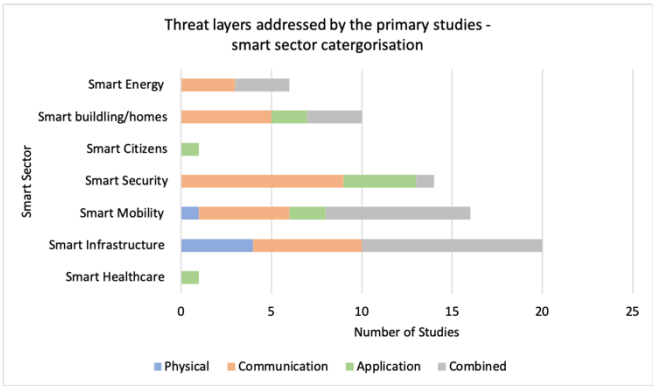

Figure 6. Reference model layers categorisation of smart sectors addressed by the primary studies. In this graph, multiple sectors addressed in a single study are reported individually to preserve sector visibility.

When investigating the adversary type, the results show that 19% of the primary studies considered internal and external threats in their research, as presented in Table 7. In 45% of the studies, the threat type was not sufficiently clarified. However, we observed a continued increase in studies focused on a combination of external and internal threats, as presented in Figure 7, generally with the greatest aggregation of studies in the smart infrastructure and smart mobility sectors (Figure 8).

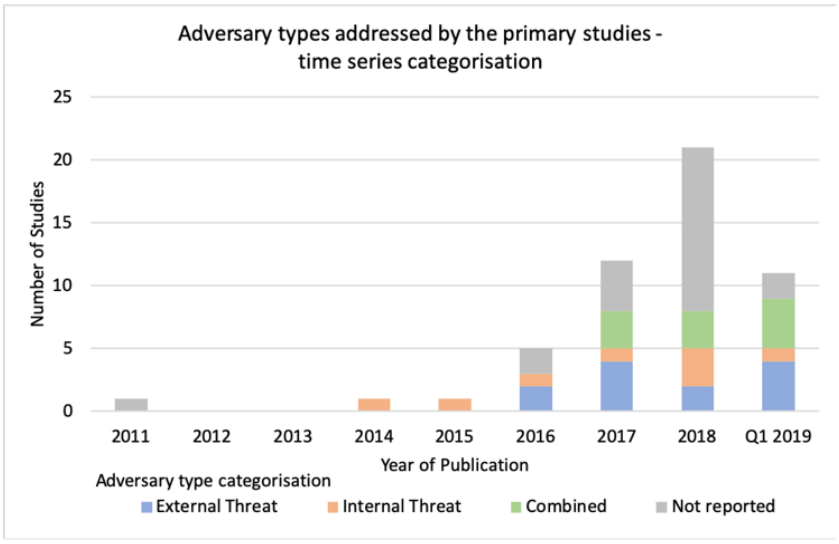

Figure 7. Time series categorisation of adversary type threat factor of smart sectors addressed by the primary studies.

Some studies [52] addressed insider threats on smart devices such as smart meters, which can be compromised by an active attacker to disrupt the network communication. The study in addition to considering the compromise of the physical nodes addresses the ability of the protocol to absorb the degradation following an insider attack. In [111], the focus of the study are large-scale distributed CPSs proposing a quantitative cyber-physical security assessment methodology, Ref. [136] provides and overview and discusses related risk assessment methods. Another study [99] investigated external threats and articulated that the challenges of the IoT devices provide means for hackers to access such devices. Therefore, the proposed testbed aimed to facilitate the analysis of various types of IoT devices either by using the conventional penetration testing methodology or advanced security testing utilising a machine learning approach. Internal and external faults including malicious activity were addressed by other studies [14,100,129]. In reference [14], the focus of the paper is on a multiple characteristic

association (MCA) approach to address cyberattacks and faults in electrical cyber–physical systems and reference [129] utilised an attribute-based time-sensitive and location-centric access control model consisting of an administrative and an operational component with applicability to remote and local operations.

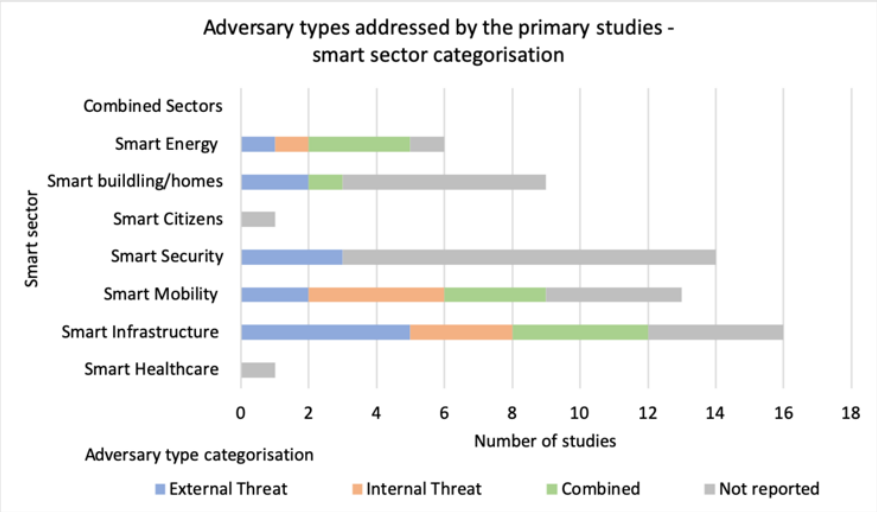

Figure 8. Adversary type threat factor categorisation of smart sectors addressed by the primary studies. In this graph, multiple sectors addressed in a single study are reported individually to preserve sector visibility.

Table 7. Primary studies categorisation by adversary threat type.

Threat Type	Primary Studies
Internal and External Threat	[33,51,63,100,109,110,114,119,120,130]
External Threat	[38,65,99,104,108,111,113,115,118,121,137]
Internal Threat	[22,61,65,102,104,131,135,138]

3.3.3. DFIR Analysis

Digital forensics forms a substantial part of IR in the cybersecurity sector; it is a recognised scientific methodology with a key focus on the process and verifiable conclusions. Although several published digital investigation models outline the steps for investigation by the forensic teams, there is no single uniform IR model. The simplest lifecycle for an investigation model consists of three stages, "acquisition", "analysis" and "reporting". However, with the increased penetration of digital technologies into modern lives, there were several revisions to the investigation stages. The U.S. Department of Justice (DoJ) proposed four-stage process consisting of "acquisition", "identification", "evaluation" and "admission as evidence" [138]; the DFRWS model consists of six phases namely "identification", "preservation", "collection", "examination", "analysis" and "presentation" [139]. The ADFM has expanded the process by three more stages: "preparation", "approach strategy" and "returning evidence" [140]. Due to the evolving sources of digital evidence, the digital and physical environments are closely converged where physical artefacts contain the digital evidence, which is reflected in the Integrated Digital Investigation Process (IDIP) consisting of five stages defined as "readiness", "deployment", "physical crime scene", "digital crime scene" and "review" [141]. Similar to the DFRWS model, the ISO/IEC 27050-3:2017, a general-purpose framework for electronically stored information (ESI) was developed for digital investigations containing seven stages: "identification", "preservation", "collection", "processing", "analysis", "review" and "production". The National Institute for Standards and Technology published an IR procedure NIST 800-61 in response to the frequency of emerging incidents consisting of four stages: "preparation", "detection and analysis",

"containment, eradication and recovery" and finally "post-incident activity". In CPSs, IR is a complex, multifaceted problem crossing the physical and cybersecurity boundaries.

The primary studies were classified by their key themes into groups according to the NIST 800-61 IR stages [98]. The studies were determined to have focused predominantly on the detection and analysis stage, as shown in Table 8.

Table 8. DFIR key stages categorisation of primary studies.

Key Stage	Primary Studies
Preparation	[13,48,100,111]
Detection and Analysis	[2,33,36–40,51,63–65,67,99–105,107–111,113,115–120,122–126, 128,129,131–133,137,142]
Containment, Eradication and Recovery	[40,49,52,100,103,104,107,114,121,127,129,130,133,135]
Post-Incident Activities	none

Preparation is an important part of the IR. Apart from compiling assets, creating a communication plan, setting metrics or creating an incident plan for each type of incident, security event simulation is also a valuable part of this stage. Simulation or modelling helps identify gaps, determine and optimise which security events and at what trigger should be investigated; therefore, they provide a controlled opportunity to strengthen weaker areas and improve cyber resilience, which we discussed in the previous section. For example, the author in reference [13] proposed a novel framework using Fuzzy Analytic Hierarchy Process to evaluate and rank the cybersecurity challenges in smart cities. Amongst the 9 identified smart sectors (factors) and 32 sub-factors, smart security was rated highest for being influenced by cybersecurity challenges in smart cities. The results of the study placed the sub-factors identified as part of the smart security in the highest priority areas influenced by cybersecurity challenges which were identified as the "surveillance and biometrics" followed by "simulation and modeling" and "intelligent threat detection". Our results show that smart security sector studies do not have a specific focus on cyber resilience aspects, see Table 5. and research focus relates predominantly to the communication layer threats, see Figure 6. A security-by-design (SbD) approach was proposed by reference [48] articulated as a framework to develop a highly secure and trustworthy smart car service and protect them from cyberattacks. The authors argue ABA is a more suitable approach because of the sensors' low computational power and therefore a lack of encryption techniques applicability. The sensor profiling was accomplished by using the discrete wavelet transform (DWT) coefficients and the Euclidean distance was utilised for sensor classification. The presented results demonstrated an up to 95% accuracy for unknown and 98% for known attacks with a low false-positive rate.

