
Article:
Czekster, Ricardo M., Metere, Roberto orcid.org/0000-0001-6992-4285 and Morisset, Charles (2022) Incorporating Cyber Threat Intelligence into Complex Cyber-Physical Systems:A STIX Model for Active Buildings. Applied Sciences (Switzerland). 5005. ISSN: 2076-3417

https://doi.org/10.3390/app12105005

---

applied sciences

MDPI

Article

Incorporating Cyber Threat Intelligence into Complex Cyber-Physical Systems: A STIX Model for Active Buildings

Ricardo M. Czekster [1,*], Roberto Metere [2,3,*] and Charles Morisset [2]

[1] School of Informatics and Digital Engineering, Aston University, Birmingham B4 7ET, UK
[2] School of Computing, Newcastle University, Newcastle upon Tyne NE1 7RU, UK; charles.morisset@ncl.ac.uk
[3] The Alan Turing Institute, London NW1 2DB, UK
* Correspondence: r.meloczekster@aston.ac.uk (R.M.C.); roberto.metere@ncl.ac.uk (R.M.)

Abstract: Active buildings can be briefly described as smart buildings with distributed and renewable energy resources able to energise other premises in their neighbourhood. As their energy capacity is significant, they can provide ancillary services to the traditional power grid. As such, they can be a worthy target of cyber-attacks potentially more devastating than if targeting traditional smart buildings. Furthermore, to handshake energy transfers, they need additional communications that add up to their attack surface. In such a context, security analysis would benefit from collection of cyber threat intelligence (CTI). To facilitate the analysis, we provide a base active building model in STIX in the tool cyberaCTIve that handles complex models. Active buildings are expected to implement standard network security measures, such as intrusion-detection systems. However, to timely respond to incidents, real-time detection should promptly update CTI, as it would significantly speed up the understanding of the nature of incidents and, as such, allow for a more effective response. To fill this gap, we propose an extension to the tool cyberaCTIve with a web service able to accept (incursion) feeds in real-time and apply the necessary modifications to a STIX model of interest.

Keywords: cyber threat intelligence; situational awareness; structured cyber-attack representations; cyber-security; smart grid; cyber-physical systems; active buildings

Citation: Czekster, R.M.; Metere, R.; Morisset, C. Incorporating Cyber Threat Intelligence into Complex Cyber-Physical Systems: A STIX Model for Active Buildings. *Appl. Sci.* **2022**, *12*, 5005. https://doi.org/10.3390/app12105005

Academic Editor: Agostino Forestiero

Received: 15 April 2022
Accepted: 13 May 2022
Published: 16 May 2022

1. Introduction

The modern electrical grid, or smart grid, constantly evolves to offer an increasing variety of services that the traditional grid could not [1–3]. Such services sustain residential customers, business activities, and industrial organisations in an unprecedented scale. Smart buildings play a key role in the smart grid [4], as not only do they consume energy as traditional buildings, but they also produce (and store) energy from renewable sources. A great deal of smart grid infrastructure elements is exposed, however, to constant malicious activity [5–8]. With the strengthening of security measures, also cyber-attacks have augmented in depth, breadth, intensity, and sophistication [5,9]. These incursions have the potential of corrupting and disturbing systems, exposing users' confidential data, and causing significant damage or financial loss, particularly when adversaries coordinate skill and effort in variable length campaigns [10–12], e.g., load changing or state-sponsored attacks. The operational status of infrastructures is monitored and controlled through services adopting Internet-of-Things (IoT) devices over public and private domains in wired or wireless modes [6]. An important service is remote control; its spread adoption translates to a growth of interconnected cyber-physical systems (CPSs). One example of a CPS is the smart grid where power managers implement dynamic load responses for different energy profiles to balance supply and demand [13] that provides stability, reliability, and resilience to stakeholders [14]. Such smart components were studied in the literature employing stochastic programming, deep learning, robust hub management, and economical models [15–18]. Moreover, the assessment of threats in such systems is

traditionally collected as *cyber threat intelligence* (CTI) [19], also termed *information security threat intelligence*, or ISTI; however, we shall use CTI throughout this work.

Over time, business incentives, lower prices, and greater trust in renewable energy are convincing consumers to convert to *prosumers*, i.e., entities acting as both consumers and producers. One observes a high penetration of renewable generation devices such as solar roof-top photovoltaic or wind turbines combined with incentives to drive electric vehicles [20,21]. Future prosumers will plug their generators directly in the distribution grids and (indirectly) assist the wider grid with ancillary services, such as frequency balancing [22] and grid stability. In this paper, we focus on a special type of prosumers, active buildings, that "sustain a country's energy infrastructure" [23] and are deployed in conjunction with electrical power grids. An active building can be seen as a CPS, or an organised assembling of multiple CPSs, with capabilities to distribute energy, or exchange energy with other active buildings, potentially selling it at different prices. They could function as individual power stations, supporting the wider grid and the local domain where they are located, implementing the notion of "buildings as power stations" [4,24]. Active buildings are not only different from traditional smart buildings and microgrids from an energetic perspective, but also from a cybersecurity perspective: indeed, Figure 1 illustrates how additional communication and power links need to be setup [25,26].

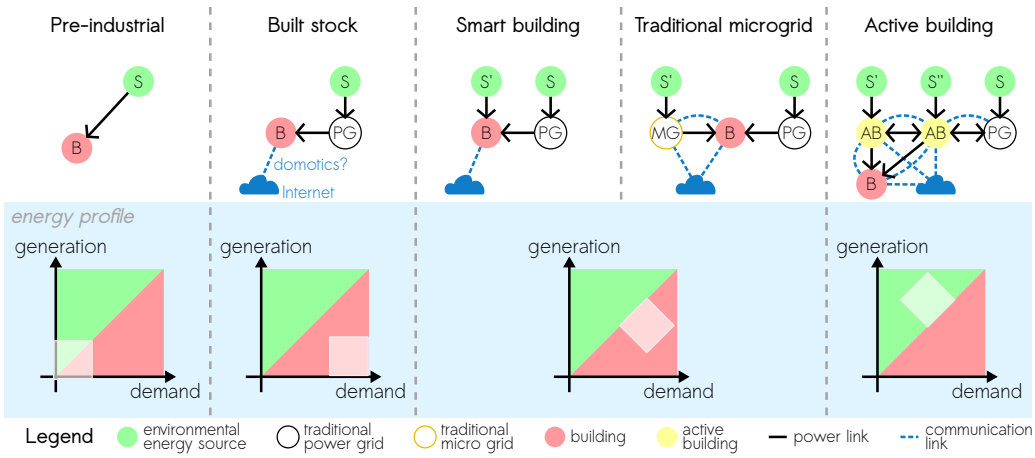

Figure 1. Active buildings have a different energy profile; they also exchange power with other entities, and the corresponding handshake to establish all the parameters of the energy transfer requires additional communications. Adapted from Fosas et al. [27].

Communication links are used to handshake sessions of bidirectional energy transfers that will physically flow due to dedicated power links. Such links can be indeed targeted by cyber attacks with the purpose of taking advantages in the energy market [7]. With respect to the energy market in microgrids, we mention the work of Dasgupta et al. [28] that identified potential cyber-attacks in such systems as well as implications to smart grids. On the same line, and conversely to what happens in microgrids, the production or storage of energy lies in the same physical infrastructure as consumers; thus, control communications in active buildings can be exchanged through the existing network channel of the building.

Different organisations may manage these communicating active buildings. We assume a context where, as a system gets eventually compromised, security officers will share CTI across pertaining trusted organisations that can benefit from using such knowledge to deter impending cyber-attacks. This exchange of CTI highlights the importance of effectively describe, report, and share it by using standardised and structured formats comprehensible by analysts across diverse disciplines. One of the most popular standard format used by cybersecurity analysts is STIX^{TM} (Structured Threat Information eXpression) [29]. STIX allows to describe, visualise, and share CTI models to support richer and wider cyber-attack narratives to explain ongoing incursions. As such, the complexity and the number of attack vectors, as well as their capacity to harm, is higher than regular smart

buildings in microgrids. Such additional complexity reflects to models that hinder the effectiveness of timely responses to incidents.

To tame such complexity, we model a basic scenario to manage CTI in the context of active buildings. We used the tool cyberaCTIve [30] to create and manage our model. The model can be exported and it is fully compliant to the STIX format, so other tools can easily manipulate it. We have chosen this tool as it implements a *timeline* that can be used for real-time analysis, where an analyst could inspect the *chain of events* and then try to reason about the progression of cyber-attacks, or other anomalies that require attention from the cybersecurity perspective. However, changes to the model in cyberaCTIve are manual, so the effectiveness of the timeline is restricted. To make it effective, we extended the tool with a service that accepts security feeds from (automated) external sources, such as intrusion detection systems (IDS). So, if an IDS detects a cyber attack, it can automatically augment the CTI with such knowledge and notify security officers, who can then promptly intervene and share their information with security officers in adjacent buildings. Next, we highlight our paper contributions:

- we survey on solutions on how to integrate CTI directly into active buildings as well as any cyber-physical system that produces output data relevant to analysis;
- an overview of literature on CTI, discussing shortcomings and advantages of its use and measures on how to best integrate indicators of anomalies, expert opinions, threat agents, and so forth, into standardised models (here, described using STIX);
- we provide a comprehensive discussion on cybersecurity prospects of active buildings, differentiating them from smart buildings and highlighting the additional datasets that are produced and how to leverage them using CTI;
- we exemplify the use of an auxiliary tool called cyberaCTIve to assist the process of identifying intelligence items and storing in a specialised information system to support sharing and understanding about cyber-attack progression and timely defences against malicious incursions; and
- we give an in-depth analysis on how to integrate cybersecurity in early phases of any active building proposition, showing the novel range of services and systems that they aggregate into the attack surface and how to cope with CTI under these considerations.

We organise our paper as follows. In Section 2, we discuss active buildings and CTI. In Section 3, we detail our base model for active buildings in STIX, whereas in Section 4, we discuss our proposition and outline advantages and trade-offs. We end the paper on Section 5 with our conclusion and future work.

2. Cyber Threat Intelligence and Active Buildings

Threat intelligence is knowledge collected with the purpose of responding to incidents due to malicious adversaries (our focus), hazards, or faults. Thus, such knowledge includes context, mechanisms, technologies, entities, campaigns and mitigations that can be used by security experts to avoid or respond to similar incidents in the future. It has been long observed that data, information, knowledge, intelligence, and wisdom are interrelated concepts that play a crucial role toward an effective system analysis [31]. Recent advances introduced the terminology *cyber threat intelligence* (CTI) [19,32] to encompass information technologies.

In the real world, CTI holds value to enterprises wishing to enlarge the analysis scope when considering cyber-attacks. We mention the SANS Institute (SANS is a US institute and the acronym stands for SysAdmin, Audit, Network, and Security.) report tackling how it is employed by organisations [33]. They noticed an increase in interest over the years; however, stakeholders comment on the need of expanding use cases to enhance how to understand the CTI benefit and security posture gains. The analysis also discussed on the need for improving report automation and ways of enlarging adoption by government-sponsored groups, private sector, and industry-focused groups, to name a few of their findings.

CTI does not enjoy a solid, established, standardised, or recognised format to store intelligence. Examples of data sources [33] combine technical, human, and internal domains, and the knowledge could be both structured and unstructured [19,34]. This naturally raises concerns about the *quality* of CTI-based feeds: indeed, it is a topic of wide interest [35,36]; Tundis et al. [37], for instance, investigated automated assessment of sources and computed a relevance score index to reduce the time needed to verify gathered intelligence. Another task on the same line is that of assessing and evaluating data made available from various sources: open (publicly available) CTI feeds, data from security vendors, industry reports on vulnerabilities, open-source intelligence (OSINT) reports [38], security data extracted from IDS or firewall, data from the security, information, and event management (SIEM) platform, incident response systems, and network traffic and flow logs, to mention a few. Ramsdale et al. [39] conducted a comparative analysis of threat intelligence sources, highlighting structured standards such as STIX [29], Trusted Automated Exchange of Indicator Information (TAXII™) [40], and Cyber Observable eXpression (CybOX™) [41,42].

CTI is undoubtedly a valuable instrument for the protection of cyber-physical systems [19]. A complex CPS can comprise many devices, interlinked through either power or communication lines, or both and in manifolds, e.g., an IoT device can be connected to the power line as well as to the Internet through a cable, a WiFi, and a mobile data connection. The more elements constitute a CPS, the bigger is its attack surface exposed to cyber attacks, and that translates to a higher amount of information collected as CTI. One example of such complex system is active buildings.

2.1. Active Buildings

Active buildings are an emerging technology having a special role in the transition to a sustainable energy infrastructure and a decarbonised society [27]. They are not traditional smart buildings, as, conversely, active buildings communicate with other peers not only for coordination purposes but also for exchanging energy among them [43]. Thus, they can energise not only their own premises but also their surrounding peers without the intervention of the conventional power grid. Active buildings employ intelligent sensing and information systems to enhance power quality [44,45] and make prompt decisions to support the main grid's national infrastructure and promote near-zero energy [46–48]. Figure 2 shows an overview of the devices within the active building offering, that must be taken into account as potential attack vectors in cybersecurity analyses. From the cybersecurity perspective, the additional services brought by active buildings would provide further incentives to perform attacks. Furthermore, their effect can be devastating on the security of the power grid. Being the power grid a critical infrastructure, the increased purposes for carrying out an attack to an active building incentivise malicious entities to perpetrate an attack.

Active buildings need not be a single large smart building with energy distribution capabilities. For example, a collection of residential houses equipped with static batteries may be controlled to synchronously act like active buildings. Residents will plug their electric vehicles into smart charging stations, several smart home appliances such as smart plugs, sensors, alarm systems, surveillance systems, dishwashers, air conditioning, and so on. Energy trading, albeit an interesting feature, will be considered after the core business propositions on active buildings have been addressed. Clearly, an oversimplification of active buildings models translates to a reduction of the CTI taken into consideration, which would make a security analysis ineffective, and so the related incident responses.

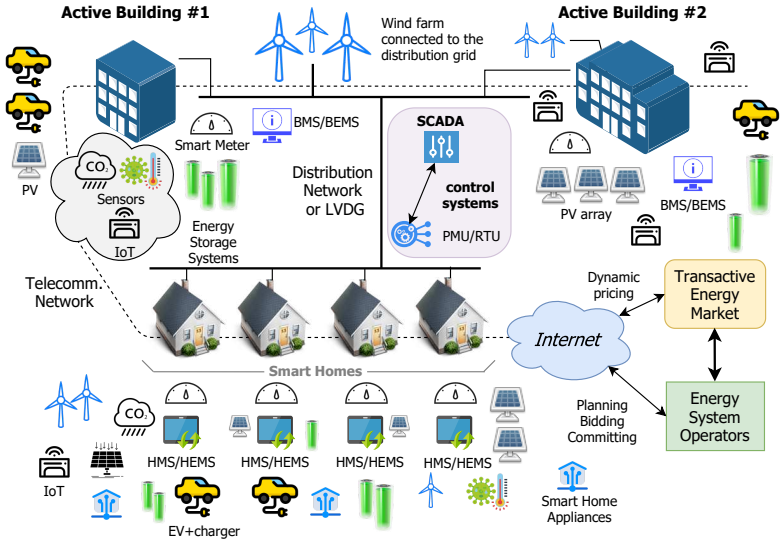

Figure 2. Overview of a tentative architecture and most likely devices that managers will deploy for enacting the active building business proposition.

The complexity of cyber-attack types potentially affecting active buildings is increased from their ability to generate and consume locally without ever disconnecting from the main (conventional) grid, de facto acting as (part of) a *microgrid*. Microgrids usually operate in low-voltage distribution grids or in active distribution networks [49]. An example of an issue in these contexts could be forcing prosumers to use the main grid instead of using the services provided by active buildings. An adversary might exploit vulnerabilities of smart meters or smart chargers to carry out such attacks. We do not cover all aspects of cybersecurity but provide enough elements to appreciate the complexity of CTI in active buildings. With the same aim, Figure 3 shows an overview of data sources that is generally required to readily review for assessing cybersecurity in the context of active buildings.

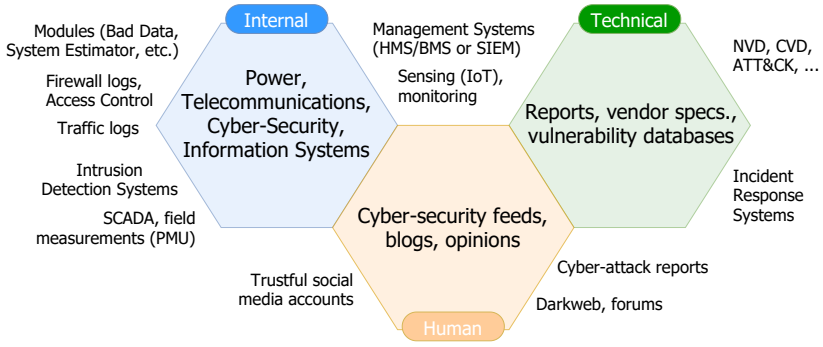

Figure 3. Common CTI sources for assessing cybersecurity concerns in non-trivial infrastructure.

A comprehensive knowledge of cybersecurity in the context of active buildings, microgrids, and cyber-physical systems is fundamental for an effective CTI model of a real scenario.