Incident Detection and Analysis (IDA) is a key phase in IR because the response cannot be manifested without accurate detection. Although incident detection is considered a reactive approach, there are detectable events that precede an incident. The results from the primary studies show that the highest distribution in the detection and analysis stage of the IR model is in the smart infrastructure sector as shown in Figure 9, and overall 67% of the sampled primary studies focus exclusively on cyberattacks detection, as shown in Figure 10. The author in reference [107] presents a framework for smart homes and smart buildings addressing multiple layers and threat types. The study utilised ABA-IDS to continuously monitor, detect and classify cyberattacks against sensors with high accuracy. The study aimed to extend the methodology to other IoT security frameworks, such as smart water systems [104] and smart grid systems [108]. Both studies rely on ABA-IDS utilising JRip classification algorithm achieving up to 99.8% and 97.18% accuracy on their respective datasets. The ABA-IDS detection and the classification results for reference [107] were similar and in some instances exceeded the results of other state-of-the-art protection systems for smart grids. Different approaches were proposed to enhance the detection of cyberattacks in industrial control systems. For example, a secure water treatment plant often consists of distributed cyber infrastructures that control physical processes.

The author in reference [118] proposed a time automata (TA) approach, whilst another study [64] focused on a hybrid of machine learning combined with a specification-based detection. An orthogonal defence mechanism consisting of several intelligent checkers was used by the author in reference [51].

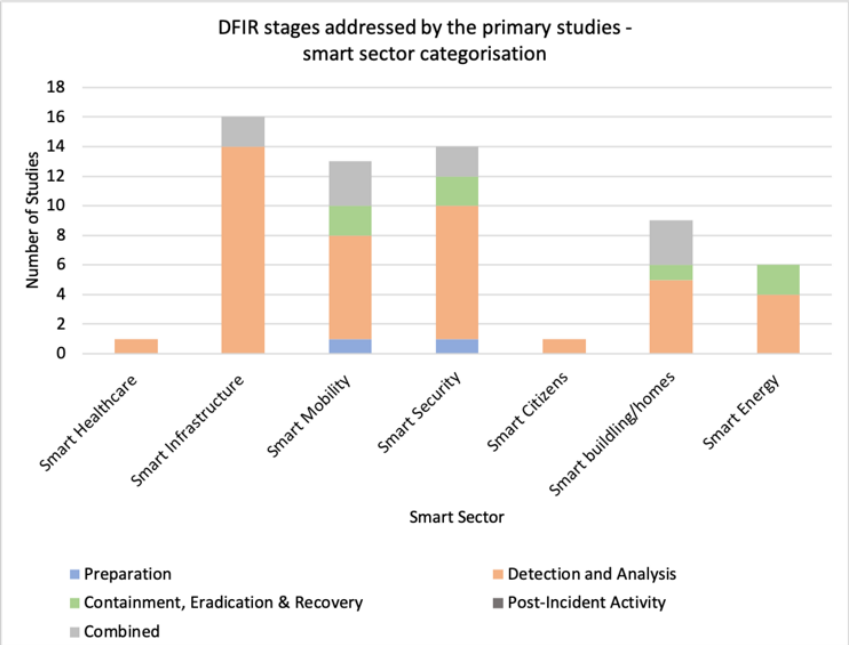

Figure 9. DFIR stages categorisation across smart sectors addressed by the primary studies. In this graph, multiple sectors addressed in a single study are reported individually to preserve sector visibility.

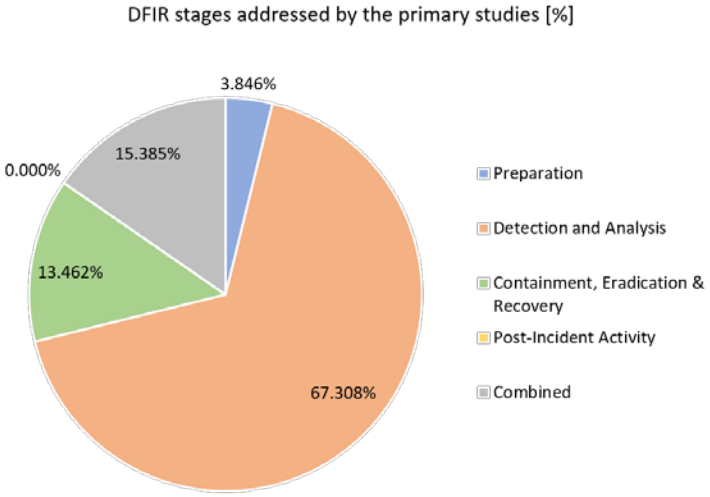

Figure 10. DFIR stages addressed by the primary studies.

Containment, Eradication and Recovery (CER) is the part of the process where models and standards differ. Whilst NIST views the CER as a single step, SANS (SysAdmin, Audit, Network, and Security), DFRWS and ISO/IEC 27050-3:2017 view them as separate segments. Furthermore, the terminology used by different frameworks and standards to identify similar steps can vary. The terminology used by NIST 800-61 refers to containment as an aim to stop the attack or threat, eradication removes it stopping cross-systems proliferation and recovery aims to get the system operation returning to business as usual.

Our figures show that only 13% of the primary studies investigate the CER segment of the IR procedure, as shown in Figure 10. For example, the focus of the following study [40] is on increasing

the resilience rather than lowering risks to demonstrate system recovery from disruption. The author argues that smart development over resilience may benefit some smart systems to achieve recovery through automation by redistributing the traffic by using alternative routes. This is part of the investigated model's algorithm. However, the limitation of the study is its consideration of large and very large urban areas; therefore, the model's applicability was not tested on smaller urban areas. Furthermore, the modelled scenario captured only a limited set of ITS disruptions, therefore, the effect of disruptions from different cyberattacks compared to those which were tested, and their method of recovery may vary. The author in reference [52] presents an interesting notion of extending the concept of resilience in networking to survivability, fault tolerance and security, however, acknowledges difficulties in defining quantitative metrics. Focusing on the internal threat, the reliance is on the protocol's capacity to absorb the attack under some failure behaviour and the resilient technique provides dynamicity to improve the self-healing capabilities of smart meters. Another study with a focus on resilience mechanisms [100] proposes achieving self-healing through a structural adaptation approach by substituting failed components as a method of recovery for compromised CPSs. The author asserts that this is achievable provided the compromised component is redundant and can be isolated. The author in reference [107] proposed an IoT security framework and based on the detection of abnormal behaviour, recovery actions can be taken. Other studies acknowledge the elapsed period before IR starts after the attack occurs. For example, the study in reference [135] presents a hybrid solution of distributed and centralised continuously evolving trust-based intrusion detection model aggregating multiple trust data sources to enable an effective in-flight network defence. The study claims, that following an abnormal patterns emergence, trust-value triggered IR with active defence is possible. Comparable to the results in Section 2, the results from the primary studies show that research often focused on one aspect of DFIR, see Figure 10.

Post-Incident Activity (PIA) is one of the most important phases of the IR process, but it is most often omitted [143]. This phase provides an opportunity to contribute to continuous learning, an evidence-based body-of-knowledge and to form a robust CTI. The IR can be accelerated by having an effective and specific CTI context around an initial indicator [144]. Therefore, a review of what occurred and defining actionable advice that can be used to inform decisions in the IR's preparation phase are important to achieve a closure of the IR process. The PIA has not been addressed by the primary studies.

3.3.4. Data Source Analysis

Through this research, a lack of available real datasets from CPS systems was identified. Although experimentation was carried out, predominantly this was limited to software-based simulations (46%) and simulation infrastructure (42%) by the primary studies, as shown in Figure 11. The infrastructure-based simulations typically relied on testbeds to replicate real-life CPS device settings such as a secure water treatment (SWaT) or water treatment plant (WTreat) testbeds [109,119]. However, in 12% of the studies published between 2018 and early 2019, public scientific datasets like BATADAL [110] or CAIDA [125] were used either solely or in conjunction with software-based simulation. Carrying out experimentation in an isolated environment limits the testing in a number of ways. For example, the unavailability of a current real dataset limits the reflection of the current threat types and limits the full contextualisation of the actual CPS devices' constraining factors such as resources or connectivity disruptions.

3.3.5. Analysis of Primary Studies Cross-Sector Proposals or Applications to Improve Digital Forensics

The purpose of analysing the cross-sector proposals or applications in smart cities is to explore transferable solutions that emerge from individual smart sectors to investigate possible trends and attempts to improve digital forensic investigations. To achieve this, the primary studies were organised accordingly to the smart sector's distribution according to the scope of our research, as shown in Figure 12.

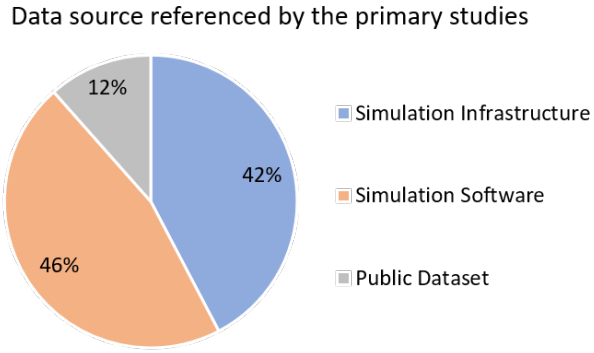

Figure 11. Data source referenced by the primary studies.

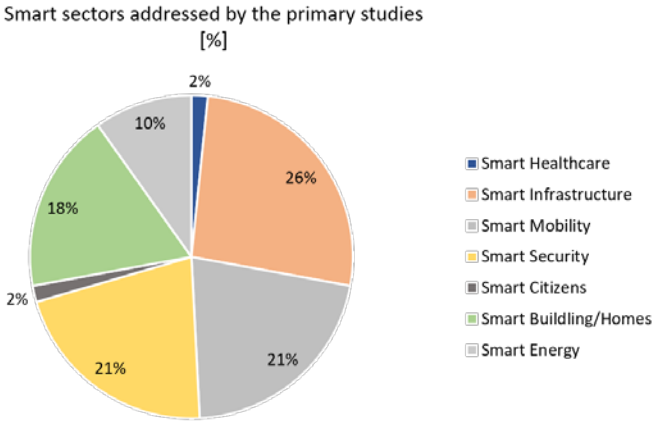

Figure 12. Smart sectors addressed by the primary studies.