Cybersecurity of Active Buildings

There is also preoccupation with data handling throughout active buildings, protecting stakeholders from improper use, and caring about privacy concerns. Active buildings present a large attack surface to protect where adversaries might seek to disturb these elements and provoke chaos, intercept/eavesdrop/delay communications, steal/divert power for financial gains, or exfiltrate data (for ransom or other malicious reasons). Cybersecurity should adapt to emerging technologies that will be attached to active buildings' operation as well as agnostic regarding telecommunication protocols deployed. Timely and regular

vulnerability assessment will prioritise key devices into the cybersecurity posture and act on preparedness to withstand most common threats to tackle cyber-attacks.

This equipment will run embedded software that are highly susceptible of cyber-attacks. These devices correspond to both low and high wattage power spectra, from lightweight (e.g., for lighting) to energy-hungry (e.g., for lifts). Under active buildings' infrastructure, attack detection will play a significant role for determining and thwarting malicious interventions. This is true in long term incursions such as advanced persistent threats [50,51] that are hard to perceive and may cause massive damage and financial loss to stakeholders. Active buildings will provide seamless and flexible power provision for stakeholders that will see clear advantages and incentives to step forward towards transitioning to active propositions.

Given its reduced scale, microgrids are more susceptible to cyber-attacks. They employ fewer contingencies to tackle imbalances in frequency due to differences in supply-demand [10,12]. The wider grid, on the other hand, has several physical security measures to withstand even disproportionate imbalances that may occur (for various reasons). For instance, standardisation institutes such as the North American Electric Reliability Corporation (NERC—US) and the European Programme for Critical Infrastructure Protection (EPCIP) proposed strict security measures and contingencies for electric power systems. For example, they are designed to withstand so called $(N-1)$ single contingency criterion to enforce reliability constraints, making the system withstand a single failure to remain operating. Refer to NERC Standard 51—http://www.nerc.com (accessed on 15 May 2022).

It is under investigation how to efficiently deploy active buildings and equip it with intelligent and flexible demand response features that could prevent cyber-attacks from scaling over the localised network. For example, Yankson and Ghamkhari [52] have studied how the energy system may influence power provision and even thwart load changing attacks altogether. Another way is to profit from smaller-scale data generation (far less than what is generated in the wider grid) and inspect anomalies and customer usage peaks to identify, confirm, and differentiate over-use from cyber-attacks. There is an abundance of work on detecting faults for grid-connected photovoltaic power systems [53,54] using varied techniques such as on-line fault detection or failure diagnosis [55–57].

2.2. Cybersecurity and CTI in Active Buildings

Without going into many details, we summarise what kind of CTI and CTI sources we expect that active buildings will inherit or reuse from related technologies. There is a wealth of contributions on cybersecurity of smart grids [5,58], microgrids [25,26,59,60], in IoT [6], and smart metering [61] that can directly apply for active buildings. Zografopoulos et al. [62] discussed cybersecurity issues, threat modelling, and risk assessments in so called cyber-physical energy systems (CPES), again strongly relatable to active buildings. Kavallieros et al. [63] discussed threats, actors, and cyber-attacks across domains citing databases, methodologies, and threat related taxonomies and frameworks. Common protective measures such as cybersecurity awareness, risk communication, networking firewalls, and IDS across levels in home/building management systems. In business/enterprise levels, analysts depend on accurate measurements and historic data to perform medium/long planning efforts. We suggest further reading about the cybersecurity underpinnings behind the active buildings from Czekster et al. [64], where its authors detail a roadmap for tackling cyber-attacks in this architecture.

To appreciate some of the knowledge that one could find inspecting CTI on active buildings, we describe some of the known vulnerabilities that have been found across the years on the fields which they extend or can be a part of. Previous work discussed malicious interventions in power grids and industrial control systems (ICS) over the years [65]. ICSs are particular CPSs allowing remote, automated control of industrial systems. Those incursions caused extensive damage and financial losses, sometimes blacking out entire regions or incapacitating information systems. As an example, the Stuxnet malware acquired the control of nuclear facilities in Iran and induced physical damages to

turbines with catastrophic damage [66–70]. Another malicious incursion called BlackEnergy [71,72] employed DoS attacks in SCADA systems in ICS. Furthermore, the Industroyer or Crashoverride [73,74] also targeted ICS as a malware that corrupted switches, breakers, and substation communication protocols and was responsible for a power grid failure in Ukraine. The Dragonfly [75] allowed adversaries to access and gain unauthorised control over critical systems whereas Wannacry [76,77] targeted information systems at healthcare facilities (mostly hospitals), banks, and universities and demanded ransomware so administrators could resume operations. More recently, the Trisis [78] malware successfully attacked equipment employed in energy, oil, and gas control systems. Other research dealt with a combined analysis of BlackEnergy, Crashoverride, and Trisis [79], whereas Hemsley et al. [80] discussed the history of ICS cyber incidents.

There are significant initiatives to deal with the above malicious incursions. MITRE, a US based organisation, has developed the adversarial tactics, techniques, and common knowledge (ATT&CK®) framework [81] and defined 'matrices' (namely enterprise and mobile domains) to help stakeholders understand the tactics, techniques, and procedures (TTP) deployed by attackers. MITRE has also introduced a similar initiative for applying ATT&CK to industrial control systems (ICS) called ATT&CK for ICS [82], due to observed particularities in these systems. The ATT&CK framework superseded the CAPEC (Common Attack Pattern Enumeration and Classification) [83], and we witness academic and industrial partners engaging with reporting efforts to mitigate cyber-attacks. The framework is a valuable resource to help security officers to counteract cyber-attacks with threat-informed defences. ATT&CK differs from classic Cyber Kill Chain® [84] pioneered by Lockheed Martin [85] in the sense that it identifies and maps adversarial actions that could happen without any order. Kwon et al. [86] has created a method for translating ATT&CK matrix threats directly into NIST's cybersecurity framework. This clearly shows the need to cross-reference models altogether helping cybersecurity experts in their tasks.

Other data sources could employ design level techniques such as automatic cryptographic protocol language generators [87] or it could come from public databases of software vulnerability. An example is the Common Vulnerability Scoring System (CVSS) [88] that combines efforts with the US National Vulnerability Database (NVD)—https://nvd.nist.gov/ (accessed on 15 May 2022). The NVD uses CVSS to track, score, document, and describe details about discovered vulnerabilities reported by industrial partners and individuals. Computing a scoring system that is vouched by the cybersecurity expert community is invaluable for practitioners, since the numeric index provides a notion on severity and the vulnerability impact on the infrastructure. We mention also that the MITRE Corporation, in cooperation with the NIST and the NVD, maintains the Common Vulnerabilities and Exposures (CVE) database—https://cve.mitre.org/ (accessed on 15 May 2022).

Table 1 lists major developments over the years tackling novel research in cybersecurity and CTI in CPS. It highlights a host of concepts, scope, and concerns and it comments on the results' achievements, methodology, and their novelty. The table also remarks the set of key notions behind each approach thus enabling one to consider research gaps for further exploration. According to Table 1, a plethora of data is potentially produced by the elements encompassing the CPS to provide power services to stakeholders. One deficiency is about the timely processing and analysis of relevant data to produce actionable analysis artefacts for building managers and cybersecurity officers. Another aspect worth considering is to apply current state-of-the-art practices that have been proved to work and were tested in several different infrastructure and learning from best approaches to incorporate into novel architectures such as active buildings. There is also space for improving auxiliary tools for creating and sharing gathered intelligence across trustful counterparts.

Table 1. Selected state-of-the-art of cybersecurity for leveraging CTI in CPS (including active buildings).

Reference	Scope	Concern	Key Concept	Approach	Observation
[44,45]	Active buildings	Definition	Decarbonisation	Position	Authors have commented on the role of active buildings to support the wider grid.
[46–48]		nZEB	Frameworks	Position	Commentary on frameworks and discussion of what entails nZEB buildings.
[53–55]	Microgrid	Fault detection	Analysis	Simulation Discussion	Penetration of photo voltaic devices and implications in microgrids, discussing regulatory aspects and fault detection.
[56,57]		Failure diagnosis	Online diagnosis	Data analysis	Employed anomaly detection techniques including machine support vectors.
[5,58]	Cybersecurity	Smart grid	General	Survey Survey of surveys	Protective measures, techniques, models and frameworks to support cybersecurity.
[64]		Active buildings	Roadmap	Analysis	Discussion of a roadmap to tackle cybersecurity in active buildings.
[6,61] [14,62]		Smart meters IoT Microgrid CPES	Equipment	Analysis	Protective measures to components in critical infrastructure. Discussion on cybersecurity guiding principles, methodologies, and approaches to defend against attacks.
[65]		ICS	Grid	Analysis	Issues for protecting power grids.
[80]			Analysis	Historical	Commentary on history of incidents.
[50,51]		APT	Analysis	Detection	Combating APTs in critical infrastructure.
[66–68,74]		Attacks	Stuxnet	Analysis Reporting	Detailed description of attacks to electrical power grids involving large-scale ICS.
[73,75,76]			ICS	Analysis Reporting	Other attacks in ICS and power grids with large impact to customers and stakeholders.
[10,12]			LCA	Simulation	Coordinated load changing attacks involving swarms of infected IoT in high-wattage equip.
[19,32]	Cyber Threat Intelligence	Terminology	Application	Position Survey	Survey of technical CTI and threat based approaches to work with intelligence.
[63]		Taxonomy	Application	Survey	Discussion on threats, actors, and cyber-attacks across domains citing databases, methodologies, and threat frameworks.
[33]		Analysis	Statistics	Survey	It shows how CTI adoption has changed over the years as organisations became aware.
[37]		Assessment	Automation	Analysis	Authors have used meta-data to train regression models for automation of sources.
[39]		Comparisons	Threats	Analysis	Analysis of threat intelligence sources and standards (STIX, TAXII, CybOX).
[30]		Tools	Visual front-end	Implementation	A visual front-end to cope with STIX-based models and model management features.