The scientific community focused the research on smart infrastructure, followed by smart mobility and smart security sectors whilst smart healthcare and smart citizen were addressed only by a small number of studies, see Figure 12. Some of the studies address more than one themes, which is taken into consideration. This trend could be explained by the influences of key events such as Industry 4.0 and the maturity of the research of the design principles and enabling technologies in these areas [1] whereas the lack of research within the smart healthcare and smart citizen sector could be impacted by regulatory restrictions, ethical challenges, lack of relevant usable datasets and the current health care models or pathways [145].

The results show that some studies address more than one smart sector [104,120,124,126,133,145] or aim to diversify their future research [39,51,63–65,100,102,111,131,134]. For example, reference [145] explores smart support for independent living of the elderly within the community to maximise their independence whilst maintaining the ability to deal with their complex medical needs across multiple smart sectors including healthcare, homes and infrastructure. Furthermore, several studies consider developing their research to generalise applicability to other smart sectors and acknowledge the need for framework adaptability as a result of complexity and constant change of interconnected devices [133]. For example, the principles and techniques applied by reference [102] could be applied to other physical processes than the one covered by the study, whilst reference [131] suggest their methods can be applied in a number of CPS domains such as power networks, transportation, oil and natural gas systems.

Although the cyber threat landscape is changing from hobby-hacking to organised cyber-crime, the cyberattacks are becoming more sophisticated, organised and targeted; there is little scientific evidence of attempts for supporting modern digital forensics, cross-organisational information security sharing or coordination [28]. Security practices remain in silos lacking collaborative cyber defences to deal with the increased sophistication and coordination of cyberattacks including advanced persistent

threats [4,27]. This assertion is supported by our analysis of primary studies thus far. The transition from more traditional to IoT enabled CPS creates highly complex ecosystems, however, the focus of research is often limited to the boundary of the individual organisation or smart sector.

3.3.6. Typology Analysis

The purpose of the typology analysis is to separate the non-empirical and the empirical studies and to examine their chronological distribution. This analysis helps to better understand if the CPS frameworks and systems supporting cyber resilience or modern DFIR are predominantly academic ideas built on theory or do they emerge based on identified needs or as a result of relevant events.

Cyberattacks are a natural progression of physical attacks; they are more economical, reduce the risk for the attacker and have fewer geographical constraints. Studies from the sample recognised the cybersecurity risk factors that the integration of connected devices, sensors and automation helped by artificial intelligence have on smart ecosystems. In 2011, the focus of an [102] empirical study was attacks on sensor networks and their impact on the process control system. The research study referred to the example of the targeted ICS-based attacks such as the Maroochy Shire Council sewage attacks in Queensland, Australia in 2000; Ohio's 2003 Davis-Besse Slammer worm private network attack and the 2007 Iranian nuclear plant Stuxnet worm attack. The control systems' vulnerability such as Stuxnet and urban migration are also referred to by reference [107]. In 2007, the disruption and economic consequences of a large-scale cyberattack on the USA power grid were studied [108]. Several non-empirical studies investigated the theoretical concepts or potential challenges to be addressed for different aspects of the cyber defences against targeted attacks related to the increased interconnectivity and heterogeneity of the physical and cyber convergence. In 2014, the following study [21] investigated a federated building information system as a method of preventing hostile reconnaissance, managing intellectual property and enabling operational security. The study refers to a 2013 incident in Hackney, London in which a piling rig penetrated the roof of a Network Rail tunnel.

Therefore, the proliferation of digital technologies and the integration of IoT with physical systems expands the scope of forensic science creating a need for new specialised forensic techniques to reduce the backlog, workload and the cost of the forensic investigation process [146]. Digital forensics (DF) has developed as a branch of forensic science alongside the conventional forensic disciplines covering diverse digital technologies that can be exploited by the criminals.

The results presented in Figure 13 demonstrate the chronological trend between surveys, non-empirical and empirical studies. The focus of this SLR is on primary empirical studies. The total of the studies shows that non-empirical studies including the survey-type studies amounted to 64% compared with 36% of the empirical studies of the reviewed samples. Although the number of survey studies consistently increased, a sharp increase of the empirical research is observed during 2017 and a similar surge of the non-empirical studies is observed in 2018. Depending on this evidence, it is possible to argue that this dynamic could be influenced by the key events discussed in Section 1. Furthermore, from the empirical studies, it emerges that the focus of the research was informed by the threats of specific events, driven by the need for defence-in-depth mechanisms and influenced by the implementation of technological innovation and application within smart sectors.

3.3.7. Geographic Analysis

The purpose of the geographic analysis is to support our analysis in previous sections and gain a better understanding of where the research is concentrated, which geographical sectors have interest and opportunities for research addressing CPS-related cyber resilience and DFIR in smart cities. To achieve this, from the primary studies' authorship list, each unique country was recorded and assigned to the continent, as demonstrated in Figure 14. The colour hue represents the frequency of research carried out within the geographic region. The geographic analysis shows that the USA with 23% has the highest number of contributions of reviewed studies, followed by Singapore with 10%, the UK with 8% and Australia with 7% of contributions in the reviewed studies. In terms of continents,

Figure 15 shows that Asia is the continent with the highest concentration of the relevant CPS research at 37%, closely followed by Europe at 30% and North America at 26%. Central and South Americas, Australia and Africa are the continents with the lowest number of published studies within the scope of our research.

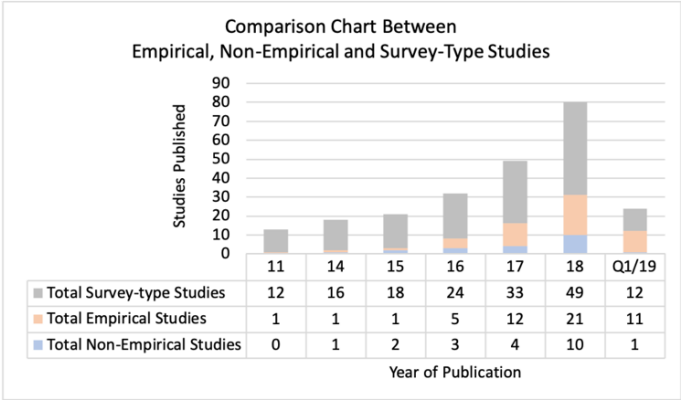

Figure 13. Comparison chart between empirical, non-empirical and survey studies. Non-empirical studies passed the systematic Phase0, Phase1 and Phase2 selection process' stages. Survey-type studies were considered, based on the original search string, in Phase0 and Phase1 of the selection process.

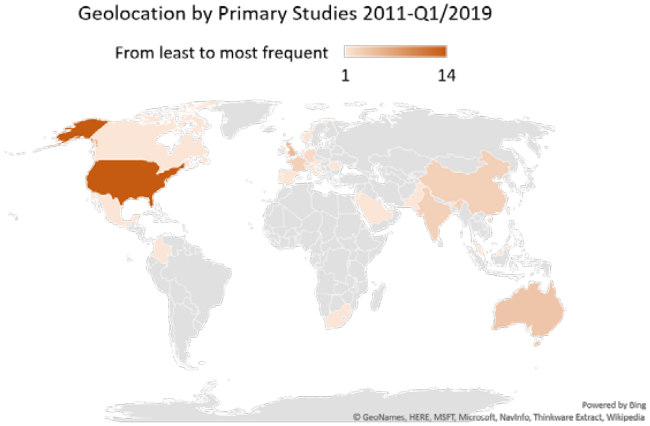

Figure 14. Geolocation by primary studies 2011-Q1/2019. (Microsoft product screenshot(s) reprinted with permission from Microsoft Corporation. https://www.microsoft.com/en-us/maps/product/print-rights).

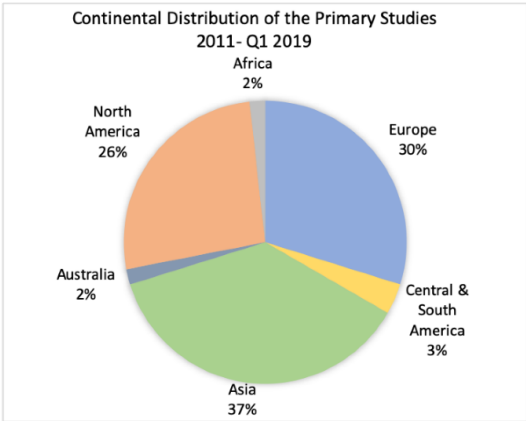

Figure 15. Continental distribution of primary studies.

4. Discussion

Our analysis revealed that in the last decade, CPSs have emerged as a new paradigm and as a result of the increased growth, complexity and heterogeneity of these infrastructures [14,82], the volume and the variety of vulnerabilities and attacks have evolved highlighting the need for defence mechanisms [147], need for cyber resilience and capability to support DFIR [26,29,30,33]. In this paper, the analysis of the primary studies supports our assertion that CPS-related cyber resilience and DFIR are active research domains. As has been noted in our results analysis, several empirical research studies have focused on CPS-related cyber resilience and DFIR. For example, Table 5 summarises primary studies which focused on aspects of cyber resilience across a number of different smart sectors, whilst a summary of primary studies with focus on DFIR's key stages in smart cities is shown in Table 8. In fact, several empirical research papers studied presented ways to solve real problems [37,122,135,148]. However, despite the importance of cyber resilience and support for DFIR in smart cities, these aspects have not been extensively considered by researchers in the context of CPSs. As we already noted, Figure 7 demonstrates a different level of scientific interest in adversary type research whilst Figure 8 further analyses the phenomena and presents the gaps across specific smart sectors. Furthermore, summarised in Figures 9 and 10, the analysis revealed differences in scientific interest in the DFIR stages with further variations across smart sectors. This poses an important question as to the reason for those differences. However, it is not the aim of this paper to provide the answer but to identify the gaps and present some open challenges and findings that can be used as future research directions [107,149].

The initial keyword searches highlighted that although there is an active research interest in the security of CPSs, frameworks addressing CPS cyber resilience, support for DFIR and their applications for developing cross-smart sector opportunities for collaborative cyber-defence practices are still emerging. Plans for cross-sector applications and diversifying the research to other areas of smart city sectors is often part of the future research direction [99,114,134].

The search criteria identified several non-empirical studies which provide concepts or theoretical bases to problem solutions and survey type studies that focused on consolidating the body of research related to our research scope aspects [21,55–59,61,150]. Whilst survey type studies are important, enable knowledge consolidation and identify areas of future research directions, several of the selected primary studies were empirical and provided practical solutions to a range of challenges related to cyber resilience and support for DFIR using innovative techniques.

The validation of the proposed solutions of the primary studies within the scope of our research inevitably always depends on carrying out cyberattacks or otherwise adversely impacting the infrastructure. Therefore, any validation must be carried out in a strictly controlled environment to avoid accidental disruption to CNI or compromise to data privacy. Validation can be economically challenging and requires funding to facilitate validations using a realistic simulation environment often involving physical infrastructure [47,51,64,109,119,131,137,142]. Almost three-quarters of the primary studies reported funding supported by research grants, defence or governmental sectors. Notable exceptions included only two primary studies which did not report funding and validated their proposal using infrastructure-based simulation utilising a smart home [129] and smart water system [116] infrastructures. In their current states, mainstream systems may not be equipped with infrastructure to facilitate such testing and would require significant change. Therefore, funding could be a contributing factor to empirical research in this field of study.

In addition to challenges accessing infrastructure-based simulators or testing in a production environment, there is a lack of publicly accessible datasets (Figure 11). The following study [18] stressed the need for access to public data to enable the successful adoption of technological innovations. To validate Industry-4.0-based proposals, the following study [2] relied on a combination of datasets. The limitation of the dataset used by reference [125] covering malicious IoT devices is the use of the CAIDA darknet datasets which predominantly contain malicious material. Based on the results, the research community appears to lean on software-based simulation using established platforms, predominantly Matlab [39,101,117,118,132], but researchers also utilise UPPAAL [118] and ProModel

Process [39] simulators. Therefore, software-based simulations are a frequent choice to test experimental concepts. However, using software-based simulations may not be most suitable in some cases, for example, in smart mobility scenarios involving driving where reactions could be very different in a simulated environment knowing that a simulator can be restarted in a click of a button compared to a non-simulated experiment. This may have profound consequences to the required acceleration of research of cyber defence of CPSs within smart cities since there is reliance on simulators for sufficient presentation of threats compared to reliable decision making in a real-world environment.

Concerning RQ1, during the primary studies' selection process, the researchers observed the availability of studies related to CPS applications. Within those studies, aspects of security may have been mentioned but they were not the focus of the study and often cyber defence was omitted altogether [18]. Moreover, although CPSs proliferate many aspects of modern lives and the demand and need for resilience in CPSs increases [151], the analysis revealed a distinct lack of available empirical research focused on the cyber resilience in the smart healthcare and smart citizen sectors (Figure 6). Possible reasons include the maturity of the Industry 4.0 technology compared with the smart sectors summarised in Figure 4 [84,85]. Moreover, the scale of media coverage of attacks on CNI like the cyberattack on the Ukrainian power grid [35] or Stuxnet [34] could also contribute to the prominence of the research in those sectors. Likewise, smart-healthcare- and smart-citizen-related research has complex and diverse ethical challenges including privacy and confidentiality concerns [145].

Infrastructure in smart cities consists of a growing number of highly integrated CPSs including traditional devices or entire cities retrofitted with new technologies to facilitate IoT connectivity [4,7,9]. Concerning RQ2, these devices contribute very little to support a systematic DFIR process in smart cities. Therefore, there is a need to develop a process-driven DFIR to deal with the evolving cyber threat landscape, the expanded attack surface and attack vector introduced through IoT connectivity [17,28]. Furthermore, as the sources of evidence evolve, digital evidence is contained within the physical artefacts [44]. For example, image-based evidence can be gained through closed-circuit television (CCTV) surveillance or from social media. Behavioural anomaly detection can be used to detect unauthorised vehicle use through driver profiling [152], detect attacks on smart water systems [104] or unauthorised access within smart workplaces [24].

Digital evidence, similar to physical evidence, seized at a crime scene or following a security incident, is relevant during digital forensic investigations [67]. The majority of the primary studies have researched a subset of an IR process, predominantly focusing on the "detection and analysis" phase (Figure 10) of an incident utilising different approaches including profile detection, behavioural anomaly, system monitoring or audit analysis [47,48,65,99,100,103,104,108,120,123,124,127]. Whilst incidents' detection is a reactive activity by nature, it is a key enabler for subsequent digital forensic processes, which cannot occur without detection and identification of an incident. However, leaning on Locard's theory, contact between items cause an exchange. Without CPS-specific support for modern DFIR, a forensic investigation from a complex interconnected cyber–physical environment may not extract digital evidence appropriately. Therefore, the important artefacts gathered during the acquisition stage may not be admissible in the court of law because the validity and integrity of the digital evidence is not appropriately maintained. Best practice guides are published—within UK jurisdiction, the Association of Chief Police Officers (ACPO) [153] and, in the US, with the Best Practices for Seizing Electronic Evidence [154]—to support incident practitioners.

In fact, the authors of the following study [37] argue that in some smart sectors such as smart homes, the application of digital forensics is an emerging field of study and asserts that there is a distinct lack of formal methodologies addressing the application of digital forensics in incident responses. Furthermore, recent studies show that the integration of CPSs in smart cities would significantly benefit from a specific forensic methodology as part of forensic preparedness to deal with security incidents [37,66]. However, a lack of consensus and formal process models in the digital forensics field that can be used to determine the reliability of digital evidence in courts is argued by reference [155]. Despite recognition of the importance of SbD by some researchers, our findings show an absence of

references to a digital forensic process in response to incidents. Finally, the increasing integration of technology into modern lives and the breadth of digital technologies exploitable by criminals requires extensive research to develop appropriate frameworks.

Concerning RQ3, the significance of the primary studies investigated is that despite the transition from traditional to IoT-enabled environments, our research findings show limited evidence of cross-sector proposals or applications for improving digital forensics. The authors of [28] claim that there is little evidence of cross-organisational information security sharing, structure and coordination. Considering this assertion within the context of CPSs, although researchers recognise the lack of shared practice, efforts are made to expand and improve cyber defence often as part of their future research direction. However, the various attempts to improve the ability to withstand targeted attacks [102] remain within a smart sector; for example, discussions are initiated between groups like the control and security practitioners but very few studies exploit the idea of cross-sector efforts to improve digital forensics. For example, authors of [64] consider their underlying idea applicable to multiple smart sectors which indicates recognition of more integrated approaches. The proposal of authors of [51,133] was to increase the flexibility and application of their system in several different environments. Generally, the explored research focused on developing and improving cyber defences within a single smart sector.

In summary, we draw on the results of the extensive SLR process, present and discuss the outcomes of our findings. Our extensive review showed number of gaps which could provide the basis and create opportunities for future research.

5. Conclusions

Smart cities are complex networks of connected devices including CPSs which utilise automation and AI to control several key functions. The initial keyword searches for this study highlighted CPSs as an emerging technology that creates an enormous range of possible applications across several smart sectors. It is clear from our SLR that there is an increasing interest in theoretical research and empirical implementations of CPS cyber resilience and support for modern DFIR within smart cities. The key influencing factors include the Industry 4.0 concept, government-led support and initiatives such as the National Cyber Security Strategy in UK [5] or national infrastructure plans [85,88], innovative ideas [36] and incidents [34,156].

Some smart sectors including smart healthcare and smart citizen were addressed only by a small number of studies, see Figure 12; it is critical that future research recognises this limitation. It is also evident that interest is growing in cross-sector proposals and an interdisciplinary approach to solve real-life problems including cybercrime [39,51,63–65,100–102,111,131,134]. Going forward, an interdisciplinary approach across smart sectors and aggregated sharing of CTI from multiple sources could increase situational awareness and provide a detailed, real-time and measurable body-of-knowledge to deal with the increased sophistication and coordination of cyberattacks.

We outlined and discussed the cyber threats landscape, particularly asserting that cyberattacks are increasingly more sophisticated, coordinated and targeted including advanced persistent threats (APTs). For example, the primary studies report on attacks that can originate from both within and from outside of the organisation. Having identified that there are limitations of the current IR methods in dealing with APT, we argue that existing efforts are insufficient to address emerging threats and there is a need for a CTI-driven mitigation approach [31]. Therefore, there is much work to be done to prepare for a dynamic threat landscape, strengthen the CPS cyber resilience to have the ability to adapt and operate under adverse conditions and to recover from incidents. For example, future research could focus on applying CTI to modelling attacks on entities' critical functions and underlying systems including its people, processes and technologies. This could help an entity to assess its protection, detection and response capabilities. Therefore, lessons can be gained from the IR lifecycle to minimise disruption and reduce the attack surface. The challenges need to be addressed through innovative solutions to support a modern defence-in-depth strategy.

Additionally, the increasing integration of CPS into modern lives diversifies the scope of forensic science and forensic investigations. Thus, alongside the conventional forensic disciplines, digital forensics has developed as a branch of forensic science covering diverse digital technologies including CPSs which can be exploited by criminals. The majority of the primary studies reported on the detection and analysis phase of the IR process. Therefore, more research is required to investigate the other phases of the IR process. This creates opportunities to reduce the backlog, the workload and the cost of the digital forensic investigation processes. Implementing an evidence-based body-of-knowledge by forming a robust CTI could solve real-life problems. Future work on addressing CPS in smart cities to support modern DFIR should consider integrating CTI into the IR. Such integration could enable faster threat detection, digital forensic investigation, repelling of attacks minimising disruption and escalated response time to prevent adversaries from successfully compromising their target.