3. A Base STIX Model for Active Buildings

Part of our effort is generating a tentative base STIX model that captures the most peculiar parts of active buildings. We argue that even a real-world model would not be final, as some parts would need continuous updates, e.g., the CTI database, adversarial behaviour and feeds, as opposed to other parts that seldom (but still) change or are upgraded, e.g., the infrastructure. We show how even a base model for active building looks complicated if illustrated by the traditional automated graph visualisers for STIX models; however, we provide a (manually) simplified graph to effectively describe the components of our base model. Alternatively, the same simplicity is offered by cyberaCTIve through its dashboard view, where groups are clearly marked, as well as relations are organised in a way that do not visually overlap and are much easier to manipulate. We discuss all these details later in this section.

As introduced above, an important point to consider is that practical models are not supposed to be *final*, at least because CTI changes over time, e.g., new vulnerabilities are found or new services or protocol versions are implemented. In particular, Figure 4 shows the continuous modelling effort for devising a comprehensive STIX model for active buildings. This could be viewed as a cyclical process where cybersecurity officers consider the infrastructure, the feeds, the intelligence, and the adversarial behaviours. The centre of the figure shows the services of active buildings and what some key devices that it manages to support their sustainable operation.

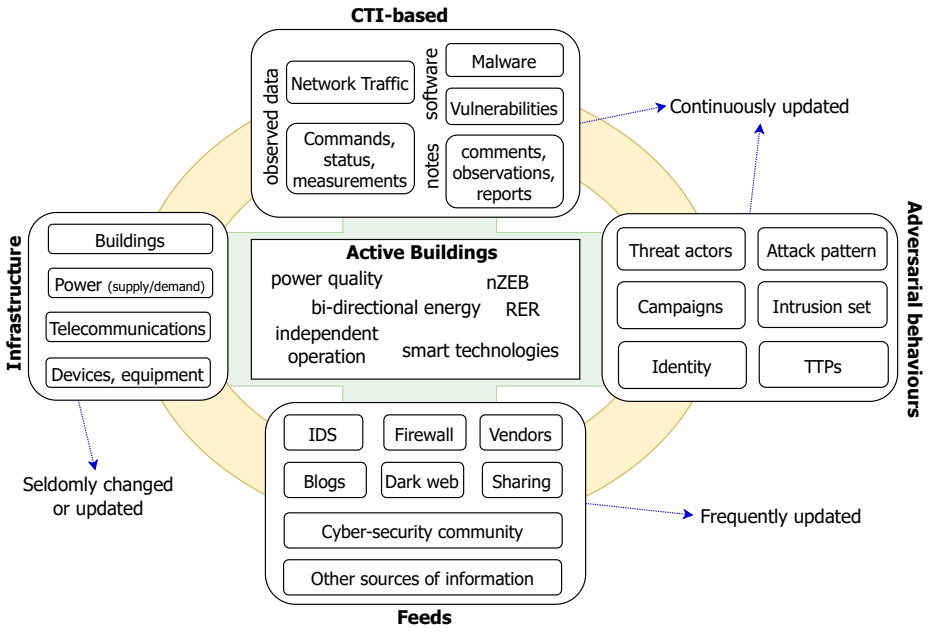

Figure 4. Modelling effort for Active Buildings encompassing infrastructure, intelligence, and feeds, all coupled with adversarial behaviours.

The rightmost part of Figure 4 highlights the potential attack surface of active buildings as well as the required STIX elements to compose a CTI solution that encompasses the cyber-physical elements coupled with adversarial actions plus available intelligence streams. Changes in infrastructure will demand low effort (only when new devices or equipment ingress the network) whereas CTI-based information and adversarial behaviour will necessitate continuous updating, to keep up with potential malicious incursions that are documented in cybersecurity feeds or community reports.

Conscious that models cannot be final, we prepared a base model for active buildings that at least captures all their peculiarities, in the sense that if elements are removed, then it reduces to systems that are usually addressed differently. An example can be that of removing a power generation source inside the building, e.g., solar panels; if removed, the building would not have the capacity to provide energy to its neighbours (on average), as opposed to what active buildings do.

Figures 5 and 6 shows the base STIX model for two active buildings cooperating as energy agents exchanging contextual data and energy altogether (compared with how they are drawn by the official STIX visualiser in Figure A1 in Appendix A). Future deployments of active buildings should also address incorporating CTI feeds into this proposition, as it is a valuable tool to thwart cyber-attacks in preparedness efforts and cybersecurity hardening practices. The former shows a graph view from the official STIX visualizer, while the latter is a simplified graph manually reconstructed to simplify its description. We shall proceed explaining a representative model to study the incorporation of CTI into active buildings. For this model, we will work with the following definitions for two active buildings (namely `Active Building#1` – AB#1 and `Active Building#2 - AB#2` having different components. For instance, `AB#1` is called "Greenwich Building" with an EV charger

station, whereas AB#2 is called "Woolwich Building". Both active buildings have smart meters and a solar array, reinforcing the concept that they share infrastructure elements altogether. In terms of CTI, AB#1 has assigned a malicious campaign that uses a malware from an APT group, whereas AB#2 has associated to the model some unusual data streams (with network traffic objects).

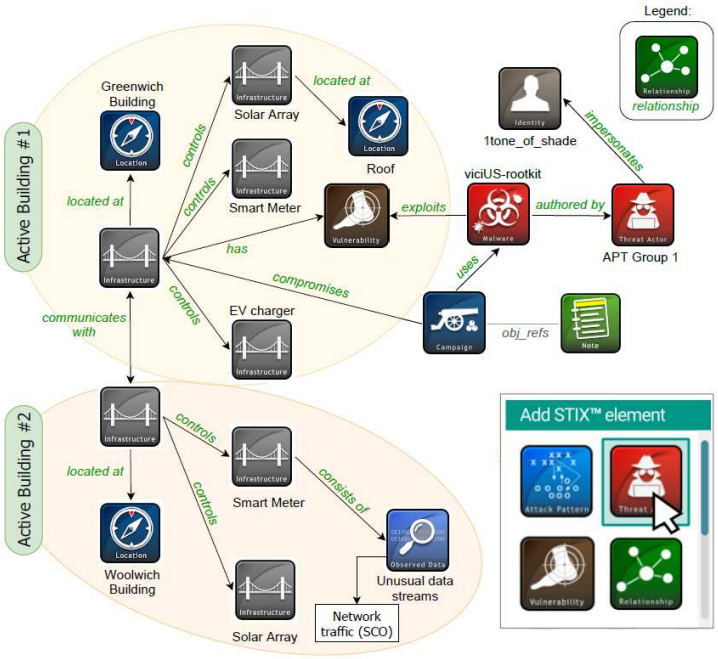

Figure 5. Base STIX model for active building as a graph manually simplified aiming for an intuitive representation. The arrows map relations among STIX elements.