Further, we identified a lack of available current publicly accessible real CPS-generated datasets that limit the ability of comparative experiments by other researchers, for example, to test and validate the accuracy of results robustly. Future works could consider addressing this limitation to create a pool of scientific resources. Publicly accessible datasets could accelerate the development of countermeasures against cybersecurity threats strengthening the cyber defence in smart cities to continue to function effectively under adverse conditions [43].

Author Contributions: Conceptualization, G.A.-A. and H.A.-K.; methodology, investigation, data curation, formal analysis, visualisation, writing—original draft, G.A.-A.; validation, H.A.-K., G.E., C.M.; writing—review and editing, H.A.-K., G.A.-A., G.E., C.M.; supervision, H.A.K. and G.E.; All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

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

References

1. Vogel-Heuser, B.; Hess, D. Guest Editorial Industry 4.0–Prerequisites and Visions. *IEEE Trans. Autom. Sci. Eng.* **2016**, *13*, 1–3. [CrossRef]
2. Moustafa, N.; Adi, E.; Turnbull, B.; Hu, J. A New Threat Intelligence Scheme for Safeguarding Industry 4.0 Systems. *IEEE Access.* **2018**, *6*, 32910–32924. [CrossRef]
3. Lom, M.; Pribyl, O.; Svitek, M. Industry 4.0 as a part of smart cities. In Proceedings of the 2016 Smart Cities Symposium Prague (SCSP), Prague, Czech Republic, 26–27 May 2016; pp. 1–6. [CrossRef]
4. Postránecký, M.; Svítek, M. Smart city near to 4.0—An adoption of industry 4.0 conceptual model. In Proceedings of the 2017 Smart City Symposium Prague (SCSP), Prague, Czech Republic, 25–26 May 2017; pp. 1–5. [CrossRef]
5. HM Government. National Cyber Security Strategy 2016–2021. 2016. Available online: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf (accessed on 15 October 2017).
6. Nam, T.; Pardo, T.A. Conceptualizing smart city with dimensions of technology, people, and institutions. In Proceedings of the 12th Annual International Digital Government Research Conference: Digital Government Innovation in Challenging Times, College Park, MA, USA, 12–15 June 2011.
7. Parliament, E. Mapping Smart Cities in the EU. 2014. Available online: http://www.europarl.europa.eu/RegData/etudes/etudes/join/2014/507480/IPOL-ITRE_ET%282014%29507480_EN.pdf (accessed on 26 April 2019).
8. Albino, V.; Berardi, U.; Dangelico, R.M. Smart Cities: Definitions, Dimensions, Performance, and Initiatives. *J. Urban Technol.* **2015**, *22*, 3–21. [CrossRef]
9. Harrison, C.; Eckman, B.; Hamilton, R.; Hartswick, P.; Kalagnanam, J.; Paraszczak, J.; Williams, P. Foundations for Smarter Cities. *IBM J. Res. Dev.* **2010**, *54*, 1–16. [CrossRef]
10. Caragliu, A.; Del Bo, C.F.M.; Nijkamp, P. Smart Cities in Europe. *J. Urban Technol.* **2011**, *18*, 65–82. [CrossRef]
11. Lazaroiu, G.C.; Roscia, M. Definition methodology for the smart cities model. *Energy* **2012**, *47*, 326–332. [CrossRef]

12. Barrionuevo, J.M.; Berrone, P.; Costa, J.E.R. Smart Cities, Sustainable Progress: Opportunities for Urban Development. *IESE Insight* **2012**, 50–57. [CrossRef]
13. Belgaum, M.; Alansari, Z.; Jain, R.; Alshaer, J. A Framework for Evaluation of Cyber Security Challenges in Smart Cities. In Proceedings of the Smart Cities Symposium, Bahrain, 22–23 April 2018; Volume 4, p. 6. [CrossRef]
14. Elmaghraby, A.S.; Losavio, M.M. Cyber security challenges in Smart Cities: Safety, security and privacy. *J. Adv. Res.* **2014**, *5*, 491–497. [CrossRef]
15. Baig, Z.A.; Szewczyk, P.; Valli, C.; Rabadia, P.; Hannay, P.; Chernyshev, M.; Johnstone, M.; Kerai, P.; Ibrahim, A.; Sansurooah, K.; et al. Future challenges for smart cities: Cyber-security and digital forensics. *Digit. Investig.* **2017**, *22*, 3–13. [CrossRef]
16. Vattapparamban, E.; Guvenc, I.; Yurekli, A.I.; Akkaya, K.; Uluagac, S. Drones for smart cities: Issues in cybersecurity, privacy, and public safety. In Proceedings of the 2016 International Wireless Communications and Mobile Computing Conference (IWCMC), Paphos, Cyprus, 5–9 September 2016; pp. 216–221.
17. Bajramovic, E.; Waedt, K.; Ciriello, A.; Gupta, D. Forensic readiness of smart buildings: Preconditions for subsequent cybersecurity tests. In Proceedings of the 2016 IEEE International Smart Cities Conference (ISC2), Trento, Italy, 12–15 September 2015; pp. 1–6.
18. Hollands, R.G. Will the real smart city please stand up? *City* **2008**, *12*, 303–320. [CrossRef]
19. Cocchia, A. *Smart and Digital City: A Systematic Literature Review*; Smart City: How to Create Public and Economic Value with High Technology in Urban Space; Dameri, R.P., Rosenthal-Sabroux, C., Eds.; Springer International Publishing: Cham, Switzerland, 2014; pp. 13–43.
20. Oliveira, Á.; Campolargo, M. From Smart Cities to Human Smart Cities. In Proceedings of the 2015 48th Hawaii International Conference on System Sciences, Kauai, HI, USA, 5–8 January 2015; pp. 2336–2344.
21. Boyes, H.; Watson, T.; Norris, P.; Isbell, R. Enabling intelligent cities through cyber security of building information and building systems. In Proceedings of the IET Conference on Future Intelligent Cities, London, UK, 4–5 December 2014; pp. 1–6.
22. Negri, E.; Fumagalli, L.; Macchi, M. A Review of the Roles of Digital Twin in CPS-based Production Systems. *Procedia Manuf.* **2017**, *11*, 939–948. [CrossRef]
23. Desmit, Z.; Elhabashy, A.E.; Wells, L.J.; Camelio, J.A. An approach to cyber-physical vulnerability assessment for intelligent manufacturing systems. *J. Manuf. Syst.* **2017**, *43*, 339–351. [CrossRef]
24. Ahmadi-Assalemi, G.; Al-Khateeb, H.M.; Epiphaniou, G.; Cosson, J.; Jahankhani, H.; Pillai, P. Federated Blockchain-Based Tracking and Liability Attribution Framework for Employees and Cyber-Physical Objects in a Smart Workplace. In Proceedings of the 2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3), London, UK, 16–18 January 2019; pp. 1–9.
25. Hsu, D.F.; Marinucci, D. *Advances in Cyber Security: Technology, Operations, and Experiences*; Oxford University Press: Oxford, UK, 2012.
26. ENISA. ENISA Threat Landscape Report 2018, 15 Top Cyberthreats and Trends. 2019. Available online: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018 (accessed on 20 October 2019).
27. Tankard, C. Advanced Persistent threats and how to monitor and deter them. *Netw. Secur.* **2011**, 16–19. [CrossRef]
28. Skopik, F.; Settanni, G.; Fiedler, R. A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing. *Comput. Secur.* **2016**, *60*, 154–176. [CrossRef]
29. Verizon. Data Breach Digest. 2016. Available online: https://enterprise.verizon.com/resources/reports/2016/data-breach-digest.pdf (accessed on 2 November 2019).
30. Verizon. 2016 Data Breach Investigations Report. 2016. Available online: https://regmedia.co.uk/2016/05/12/dbir_2016.pdf (accessed on 2 November 2019).
31. Hutchins, E.M.; Cloppert, M.J.; Amin, R.M. Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. In *Leading Issues in Information Warfare & Security Research*; Academic Publishing International Ltd.: Reading, UK, 2011; Volume 1, p. 80.
32. Europol: Internet Organised Crime Threat Assessment (IOCTA). 2019. Available online: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2019 (accessed on 22 October 2019).
33. Wang, Y.; Yan, G. A new model approach of electrical cyber physical systems considering cyber security. *IEEJ Trans. Electr. Electron. Eng.* **2018**, *14*, 201–213. [CrossRef]

34. Langner, R. Stuxnet: Dissecting a Cyberwarfare Weapon. *IEEE Secur. Priv. Mag.* **2011**, *9*, 49–51. [CrossRef]
35. Case, D.U. *Analysis of the Cyber Attack on the Ukrainian Power Grid*; Electricity Information Sharing and Analysis Center (E-ISAC): New York, NY, USA, 2016.
36. Bryant, N.; Spencer, N.; King, A.; Crooks, P.; Deakin, J.; Young, S. IoT and smart city services to support independence and wellbeing of older people. In Proceedings of the 2017 25th International Conference on Software, Telecommunications and Computer Networks (SoftCOM), Split, Croatia, 21–23 September 2017; pp. 1–6.
37. Do, Q.; Martini, B.; Choo, K.-K.R. Cyber-physical systems information gathering: A smart home case study. *Comput. Netw.* **2018**, *138*, 1–12. [CrossRef]
38. Jia, X.; Li, X.; Gao, Y. A Novel Semi-Automatic Vulnerability Detection System for Smart Home. In Proceedings of the International Conference on Big Data and Internet of Thing, London, UK, 20–22 December 2017; pp. 195–199.
39. Comert, G.; Pollard, J.; Nicol, D.M.; Palani, K.; Vignesh, B. Modeling Cyber Attacks at Intelligent Traffic Signals. *Transp. Res. Rec. J. Transp. Res. Board* **2018**, *2672*, 76–89. [CrossRef]
40. Ganin, A.A.; Mersky, A.C.; Jin, A.S.; Kitsak, M.; Keisler, J.M.; Linkov, I. Resilience in Intelligent Transportation Systems (ITS). *Transp. Res. Part C Emerg. Technol.* **2019**, *100*, 318–329. [CrossRef]
41. Holland, K. Update on SFMTA Ransomware Attack. 2016. Available online: https://www.sfmta.com/blog/update-sfmta-ransomware-attack (accessed on 1 November 2019).
42. National Cyber Security Centre. *The Cyber Threat to UK Business*; National Crime Agency, Ed.; UK Government: London, UK, 2018; p. 28.
43. Sterbenz, J.P.G.; Hutchison, D.; Çetinkaya, E.K.; Jabbar, A.; Rohrer, J.P.; Schöller, M.; Smith, P. Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines. *Comput. Netw.* **2010**, *54*, 1245–1265. [CrossRef]
44. Al-Khateeb, H.; Epiphaniou, G.; Daly, H. Blockchain for Modern Digital Forensics: The Chain-of-Custody as a Distributed Ledger. *Phys. Autom. Target Recognit.* **2019**, 149–168. [CrossRef]
45. NIST. *Cybersecurity Framework*; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2018; p. 55.
46. Griffor, E.R.; Greer, C.; Wollman, A.D.; Burns, M.J. Framework for cyber-physical systems: Volume 1, Overview. *Natl. Inst. Stand. Technol.* **2017**, *1*. [CrossRef]
47. Pacheco, J.; Hariri, S. *IoT Security Framework for Smart Cyber Infrastructures*; IEEE: New York, NY, USA, 2016; pp. 242–247. [CrossRef]
48. Pacheco, J.; Satam, S.; Hariri, S.; Grijalva, C.; Berkenbrock, H. IoT Security Development Framework for building trustworthy Smart car services. In Proceedings of the 2016 IEEE Conference on Intelligence and Security Informatics (ISI), Tucson, AZ, USA, 28–30 September 2016; pp. 237–242. [CrossRef]
49. Rahman, A.; Rashid, M.; Hossain, M.S.; Hassanain, E.; Alhamid, M.F.; Guizani, M. Blockchain and IoT-Based Cognitive Edge Framework for Sharing Economy Services in a Smart City. *IEEE Access* **2019**, *7*, 18611–18621. [CrossRef]
50. Lee, J.; Bagheri, B.; Kao, H.-A. A Cyber-Physical Systems architecture for Industry 4.0-based manufacturing systems. *Manuf. Lett.* **2015**, *3*, 18–23. [CrossRef]
51. Shrivastava, S.; Adepu, S.; Mathur, A. Design and assessment of an Orthogonal Defense Mechanism for a water treatment facility. *Robot. Auton. Syst.* **2018**, *101*, 114–125. [CrossRef]
52. Erdene-Ochir, O.; Abdallah, M.; Qaraqe, K.; Minier, M.; Valois, F. Routing resilience evaluation for smart metering: Definition, metric and techniques. In Proceedings of the 2014 IEEE 25th Annual International Symposium on Personal, Indoor, and Mobile Radio Communication (PIMRC), Washington, DC, USA, 2–5 September 2014.
53. Farley, T.R.; Colbourn, C.J. Multiterminal resilience for series-parallel networks. *Networks* **2007**, *50*, 164–172. [CrossRef]
54. Cholda, P.; Mykkeltveit, A.; Helvik, B.E.; Wittner, O.J.; Jajszczyk, A. A survey of resilience differentiation frameworks in communication networks. *IEEE Commun. Surv. Tutor.* **2007**, *9*, 32–55. [CrossRef]
55. Leszczyna, R. A review of standards with cybersecurity requirements for smart grid. *Comput. Secur.* **2018**, *77*, 262–276. [CrossRef]
56. Lezzi, M.; Lazoi, M.; Corallo, A. Cybersecurity for Industry 4.0 in the current literature: A reference framework. *Comput. Ind.* **2018**, *103*, 97–110. [CrossRef]

57. Daneva, M.; Lazarov, B. (Eds.) Requirements for smart cities: Results from a systematic review of literature. In Proceedings of the 2018 12th International Conference on Research Challenges in Information Science (RCIS), Nantes, France, 29–31 May 2018.
58. Sterbenz, J.P. Smart City and IoT Resilience, Survivability, and Disruption Tolerance: Challenges, Modelling, and a Survey of Research Opportunities. 2017. Available online: https://doi.org/10.1109/RCIS.2018.8406655 (accessed on 7 December 2019).
59. McKee, D.; Clement, S.J.; Almutairi, J.; Xu, J. Survey of advances and challenges in intelligent autonomy for distributed cyber-physical systems. *CAAI Trans. Intell. Technol.* **2018**, *3*, 75–82. [CrossRef]
60. Yu, W.; Liang, F.; He, X.; Hatcher, W.G.; Lu, C.; Lin, J.; Yang, X. A Survey on the Edge Computing for the Internet of Things. *IEEE Access* **2018**, *6*, 6900–6919. [CrossRef]
61. Lin, J.; Yu, W.; Zhang, N.; Yang, X.; Zhang, H.; Zhao, W. A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications. *IEEE Internet Things J.* **2017**, *4*, 1125–1142. [CrossRef]
62. Kitchenham, B.A.; Charter, S. Guidelines for Performing Systematic Literature Reviews in Software Engineering 2.3. Available online: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.154.1446&rep=rep1&type=pdf (accessed on 22 January 2019).
63. Cheh, C.; Keefe, K.; Feddersen, B.; Chen, B.; Temple, W.G.; Sanders, W.H. Developing Models for Physical Attacks in Cyber-Physical Systems. In Proceedings of the 2017 Workshop on Cyber-Physical Systems Security and PrivaCy, Dallas, TX, USA, 3 November 2017; pp. 49–55.
64. Lin, Q.; Adepu, S.; Verwer, S.; Mathur, A. TABOR. In Proceedings of the 2018 on Asia Conference on Computer and Communications Security, Incheon, Korea, 4–8 June 2018; pp. 525–536.
65. Li, F.; Shi, Y.; Shinde, A.; Ye, J.; Song, W.Z. Enhanced Cyber-Physical Security in Internet of Things through Energy Auditing. *IEEE Internet Things J.* **2019**, *6*, 5224–5231. [CrossRef]
66. Oriwoh, E.; Jazani, D.; Epiphaniou, G.; Sant, P. Internet of Things Forensics: Challenges and Approaches. In Proceedings of the 9th IEEE International Conference on Collaborative Computing: Networking, Applications and Worksharing, Austin, TX, USA, 20–23 October 2013.
67. Feng, X.; Dawam, E.S.; Amin, S. A New Digital Forensics Model of Smart City Automated Vehicles. In Proceedings of the 2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Exeter, UK, 21–23 June 2017.
68. Clarke, A.C.; Crane, A. Cross-Sector Partnerships for Systemic Change: Systematized Literature Review and Agenda for Further Research. *J. Bus. Ethic* **2018**, *150*, 303–313. [CrossRef] [PubMed]
69. Wohlin, C. Guidelines for snowballing in systematic literature studies and a replication in software engineering. In Proceedings of the 18th International Conference on Evaluation and Assessment in Software Engineering, London, UK, 13–14 May 2014; pp. 1–10.
70. Li, Z.; Shahidehpour, M. Deployment of cybersecurity for managing traffic efficiency and safety in smart cities. *Electr. J.* **2017**, *30*, 52–61. [CrossRef]
71. Sani, A.S.; Yuan, D.; Jin, J.; Gao, L.; Yu, S.; Dong, Z.Y. Cyber security framework for Internet of Things-based Energy Internet. *Futur. Gener. Comput. Syst.* **2019**, *93*, 849–859. [CrossRef]
72. Salimitari, M.; Bhattacharjee, S.; Chatterjee, M. Prospect Theoretic Approach for Data Integrity in IoT Networks under Manipulation Attacks. *arXiv* **2018**, arXiv:1809.07928.
73. Arnautovic, E. Consolidated State-of-the-Art Report, Computer Networks. 2010. Available online: https://iot4cps.at/wp-content/uploads/2019/03/IoT4CPS_D2.1_V1.2b.pdf (accessed on 26 April 2019).
74. Schmittner, C.; Ratasich, D.; Matschnig, M. Design & Methods Concept Transactions on Emerging Telecommunications Technologies. 2018. Available online: https://iot4cps.at/wp-content/uploads/2019/03/IoT4CPS_D3.1_V1.0.pdf (accessed on 26 April 2019).
75. Xia, Z.Q.; Jiang, L.L.; Xu, M. Electric power CPS attack prediction method based on path analysis. *J. Tsinghua Univ. Nat. Sci. Ed.* **2018**, *58*, 157–163.
76. Pullen, D.; Anagnostopoulos, N.A.; Arul, T.; Katzenbeisser, S. Poster: Hierarchical Integrity Checking in Heterogeneous Vehicular Networks. In Proceedings of the 2018 IEEE Vehicular Networking Conference (VNC), Taipei, Taiwan, 5–7 December 2018. [CrossRef]