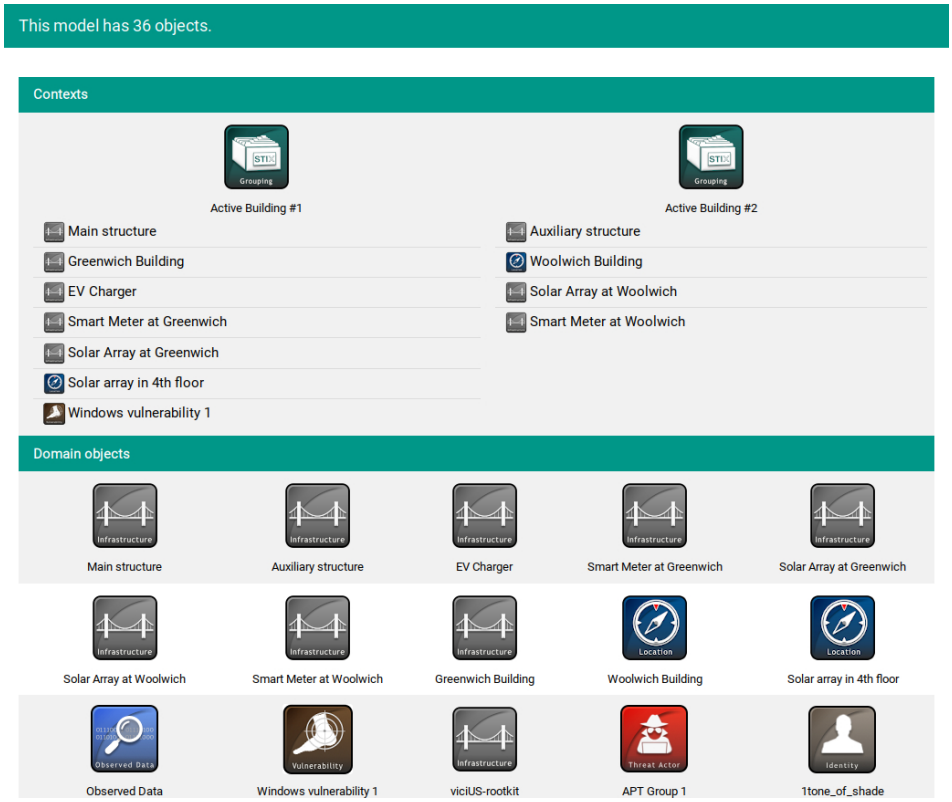

Figure 6. Base STIX model for active buildings in the dashboard of cyberaCTIve.

The STIX model shown in the figure details the infrastructure behind the active buildings and it combines with CTI data and potential observed TTPs for a malicious actor (in this example, by `APT Group 1`, a fictitious group that operates by installing malware in smart buildings). It is worth noticing that this base example only shows basic elements required to understand the possibilities enabled by the tool. Advanced analysis should encompass the totality (or almost) of the attack surface and points that may be used by cyber-attackers for exploring vulnerabilities.

Feed the Model with Real-Time CTI

Among the features of cyberaCTIve, one is to log modifications to the STIX model as *events in a timeline*. This allows for basic forensic analysis on the model, e.g., in our case the model of an active building. Unfortunately, cyberaCTIve [30] does not implement any automation for feeding the model with real-time incidents. So, we extended the tool to allow an *external* source of CTI to augment the STIX model (Observation: we shall release this extension as open-source in due course, adjusting it to include a link to it in the final version of this paper.). This is a critical improvement that would allow an IDS not only notifying security officers but also to apply in real-time the incident into an existing model of the active building. In this sense, the whole modelling architecture, i.e., the web-app cyberaCTIve, the IDS and the notification system, can be seen as a digital twin of the active building.

These data is used to represent a STIX model for active buildings. The actual implementation is provided as a web service, whose architecture is illustrated in Figure 7.

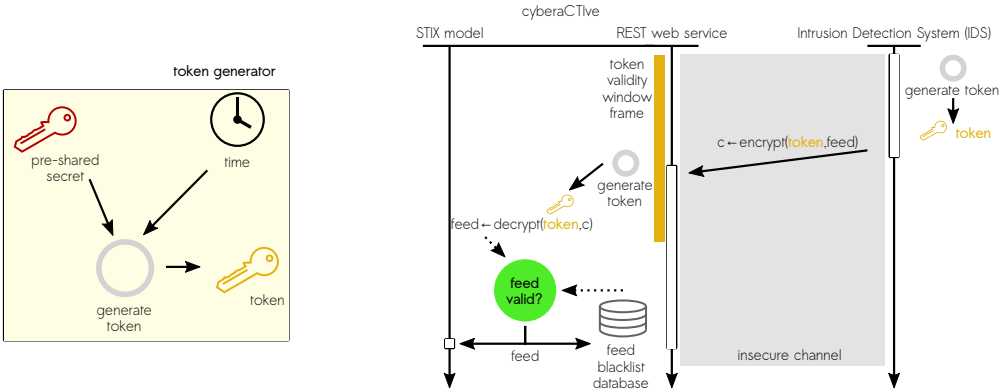

Figure 7. Architecture of the real-time feeder that extends cyberaCTIve.

The web service is a PHP implementation of a representational state transfer (REST) service [89] with authentication. To do so, our web service extends the authentication capabilities of cyberaCTIve to allow external devices (the IDS) to authenticate themselves through lightweight encryption system based on a preshared password. Obviously, we do not expect incursions (or faults) to happen at a high rate to justify a lightweight requirement. However, one the most dangerous cyber attacks that undermines the availability of the services (up to blackouts) are Denial-of-Service (DoS) attacks. DoS attacks are often carried out through flooding the (communication) network [90], that would much more likely prevent a nonlightweight communication to be delivered. In conclusion, being the feeder a lightweight protocol is a clear and significant advantage to get updates on such situations as quickly as possible. A solid alternative would be to create a dedicated communication line between the feeder and cyberaCTIve, but this solution would require additional expensive setup.

A token generation algorithm $\mathcal{G} : K \times T \to K_T$, where K denotes the space of all *valid* (An administrator may ban low-entropy passwords, e.g., short or easy to crack by a dictionary-based brute-force attack.) preshared keys, T the set of timestamps and K_T the set of valid tokens. Tokens will be used as ephemeral keys in a probabilistic symmetric encryption scheme, whose encryption algorithm is $\mathcal{E} : K_T \times F \to C$, where F is the set of

all feeds and C all the ciphertexts, and whose decryption algorithm is $\mathcal{D} : K_T \times C \to F$. The encryption system need not to use strong tokens (with a high number of bits) as their validity is used only to achieve authentication and they are refreshed frequently. In concrete, they get refreshed much before than a brute-force attack would be successful.

The sequence diagram in Figure 7 shows that as soon as an incursion is detected, the IDS generates a token $k \leftarrow \mathcal{G}(s,t)$ where s is the preshared secret between the IDS and cyberaCTIve and t is the current timestamp in the IDS. The token k is used as an ephemeral key to encrypt the feed $c \leftarrow \mathcal{E}(k,f)$. The encrypted feed c is sent to cyberaCTIve through the REST web service. Upon reception, the web service regenerates the token $k' \leftarrow \mathcal{G}(s,t')$, with its current timestamp. We note that $k' = k$ only if the message is processed within the allowed window frame. Additionally, it checks if the feed has already been processed (with that token). This validity check is necessary if we want to avoid *replay attacks*. Importantly, the time as measured by cyberaCTIve must be well synchronised with the time as measured by the IDS (this can be done through a centralised time server that is easy to set up). Also, an *expected* communication delay $\bar{t}$ might be subtracted by the web service to reconstruct the token, $k \leftarrow \mathcal{G}(s,t'-\bar{t})$. The validity of the token cannot be directly verified, but if the token is incorrect, then its decryption with another token would generate a nonunderstandable feed that would be invalid. Conversely if the token is correct, the right feed $f \leftarrow \mathcal{D}(k,c)$ can be reconstructed. If the pair feed-token, (f,k), is not in a database of processed feeds, it means that is yet to be processed. Finally, the feed f can be safely sent to augment the STIX model and the pair (f,k) is stored into the database of processed feeds (that would blacklist, hence invalidate, an eventual reception of the same feed twice).

Identical feeds can be processed only if the token is different: we notice that an adversary should not be able to forge a new encrypted feed. This requires the encryption system to leak negligible information over time; in particular, even an adversary should not able to reconstruct tokens in those cases where the feed is known to the adversary (or predictable upon a specific malicious action). Authentication is achieved as a valid token can only be known by the IDS or the web service, and once a token is used for a feed, it cannot be reused. As shown in Figure 7, the key to provide authentication is the pre-shared password s that is given as input to the token generator $\mathcal{G}$. During a specific time frame, the same token would be generated. The duration of the time frame can be configured as convenient through granularity of time ticks: for example, to have a time frame of half a second, it suffices to round up the time to half a second.

4. Discussion

Active buildings are the vector towards sustainable energy offerings and independence from carbon based economies. They sustain the wider grid with localised energy exchange that is key for net zero energy and net zero carbon that aims to reduce emissions by 2030 and and reach 'net zero' around 2050 as outlined by the Intergovernmental Panel on Climate Change (IPCC); as stated in IPCC's 2018 report: "Global net human-caused emissions of carbon dioxide (CO2) would need to fall by about 45 percent from 2010 levels by 2030, reaching 'net zero' around 2050.", source: https://www.ipcc.ch/2018/10/08/summary-for-policymakers-of-ipcc-special-report-on-global-warming-of-1-5c-approved-by-governments/ (accessed on 15 May 2022). This vision is shared by many countries and organisations around the globe, as it is perceived to be the logical movement on investment that will have a long term impact on the environment.

The novel energy infrastructure offered by active buildings must provide means to enact effective threat hunting [91], digital forensics and CTI collection, where managers, analysts, cybersecurity officers and network administrators engage with anomalous behaviours to thwart cyber-attacks. The integration with *smart* features in sensing or tracking embedded into physical counterparts in the infrastructure will require advanced analysis mechanisms to cope with unusual surges in demand or abnormal happenstances. In our view, CTI plays a crucial role, acting as a useful mechanism to append to other protective mechanisms in place since it provides the context for determining cyber-attacks. Ana-

lysts use threat data feeds from multiple sources to help them understand and respond to malicious incursions. CTI is still in its early stages as more mature tools and techniques are developed and adopted by organisations. It must be used in conjunction with other techniques such as attack modelling techniques (AMT) [92] where examples are attack trees or fault tree analysis, co-simulation [93], focus on advanced persistent threats or load changing attacks [11], threat modelling, or advanced statistical analysis (artificial intelligence/machine learning) [76,94], to name a few.

As mentioned, governments around the globe share a keen interest for devising incentives for both old and new buildings to increase its 'smartness' through sensing and remote management features to improve the control over a myriad of distributed assets. Building managers should consider ways of how to adapt to nZEB perspectives and enact ways to reduce carbon emissions to meet greener commitments outlined by legislation. They will push for change in the private and public sector by for instance promoting incentives for customers to purchase equipment and operate as active prosumers in the grid. So, broader prosumer engagement, dynamic energy pricing and market considerations, utilities, smart settings, and remote-control capabilities will demand thorough cybersecurity concerns across the infrastructure. In this sense, nZEB will become an overspread reality given its advantages. Beyond helping the climate and ease the strain on power grid on critical hours of the day, "behind-the-meter" generation and intelligent storage and release mechanisms will promote energy sharing in the grid network, compensating customers accordingly.

As explained here, active buildings are equipped with intelligent control and sensing technologies to support the wider grid by integrating renewable distributed energy resources to sustain power, heat, telecommunication, and transportation provision. The major assets of active buildings are renewable energy resources sustained by photovoltaic, wind turbines, heat pumps, feeding energy into batteries (static and mobile ones in electric vehicles), to name a few. All these devices are controlled by managerial systems that timely detect shifts in supply/demand to adapt power accordingly. We address here the cybersecurity components in place that are required to keep these active buildings as cyber-physical resilient as possible. Adversaries have a huge attack surface to consider when willing to compromise it where they may attack not only the physical infrastructure but also tweak the flexible controls in place. This could increase the chances of relying on the conventional power grid to meet electricity demand instead of the localised features offered by active buildings.

In the ever-changing threat landscape and the ubiquitous use of cloud-based architectures in the SG, smart buildings, and almost any CPS with IoT, a few measures should be taken into account such as:

Sharing issues	organisations have reasons for not sharing CTI, i.e., privacy, confidentiality, data related issues and protection. There are clear advantages on sharing, however, and industry and academia must discuss advantages and propose new ways of promoting it, through incentives or showing that protective measures do enhance overall cyber-defences.
Update obsolescence	as the cyber-attack unfolds and gets reported, new venues are explored by adversaries, so older reporting may become outdated.
Timeliness	offer updated indicators of compromise given emergence of new threats and highly sophisticated cyber-attacks.
Structured formats	there is a need for standardised ways of communicating threats, vulnerabilities, and attacks, also on simplified reporting when depicting and learning about malicious incursions.
Trustfulness	peers exchanging newest attacks in standardised fashion.
Model management	cybersecurity officers already have a lot of work deterring cyber-attackers, and modelling should not hinder their activities or impact their productivity. Instead, it should help them and guide better analysis and quick responses.

Cognitive load	the magnitude and breadth of data available for analysts could act as the cause for impairing better judgements, given the number of new variables to consider. CTI should offer a minimum set of data points so stakeholders are not overwhelmed by it.
Scalability	concerns on emergence of new devices in the infrastructure and reporting.

Active buildings pose special concerns to stakeholders addressing cybersecurity in power, telecommunications, and building management. For instance, active buildings could start as new buildings, where all necessary controls are already in the design. However, older building managers and customers will observe the gains of changing towards active propositions. The retrofitting task of converting buildings into active buildings will present new challenges for protecting and securing customers participating the network.

5. Conclusions

With this work, we explored the possibility of collecting, storing and sharing cyber-threat intelligence in the context of active buildings, which can be briefly described as smart buildings capable of distributing energy among connected energy peers through renewable energy resources. We base our contribution over STIX modelling, a popular ad-hoc notation for storing and sharing CTI across trustful counterparts. For this work, we have employed a tool based on STIX called cyberaCTIve [30], that offers two functionalities: a dashboard visualiser that is clear when managing complex models, as active buildings require, and a timed event list of model changes for basic forensic analysis. As active buildings are potential target of cyber-attacks that have serious repercussions to the power grid (a critical infrastructure), security officers would benefit from using IDS. These systems could potentially be automated to create feeds that incorporate detected incidents into a STIX model of an active building. cyberaCTIve does not provide facilities to actually feed the STIX model. This work provides one viable solution to the problem of timely collecting *real-time* feeds for the model by implementing an extension of cyberaCTIve that accepts (authenticated) feeds from an external system, that can well be an intrusion-detection system. Having such real-time automated feed is crucial to provide a timely response to ongoing incidents.

Future Work and Outlook

Modelling efforts cannot hinder the reasoning or the ability of addressing cyber-attacks quickly, just to strictly follow the standard. Analysts should be able to describe odd circumstances with as little information as they have at that moment, and only care about modelling details and its constraints afterwards. In early indications of potential malicious incursions, very little is known about the attacks. As they unfold and systems gather and compile more evidence, analysts may append and curate preexisting models with this data combined with exterior data sources for full contexts.

We developed here a STIX model for active buildings, where users may interact with the parameters required by the set of STIX Domain Objects (SDO), STIX Relationship Objects (SRO), or STIX Cyber-observable Objects (SCO). The idea was to enrich active buildings' analysis and allow users to perceive the expected requirements for devising more shareable models to broader audiences. Under these settings, timeliness plays a crucial factor in cyber-attacks because one should be able to share possible exposure and vulnerabilities with trusted peers as soon as possible.

We envision adding more features in future versions of the tool such as integrating cyberaCTIve with the ATT&CK framework's TTPs and Matrices (provide a static instance of some STIX elements inspired by it, such as existing Threat Actors or mitigations). We could also accommodate features for analysts such as time-based analysis and to devise ways of tracking the 'life-time' of families of cyber-attacks (those focusing on specific assets) and also improving the 'Model visualizer' feature. For instance, we could allow the selection of groups of assets (e.g., all renewable energy resources, or all information systems) and then

creating empty objects that will be filled out in another moment. Because we expect analysts to deploy our tool in their workspaces, we will need to review our features proposition with input from power-based domain experts. In this evaluation they may specify new streams to look at that are considered essential when inspecting cyber-attacks. Also, we shall conduct usability testing subjecting users to the tool and inspecting learning curves, whether expectations were met, and incorporating suggestions to improve the tool.

As new implementation to add to cyberaCTIve, we will consider: (i) increase basic security by logging actions and movements of users, versioning models and objects, showing users older versions visually (e.g., font colour fading); (ii) improve the 'timeline' feature and implement the 'sharing' CTI feature using actual TAXII servers; (iii) ability to 'redact' models and objects before sharing, avoiding unintended disclosure of sensitive data or concerns due to confidentiality issues; iv) implement remaining STIX parameters not tackled by the current tool version, e.g., `cyber-kill-chain`, `marking definitions`, and `dictionary`; (v) force users to provide well-formed input for specific types in accordance with the STIX specification when creating URLs, e-mail addresses, informing (existing/valid) cities or countries (for instance); (vi) reuse objects from other previously created models; (vii) allow analysts to operate in different capacities (consulting, analyst, or administrator), across organisations, where they could share infrastructure details and locations; and (viii) exporting and importing models to and from the tool.

There are advantages for implementing systems and employing JSON files to map all objects, types, and vocabularies within the same solution. Now, any changes in the STIX specification will translate to changes in the JSON files and the system will retain its basic functionality. The tool we have chosen to model active buildings (cyberaCTIve) offers interesting features for cybersecurity analysis when modelling any malicious incursions in networks. It makes easier to understand required/optional parameters to enrich models and analysis, besides the ability of sharing models. The tool has the potential of easing analysis and capture relevant cybersecurity incident data combined with other CTI data sources when documenting most likely attacks in CI.

Author Contributions: Conceptualization, R.M.C., R.M. and C.M.; methodology, R.M.C., R.M. and C.M.; software, R.M.C. and R.M.; validation, R.M.C., R.M. and C.M.; formal analysis, R.M.C., R.M. and C.M.; investigation, R.M.C., R.M. and C.M.; resources, R.M.C., R.M. and C.M.; data curation, R.M.C., R.M. and C.M.; writing—original draft preparation, R.M.C.; writing—review and editing, R.M.C., R.M. and C.M.; visualization, R.M.C. and R.M.; supervision, C.M.; project administration, C.M.; funding acquisition, C.M. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the Industrial Strategy Challenge Fund and EPSRC, EP/V012053/1, Active Building Centre Research Programme (ABC RP).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

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

Appendix A. Comparison to the Official STIX Visualiser

We briefly demonstrate next the fact that some complex graphs depicting intricate modelling choices are not well supported by the official STIX visualiser. If the graph shown in Figure A1 is augmented with a single incursion or small alteration, it would require even more time to be processed by a security officer. This would clearly hinder timely interventions to real-time incursions. This is one of the reasons why we opted to use the tool `cyberaCTIve` [30].