77. Albela, M.S.; Fraga-Lamas, P.; Fernández-Caramés, T.M. A Practical Evaluation on RSA and ECC-Based Cipher Suites for IoT High-Security Energy-Efficient Fog and Mist Computing Devices. *Sensors* **2018**, *18*, 3868. [CrossRef]
78. Clincy, V.; Shahriar, H. Detection of Anomaly in Firewall Rule-Sets. *Adv. Intell. Syst. Comput.* **2018**, 422–431. [CrossRef]
79. Singh, S.P.; Nayyar, A.; Kumar, R.; Sharma, A. Fog computing: From architecture to edge computing and big data processing. *J. Supercomput.* **2018**, *75*, 2070–2105. [CrossRef]
80. Hosseini, S.; Turhan, B.; Gunarathna, D. A Systematic Literature Review and Meta-Analysis on Cross Project Defect Prediction. *IEEE Trans. Softw. Eng.* **2017**, *45*, 111–147. [CrossRef]
81. Hall, T.; Beecham, S.; Bowes, D.; Gray, D.; Counsell, S. A Systematic Literature Review on Fault Prediction Performance in Software Engineering. *IEEE Trans. Softw. Eng.* **2011**, *38*, 1276–1304. [CrossRef]
82. Pfeiffer, S. The Vision of "Industrie 4.0" in the Making—A Case of Future Told, Tamed, and Traded. *NanoEthics* **2017**, *11*, 107–121. [CrossRef]
83. Elliott, L.; Kollewe, J. Germany's Smaller Firms Emerge Intact from the Recession, Theguardian. 2011. Available online: https://www.theguardian.com/world/2011/mar/15/new-europe-germany-manufacturing (accessed on 4 July 2019).
84. Hancké, B.; Coulter, S. The German manufacturing sector unpacked: Institutions, policies and future trajectories, London School of Economics and Political Science, Foresight, Government Office for Science. 2013. Available online: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/283889/ep13-german-manufacturing.pdf (accessed on 4 July 2019).
85. Infrastructure and Projects Authority. *National Infrastructure Delivery Plan 2016–2021*; HM Treasury and Cabinet Office: London, UK, 2016; p. 113.
86. The White House. Fact Sheet: Cybersecurity National Action Plan. 2016. Available online: https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan (accessed on 3 July 2019).
87. World Econnomic Forum. World Economic Forum Annual Meeting 2016 Mastering the Fourth Industrial Revolution, REF 300116, Davos-Klosters. 2016. Available online: http://www3.weforum.org/docs/WEF_AM16_Report.pdf (accessed on 3 July 2019).
88. Australian Cyber Security Growth Network. *Australia's Cyber Security Sector Competitiveness Plan*; Australian Government Department for Industry: Canberra, Australia, 2018; p. 136. Available online: https://www.austcyber.com/file-download/download/public/415 (accessed on 6 July 2019).
89. House of Lords House of Commons Joint Committee on the National Security Strategy. *Cyber Security of the UK's Critical National Infrastructure*; UK Government: London, UK, 2018; p. 64. Available online: https://publications.parliament.uk/pa/jt201719/jtselect/jtnatsec/1708/1708.pdf (accessed on 6 July 2019).
90. Buhr, D.; Stehnken, T. *Industry 4.0 and European Innovation Policy: Big Plans, Small Steps*; The Friedrich-Ebert-Stiftung-Economic and Social Policy Department: Berlin, Germany, 2018.
91. Maresova, P.; Soukal, I.; Svobodová, L.; Hedvicakova, M.; Javanmardi, E.; Selamat, A.; Krejcar, O. Consequences of Industry 4.0 in Business and Economics. *Economies* **2018**, *6*, 46. [CrossRef]
92. Friedberg, I.; McLaughlin, K.; Smith, P.; Wurzenberger, M. Towards a Resilience Metric Framework for Cyber-Physical Systems. In Proceedings of the 4th International Symposium for ICS & SCADA Cyber Security Research 2016, Belfast, UK, 23–25 August 2016. [CrossRef]
93. Arghandeh, R.; Von Meier, A.; Mehrmanesh, L.; Mili, L. On the definition of cyber-physical resilience in power systems. *Renew. Sustain. Energy Rev.* **2016**, *58*, 1060–1069. [CrossRef]
94. Kissel, R. *Glossary of Key Information Security Terms*; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2013; p. 222. [CrossRef]
95. Linkov, I.; Eisenberg, D.A.; Plourde, K.; Seager, T.; Allen, J.; Kott, A. Resilience metrics for cyber systems. *Environ. Syst. Decis.* **2013**, *33*, 471–476. [CrossRef]
96. Watson, J.-P.; Guttromson, R.; Silva-Monroy, C.; Jeffers, R.; Jones, K.; Ellison, J.; Rath, C.; Gearhart, J.; Jones, D.; Corbet, T.; et al. Conceptual Framework for Developing Resilience Metrics for the Electricity, Oil, and Gas Sectors in the United States. *Concept. Framew. Dev. Resil. Metr. Electr. Oil Gas Sect. United States* **2014**. [CrossRef]

97. Internet Engineering Task Force. *Requirements for Internet Hosts-Communication Layers*; IETF: Fremont, CA, USA, 1989; p. 116. Available online: https://history-computer.com/Library/rfc1122.pdf (accessed on 20 September 2019).
98. National Institute of Standards and Technology NIST. *Computer Security Incident Handling Guide*; NIST: Gaithersburg, MD, USA, 2004; p. 148. Available online: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf (accessed on 28 August 2019).
99. Siboni, S.; Sachidananda, V.; Meidan, Y.; Bohadana, M.; Mathov, Y.; Bhairav, S.; Shabtai, A.; Elovici, Y. Security Testbed for Internet-of-Things Devices. *IEEE Trans. Reliab.* **2018**, *68*, 23–44. [CrossRef]
100. Ratasich, D.; Khalid, F.; Geissler, F.; Grosu, R.; Shafique, M.; Bartocci, E. A Roadmap toward the Resilient Internet of Things for Cyber-Physical Systems. *IEEE Access* **2019**, *7*, 13260–13283. [CrossRef]
101. Mohandes, B.; Al Hammadi, R.; Sanusi, W.; Mezher, T.; El Khatib, S. Advancing cyber–physical sustainability through integrated analysis of smart power systems: A case study on electric vehicles. *Int. J. Crit. Infrastruct. Prot.* **2018**, *23*, 33–48. [CrossRef]
102. Cárdenas, A.A.; Amin, S.; Lin, Z.-S.; Huang, Y.-L.; Sastry, S. Attacks against process control systems. In Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security, Hong Kong, China, 22–24 March 2011; p. 355.
103. Marrone, S.; Rodriguez, R.J.; Nardone, R.; Flammini, F.; Vittorini, V. On synergies of cyber and physical security modelling in vulnerability assessment of railway systems. *Comput. Electr. Eng.* **2015**, *47*, 275–285. [CrossRef]
104. Pacheco, J.; Ibarra, D.; Vijay, A.; Hariri, S. IoT Security Framework for Smart Water System. In Proceedings of the 2017 IEEE/ACS 14th International Conference on Computer Systems and Applications (AICCSA), Hammamet, Tunisia, 30 Octorber–3 November 2017.
105. Lakshminarayana, S.; Teng, T.Z.; Tan, R.; Yau, D.K.Y. Modeling and Detecting False Data Injection Attacks against Railway Traction Power Systems. *ACM Trans. Cyber-Phys. Syst.* **2018**, *2*, 1–29. [CrossRef]
106. Bathelt, A.; Ricker, N.L.; Jelali, M. Revision of the tennessee eastman process model. *IFAC-PapersOnLine* **2015**, *48*, 309–314. [CrossRef]
107. Pacheco, J.; Hariri, S. IoT Security Framework for Smart Cyber Infrastructures. In Proceedings of the 2016 IEEE 1st International Workshops on Foundations and Applications of Self* Systems (FAS*W), Augsburg, Germany, 12–16 September 2016.
108. Orozco, Á.; Pacheco, J.; Hariri, S. Anomaly behavior analysis for smart grid automation system. In Proceedings of the 2017 IEEE International Autumn Meeting on Power, Electronics and Computing (ROPEC), Ixtapa, Mexico, 8–10 November 2017.
109. Ahmed, C.M.; Zhou, J.; Mathur, A.P. Noise Matters: Using Sensor and Process Noise Fingerprint to Detect Stealthy Cyber Attacks and Authenticate sensors in CPS. In Proceedings of the 34th Annual Computer Security Applications Conference, San Juan, PR, USA, 9–13 December 2018.
110. Ramotsoela, D.T.; Hancke, G.P.; Abu-Mahfouz, A.M. Attack detection in water distribution systems using machine learning. *Hum. Cent. Comput. Inf. Sci.* **2019**, *9*, 13. [CrossRef]
111. Liu, X.; Zhang, J.; Zhu, P. Dependence analysis based cyber-physical security assessment for critical infrastructure networks. In Proceedings of the 2016 IEEE 7th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), Vancouver, BC, Canada, 13–15 October 2016; pp. 1–7.
112. Abeykoon, I.; Feng, X. A Forensic Investigation of the Robot Operating System. In Proceedings of the 2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Exeter, UK, 21–23 June 2017; pp. 851–857. [CrossRef]
113. Palleti, V.R.; Tan, Y.C.; Samavedham, L. A mechanistic fault detection and isolation approach using Kalman filter to improve the security of cyber physical systems. *J. Process. Control.* **2018**, *68*, 160–170. [CrossRef]
114. Tundis, A.; Egert, R.; Mühlhäuser, M. Attack Scenario Modeling for Smart Grids Assessment through Simulation. In Proceedings of the 12th International Conference on Availability, Reliability and Security, Reggio Calabria, Italy, 29 August–1 September 2017; p. 13.
115. Aloqaily, M.; Otoum, S.; Al Ridhawi, I.; Jararweh, Y. An intrusion detection system for connected vehicles in smart cities. *Ad. Hoc. Netw.* **2019**, *90*, 101842. [CrossRef]
116. Elsaeidy, A.; Munasinghe, K.S.; Sharma, D.; Jamalipour, A. Intrusion detection in smart cities using Restricted Boltzmann Machines. *J. Netw. Comput. Appl.* **2019**, *135*, 76–83. [CrossRef]