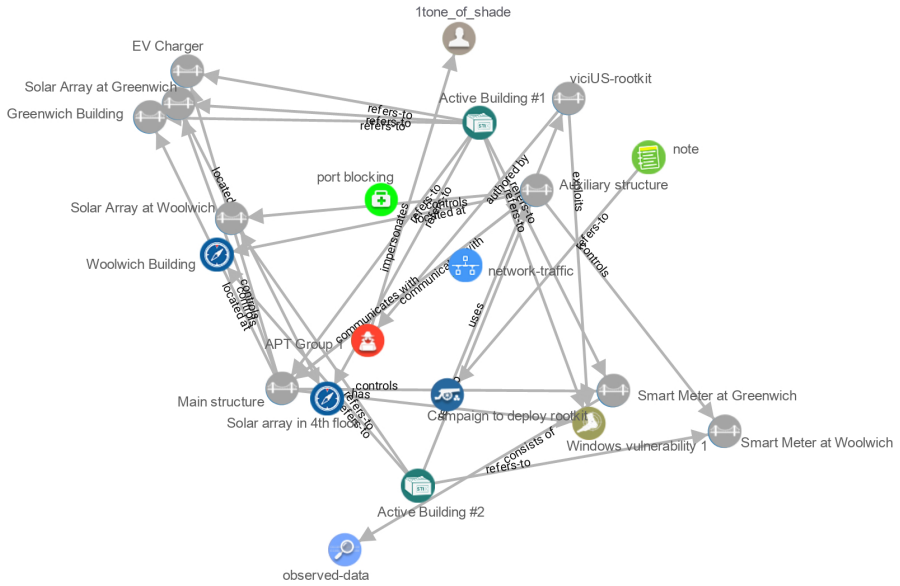

Figure A1. Base STIX model for active buildings that is too complex for the official STIX visualiser.

References

1. Rajkumar, R.; Lee, I.; Sha, L.; Stankovic, J. Cyber-physical systems: The next computing revolution. In Proceedings of the Design Automation Conference, Anaheim, CA, USA, 3–18 June 2010; pp. 731–736.
2. Shi, J.; Wan, J.; Yan, H.; Suo, H. A survey of cyber-physical systems. In Proceedings of the 2011 International Conference on Wireless Communications and Signal Processing (WCSP), Nanjing, China, 9–11 November 2011; pp. 1–6.
3. Khaitan, S.K.; McCalley, J.D. Cyber physical system approach for design of power grids: A survey. In Proceedings of the 2013 IEEE Power & Energy Society General Meeting, Vancouver, BC, Canada, 21–25 July 2013; pp. 1–5.
4. Roccotelli, M.; Mangini, A.M. Advances on Smart Cities and Smart Buildings. *Appl. Sci.* **2022**, *12*, 631. [CrossRef]
5. He, H.; Yan, J. Cyber-physical attacks and defences in the smart grid: A survey. *IET Cyber-Phys. Syst. Theory Appl.* **2016**, *1*, 13–27. [CrossRef]
6. Kimani, K.; Oduol, V.; Langat, K. Cyber security challenges for IoT-based smart grid networks. *Int. J. Crit. Infrastruct. Prot.* **2019**, *25*, 36–49. [CrossRef]
7. Gunduz, M.Z.; Das, R. Cyber-security on smart grid: Threats and potential solutions. *Comput. Netw.* **2020**, *169*, 107094. [CrossRef]
8. Kolokotronis, N.; Shiaeles, S. *Cyber-Security Threats, Actors, and Dynamic Mitigation*; CRC Press: Boca Raton, FL, USA, 2021.
9. Sridhar, S.; Hahn, A.; Govindarasu, M. Cyber–physical system security for the electric power grid. *Proc. IEEE* **2011**, *100*, 210–224. [CrossRef]
10. Dabrowski, A.; Ullrich, J.; Weippl, E.R. Grid shock: Coordinated load-changing attacks on power grids: The non-smart power grid is vulnerable to cyber attacks as well. In Proceedings of the 33rd Annual Computer Security Applications Conference, Orlando, FL, USA, 4–8 December 2017; pp. 303–314.
11. Arnaboldi, L.; Czekster, R.M.; Morisset, C.; Metere, R. Modelling Load-Changing Attacks in Cyber-Physical Systems. *Electron. Notes Theor. Comput. Sci.* **2020**, *353C*, 39–60. [CrossRef]
12. Soltan, S.; Mittal, P.; Poor, H.V. BlackIoT: IoT botnet of high wattage devices can disrupt the power grid. In Proceedings of the 27th {USENIX} Security Symposium ({USENIX} Security 18), Baltimore, MD, USA, 15–17 August 2018; pp. 15–32.
13. Alotaibi, I.; Abido, M.A.; Khalid, M.; Savkin, A.V. A comprehensive review of recent advances in smart grids: A sustainable future with renewable energy resources. *Energies* **2020**, *13*, 6269. [CrossRef]
14. Ingram, M.; Martin, M. *Guide to Cybersecurity, Resilience, and Reliability for Small and Under-Resourced Utilities*; Technical Report; National Renewable Energy Lab.: Golden, CO, USA, 2017.
15. Oskouei, M.Z.; Mohammadi-Ivatloo, B.; Abapour, M.; Ahmadian, A.; Piran, M.J. A novel economic structure to improve the energy label in smart residential buildings under energy efficiency programs. *J. Clean. Prod.* **2020**, *260*, 121059. [CrossRef]
16. Zeynali, S.; Rostami, N.; Ahmadian, A.; Elkamel, A. Two-stage stochastic home energy management strategy considering electric vehicle and battery energy storage system: An ANN-based scenario generation methodology. *Sustain. Energy Technol. Assess.* **2020**, *39*, 100722. [CrossRef]
17. Zeynali, S.; Rostami, N.; Ahmadian, A.; Elkamel, A. Robust multi-objective thermal and electrical energy hub management integrating hybrid battery-compressed air energy storage systems and plug-in-electric-vehicle-based demand response. *J. Energy Storage* **2021**, *35*, 102265. [CrossRef]
18. Jahangir, H.; Tayarani, H.; Gougheri, S.S.; Golkar, M.A.; Ahmadian, A.; Elkamel, A. Deep learning-based forecasting approach in smart grids with microclustering and bidirectional LSTM network. *IEEE Trans. Ind. Electron.* **2020**, *68*, 8298–8309. [CrossRef]