117. Firoozi, F.; Zadorozhny, V.I.; Li, F.Y. Subjective Logic-Based In-Network Data Processing for Trust Management in Collocated and Distributed Wireless Sensor Networks. *IEEE Sens. J.* **2018**, *18*, 6446–6460. [CrossRef]
118. Sugumar, G.; Mathur, A. Testing the Effectiveness of Attack Detection Mechanisms in Industrial Control Systems. In Proceedings of the 2017 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C), Prague, Czech Republic, 25–29 July 2017.
119. Ahmed, C.M.; Ochoa, M.; Zhou, J.; Mathur, A.P.; Qadeer, R.; Murguia, C.; Ruths, J. NoisePrint. In Proceedings of the 2018 on Asia Conference on Computer and Communications Security, Incheon, Korea, 4–8 June 2018; pp. 483–497.
120. Elsaeidy, A.; Elgendi, I.; Munasinghe, K.S.; Sharma, D.; Jamalipour, A. A smart city cyber security platform for narrowband networks. In Proceedings of the 2017 27th International Telecommunication Networks and Applications Conference (ITNAC), Melbourne, Australia, 22–24 November 2017; pp. 1–6.
121. Liu, J.; Zhang, C.; Fang, Y. EPIC: A Differential Privacy Framework to Defend Smart Homes against Internet Traffic Analysis. *IEEE Internet Things J.* **2018**, *5*, 1206–1217. [CrossRef]
122. Garg, S.; Singh, A.; Batra, S.; Kumar, N.; Yang, L.T. UAV-Empowered Edge Computing Environment for Cyber-Threat Detection in Smart Vehicles. *IEEE Netw.* **2018**, *32*, 42–51. [CrossRef]
123. Pacheco, J.; Zhu, X.; Badr, Y.; Hariri, S. Enabling Risk Management for Smart Infrastructures with an Anomaly Behavior Analysis Intrusion Detection System. In Proceedings of the 2017 IEEE 2nd International Workshops on Foundations and Applications of Self* Systems (FAS*W), Tucson, AZ, USA, 18–22 September 2017.
124. Zhu, X.; Badr, Y.; Pacheco, J.; Hariri, S. Autonomic Identity Framework for the Internet of Things. In Proceedings of the 2017 International Conference on Cloud and Autonomic Computing (ICCAC), Tucson, AZ, USA, 18–22 September 2017.
125. Shaikh, F.; Bou-Harb, E.; Crichigno, J.; Ghani, N. A Machine Learning Model for Classifying Unsolicited IoT Devices by Observing Network Telescopes. In Proceedings of the 2018 14th International Wireless Communications & Mobile Computing Conference (IWCMC), Limassol, Cyprus, 25–29 June 2018.
126. Mozzaquatro, B.A.; Agostinho, C.; Goncalves, D.; Martins, J.F.; Jardim-Goncalves, R. An Ontology-Based Cybersecurity Framework for the Internet of Things. *Sensors* **2018**, *18*, 3053. [CrossRef] [PubMed]
127. Hamza, A.; Ranathunga, D.; Gharakheili, H.H.; Roughan, M.; Sivaraman, V. Clear as MUD. In Proceedings of the 2018 Workshop on IoT Security and Privacy, Budapest, Hungary, 20 August 2018; pp. 8–14.
128. Khan, Z.A. Using energy-efficient trust management to protect IoT networks for smart cities. *Sustain. Cities Soc.* **2018**, *40*, 1–15. [CrossRef]
129. Anthi, E.; Ahmad, S.; Rana, O.; Theodorakopoulos, G.; Burnap, P. EclipseIoT: A secure and adaptive hub for the Internet of Things. *Comput. Secur.* **2018**, *78*, 477–490. [CrossRef]
130. Gupta, M.; Benson, J.; Patwa, F.; Sandhu, R. Dynamic Groups and Attribute-Based Access Control for Next-Generation Smart Cars. In Proceedings of the 9th ACM Conference on Data and Application Security and Privacy, Richardson, TX, USA, 25–27 March 2019; pp. 61–72.
131. Adepu, S.; Mathur, A. Distributed Detection of Single-Stage Multipoint Cyber Attacks in a Water Treatment Plant. In Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security, Xi'an, China, 30 May–3 June 2016; pp. 449–460.
132. Garg, S.; Singh, A.; Kaur, K.; Aujla, G.S.; Batra, S.; Kumar, N.; Obaidat, M.S. Edge Computing-Based Security Framework for Big Data Analytics in VANETs. *IEEE Netw.* **2019**, *33*, 72–81. [CrossRef]
133. Vegh, L. Cyber-physical systems security through multi-factor authentication and data analytics. In Proceedings of the 2018 IEEE International Conference on Industrial Technology (ICIT), Lyon, France, 20–22 February 2018; pp. 1369–1374.
134. Alansari, Z.; Anuar, N.B.; Kamsin, A.; Belgaum, M.R.; Alshaer, J.; Soomro, S.; Miraz, M.H. Internet of Things: Infrastructure, Architecture, Security and Privacy. In Proceedings of the 2018 International Conference on Computing, Electronics & Communications Engineering (iCCECE), Southend, UK, 16–17 August 2018; pp. 150–155. [CrossRef]
135. Seymer, P.; Wijesekera, D. In-Flight Aircraft Smart Space Security using Multi-Entity Trust Evaluations. In Proceedings of the 2018 IEEE/AIAA 37th Digital Avionics Systems Conference (DASC), London, UK, 10 December 2018.
136. Ralston, P.A.; Graham, J.H.; Hieb, J.L. Cyber security risk assessment for SCADA and DCS networks. *ISA Trans.* **2007**, *46*, 583–594. [CrossRef]

137. Kang, E.; Adepu, S.; Jackson, D.; Mathur, A.P. Model-based security analysis of a water treatment system. In Proceedings of the International Workshop on Software Engineering for Smart Cyber-Physical Systems, Austin, TX, USA, 16 May 2016; pp. 22–28.
138. Navarro-Ortiz, J.; Sendra, S.; Ameigeiras, P.; Lopez-Soler, J.M. Integration of LoRaWAN and 4G/5G for the Industrial Internet of Things. *IEEE Commun. Mag.* **2018**, *56*, 60–67. [CrossRef]
139. Pollitt, M. A History of Digital Forensics. In *Advances in Digital Forensics VI*; Chow, K.P., Shenoi, S., Eds.; IFIP Advances in Information and Communication Technology; Springer: Berlin/Heidelberg, Germany, 2010; Volume 337. [CrossRef]
140. Reith, M.; Carr, C.; Gunsch, G. An examination of digital forensic models. *Int. J. Digit. Evid.* **2002**, *1*, 1–12. Available online: https://pdfs.semanticscholar.org/c73f/47d8385f452dfd25bbaab754874b65594ccd.pdf (accessed on 15 August 2019).
141. Agarwal, A.; Gupta, M.; Gupta, S.; Gupta, S.C. Systematic digital forensic investigation model. *Int. J. Comput. Sci. Secur.* **2011**, *5*, 118–131.
142. Qadeer, R.; Murguia, C.; Ahmed, C.M.; Ruths, J. Multistage Downstream Attack Detection in a Cyber Physical System. *Comput. Vis.* **2017**, 177–185. [CrossRef]
143. National Institute of Standards and Technology (NIST). *NIST Special Publocation 800-183 Nentworks of 'Things'*; Department of Commerce: New York, NY, USA, 2016.
144. Friedman, J.; Bouchard, M. *Definitive Guide to Cyber Threat Intelligence: Using Knowledge about Adversaries to Win the War against Targeted Attacks*; CyberEdge Group: Annapolis, MD, USA, 2015.
145. Paolini, P.; Blas, N.D.; Copelli, S.; Mercalli, F. City4Age: Smart cities for health prevention. In Proceedings of the 2016 IEEE International Smart Cities Conference (ISC2), Trento, Italy, 12–15 September 2016; pp. 1–4. [CrossRef]
146. Boddington, R. *Practical Digital Forensics*; Packt Publishing Ltd.: London, UK, 2016.
147. Ahmadi-Assalemi, G.; Al-Khateeb, H.; Maple, C.; Epiphaniou, G.; Alhaboby, Z.A.; Alkaabi, S.; Alhaboby, D. Digital Twins for Precision Healthcare. In *Cyber Defence in the Age of AI, Smart Societies and Augmented Humanity*; Springer Nature Switzerland AG: Cham, Switzerland, 2020; pp. 133–158.
148. Rahman, A.; Hassanain, E.; Hossain, M.S. Towards a Secure Mobile Edge Computing Framework for Hajj. *IEEE Access.* **2017**, *5*, 11768–11781. [CrossRef]
149. Mackintosh, M.; Epiphaniou, G.; Al-Khateeb, H.; Burnham, K.; Pillai, P.; Hammoudeh, M. Preliminaries of Orthogonal Layered Defence using Functional and Assurance Controls in Industrial Control Systems. *J. Sens. Actuator Netw.* **2019**, *8*, 14. [CrossRef]
150. Cam-Winget, N.; Sadeghi, A.-R.; Jin, Y. Can IoT be secured: Emerging challenges in connecting the unconnected. In Proceedings of the 2016 53nd ACM/EDAC/IEEE Design Automation Conference (DAC), Austin, TX, USA, 5–9 June 2016; pp. 1–6. [CrossRef]
151. Al-Khateeb, H.; Epiphaniou, G.; Reviczky, A.; Karadimas, P.; Heidari, H. Proactive Threat Detection for Connected Cars Using Recursive Bayesian Estimation. *IEEE Sens. J.* **2017**, *18*, 4822–4831. [CrossRef]
152. Kwak, B.I.; Woo, J.; Kim, H.K. Know your master: Driver profiling-based anti-theft method. In Proceedings of the 2016 14th Annual Conference on Privacy, Security and Trust (PST), Auckland, New Zealand, 12–14 December 2016.
153. *ACPO Good PRactice Guide for Digital Evidence*; Association of Chief Police Officers: London, UK, 2012; p. 43.
154. *Best Practice for Seizing Electronic Evidence v4.2*; US Department of Homeland Security: Washington, DC, USA, 2018; p. 27.
155. Montasari, R.; Hill, R.; Carpenter, V.; Hosseinian-Far, A. The Standardised Digital Forensic Investigation Process Model (SDFIPM). In *Blockchain and Clinical Trial: Securing Patient Data*; Jahankhani, H., Kendzierskyj, S., Jamal, A., Epiphaniou, G., Al-Khateeb, H., Eds.; Springer Nature Switzerland AG: Cham, Switzerland, 2019; pp. 169–209.
156. Miller, C.; Valasek, C. Remote Exploitation of an Unaltered Passenger Vehicle. 2015. Available online: https://ericberthomier.fr/IMG/pdf/remote_car_hacking.pdf (accessed on 4 May 2019).