19. Tounsi, W. What is Cyber Threat Intelligence and how is it evolving? In *Cyber-Vigilance and Digital Trust: Cyber Security in the Era of Cloud Computing and IoT*; Wiley Online Library: Hoboken, NJ, USA, 2019; pp. 1–49.
20. Olowu, T.O.; Sundararajan, A.; Moghaddami, M.; Sarwat, A.I. Future challenges and mitigation methods for high photovoltaic penetration: A survey. *Energies* **2018**, *11*, 1782. [CrossRef]
21. Metere, R.; Neaimeh, M.; Morisset, C.; Maple, C.; Bellekens, X.; Czekster, R.M. Securing the Electric Vehicle Charging Infrastructure. *arXiv* **2021**, arXiv:2105.02905.
22. Greenwood, D.; Lim, K.Y.; Patsios, C.; Lyons, P.; Lim, Y.S.; Taylor, P. Frequency response services designed for energy storage. *Appl. Energy* **2017**, *203*, 115–127. [CrossRef]
23. Strbac, G.; Woolf, M.; Pudjianto, D.; Zhang, X.; Walker, S.; Vahidinasab, V. *The Role of Active Buildings in the Transition to a Net Zero Energy System*; Active Building Centre Research Programme: Swansea, UK, 2020.
24. Coma, E.; Jones, P. 'Buildings as Power Stations': An energy simulation tool for housing. *Procedia Eng.* **2015**, *118*, 58–71. [CrossRef]
25. Canaan, B.; Colicchio, B.; Ould Abdeslam, D. Microgrid cyber-security: Review and challenges toward resilience. *Appl. Sci.* **2020**, *10*, 5649. [CrossRef]
26. Nejabatkhah, F.; Li, Y.W.; Liang, H.; Reza Ahrabi, R. Cyber-security of smart microgrids: A survey. *Energies* **2021**, *14*, 27. [CrossRef]
27. Fosas, D.; Nikolaidou, E.; Roberts, M.; Allen, S.; Walker, I.; Coley, D. Towards active buildings: Rating grid-servicing buildings. *Build. Serv. Eng. Res. Technol.* **2021**, *42*, 129–155. [CrossRef]
28. Dasgupta, R.; Sakzad, A.; Rudolph, C. Cyber attacks in transactive energy market-based microgrid systems. *Energies* **2021**, *14*, 1137. [CrossRef]
29. Barnum, S. Standardizing cyber threat intelligence information with the Structured Threat Information eXpression (STIX). *Mitre Corp.* **2012**, *11*, 1–22.
30. Czekster, R.M.; Metere, R.; Morisset, C. cyberaCTIve: A STIX-based Tool for Cyber Threat Intelligence in Complex Models. *arXiv* **2022**, arXiv:2204.03676.
31. Ackoff, R.L. From data to wisdom. *J. Appl. Syst. Anal.* **1989**, *16*, 3–9.
32. Tounsi, W.; Rais, H. A survey on technical threat intelligence in the age of sophisticated cyber attacks. *Comput. Secur.* **2018**, *72*, 212–233. [CrossRef]
33. Brown, R.; Lee, R.M. *The Evolution of Cyber Threat Intelligence (CTI): 2019 SANS CTI Survey*; SANS Institute: Boston, MA, USA, 2019. Available online: https://www.sans.org/white-papers/38790/ (accessed on 15 May 2022).
34. Pokorny, Z. *The Threat Intelligence Handbook: Moving toward a Security Intelligence Program*; CyberEdge Group: Annapolis, MD, USA, 2019.
35. Schaberreiter, T.; Kupfersberger, V.; Rantos, K.; Spyros, A.; Papanikolaou, A.; Ilioudis, C.; Quirchmayr, G. A quantitative evaluation of trust in the quality of cyber threat intelligence sources. In Proceedings of the 14th International Conference on Availability, Reliability and Security, Canterbury, UK, 26–29 August 2019; pp. 1–10.
36. Griffioen, H.; Booij, T.; Doerr, C. Quality Evaluation of Cyber Threat Intelligence Feeds. In *International Conference on Applied Cryptography and Network Security*; Springer: Berlin/Heidelberg, Germany, 2020; pp. 277–296.
37. Tundis, A.; Ruppert, S.; Mühlhäuser, M. On the Automated Assessment of Open-Source Cyber Threat Intelligence Sources. In *International Conference on Computational Science*; Springer: Berlin/Heidelberg, Germany, 2020; pp. 453–467.
38. Huang, Y.T.; Lin, C.Y.; Guo, Y.R.; Lo, K.C.; Sun, Y.S.; Chen, M.C. Open Source Intelligence for Malicious Behavior Discovery and Interpretation. *IEEE Trans. Dependable Secur. Comput.* **2021**, *19*, 776–789. [CrossRef]
39. Ramsdale, A.; Shiaeles, S.; Kolokotronis, N. A comparative analysis of cyber-threat intelligence sources, formats and languages. *Electronics* **2020**, *9*, 824. [CrossRef]
40. Connolly, J.; Davidson, M.; Schmidt, C. *The Trusted Automated eXchange of Indicator Information (TAXII)*; The MITRE Corporation: Bedford, MA, USA, 2014; pp. 1–20.
41. Barnum, S.; Martin, R.; Worrell, B.; Kirillov, I. *The Cybox Language Specification*; The MITRE Corporation: Bedford, MA, USA, 2012.
42. Casey, E.; Back, G.; Barnum, S. Leveraging CybOX^{TM} to standardize representation and exchange of digital forensic information. *Digit. Investig.* **2015**, *12*, S102–S110. [CrossRef]
43. Bankovskis, A. *One Million Homes Constructed as "Buildings as Power Stations"—Report of Indicative Benefits*; SPECIFIC Online Report; SPECIFIC—UK Innovation and Knowledge Centre (IKC): Swansea, UK, 2017. Available online: https://www.specific.eu.com/ (accessed on 15 May 2022).
44. Clarke, J.; Jones, P.; Littlewood, J.; Worsley, D. Active buildings in practice. In *Sustainability in Energy and Buildings*; Springer: Berlin/Heidelberg, Germany, 2020; pp. 555–564.
45. Clarke, J. Designing active buildings. In *Emerging Research in Sustainable Energy and Buildings for a Low-Carbon Future*; Springer: Berlin/Heidelberg, Germany, 2021; pp. 11–24.
46. Kurnitski, J.; Allard, F.; Braham, D.; Goeders, G.; Heiselberg, P.; Jagemar, L.; Kosonen, R.; Lebrun, J.; Mazzarella, L.; Railio, J.; et al. How to define nearly net zero energy buildings nZEB. *Rehva J.* **2011**, *48*, 6–12.
47. Attia, S. *Net Zero Energy Buildings (NZEB): Concepts, Frameworks and Roadmap for Project Analysis and Implementation*; Butterworth-Heinemann: Oxford, UK, 2018.
48. D'Agostino, D.; Mazzarella, L. What is a Nearly zero energy building? Overview, implementation and comparison of definitions. *J. Build. Eng.* **2019**, *21*, 200–212. [CrossRef]

49. Series, I. *Microgrids and Active Distribution Networks*; The Institution of Engineering and Technology (IET): London, UK, 2009.
50. Skopik, F.; Friedberg, I.; Fiedler, R. Dealing with advanced persistent threats in smart grid ICT networks. In *Innovative Smart Grid Technologies (ISGT)*; IEEE Power & Energy Society: New York, NY, USA, 2014; pp. 1–5.
51. Friedberg, I.; Skopik, F.; Settanni, G.; Fiedler, R. Combating advanced persistent threats: From network event correlation to incident detection. *Comput. Secur.* **2015**, *48*, 35–57. [CrossRef]
52. Yankson, S.; Ghamkhari, M. Transactive Energy to Thwart Load Altering Attacks on Power Distribution Systems. *Future Internet* **2020**, *12*, 4. [CrossRef]
53. Eltawil, M.A.; Zhao, Z. Grid-connected photovoltaic power systems: Technical and potential problems—A review. *Renew. Sustain. Energy Rev.* **2010**, *14*, 112–129. [CrossRef]
54. Al-Shetwi, A.Q.; Sujod, M.Z. Grid-connected photovoltaic power plants: A review of the recent integration requirements in modern grid codes. *Int. J. Energy Res.* **2018**, *42*, 1849–1865. [CrossRef]
55. Harrou, F.; Taghezouit, B.; Sun, Y. Robust and flexible strategy for fault detection in grid-connected photovoltaic systems. *Energy Convers. Manag.* **2019**, *180*, 1153–1166. [CrossRef]
56. Livera, A.; Theristis, M.; Makrides, G.; Georghiou, G.E. Recent advances in failure diagnosis techniques based on performance data analysis for grid-connected photovoltaic systems. *Renew. Energy* **2019**, *133*, 126–143. [CrossRef]
57. Harrou, F.; Dairi, A.; Taghezouit, B.; Sun, Y. An unsupervised monitoring procedure for detecting anomalies in photovoltaic systems using a one-class Support Vector Machine. *Sol. Energy* **2019**, *179*, 48–58. [CrossRef]
58. Giraldo, J.; Sarkar, E.; Cardenas, A.A.; Maniatakos, M.; Kantarcioglu, M. Security and privacy in cyber-physical systems: A survey of surveys. *IEEE Des. Test* **2017**, *34*, 7–17. [CrossRef]
59. Beheshtaein, S.; Cuzner, R.; Savaghebi, M.; Guerrero, J.M. Review on microgrids protection. *IET Gener. Transm. Distrib.* **2019**, *13*, 743–759. [CrossRef]
60. Beheshtaein, S.; Cuzner, R.M.; Forouzesh, M.; Savaghebi, M.; Guerrero, J.M. DC microgrid protection: A comprehensive review. *IEEE J. Emerg. Sel. Top. Power Electron.* **2019**. [CrossRef]
61. Al-Turjman, F.; Abujubbeh, M. IoT-enabled smart grid via SM: An overview. *Future Gener. Comput. Syst.* **2019**, *96*, 579–590. [CrossRef]
62. Zografopoulos, I.; Ospina, J.; Liu, X.; Konstantinou, C. Cyber-physical energy systems security: Threat modeling, risk assessment, resources, metrics, and case studies. *IEEE Access* **2021**, *9*, 29775–29818. [CrossRef]
63. Kavallieros, D.; Germanos, G.; Kolokotronis, N. Profiles of Cyber-Attackers and Attacks. In*Cyber-Security Threats, Actors, and Dynamic Mitigation*; CRC Press: Boca Raton, FL, USA, 2021; pp. 1–26.
64. Czekster, R.M.; Morisset, C.; van Moorsel, A.; Mace, J.C.; Bassage, W.A.; Clark, J.A. Cybersecurity Roadmap for Active Buildings. In *Active Building Energy Systems: Operation and Control*; Vahidinasab, V., Mohammadi-Ivatloo, B., Eds.; Springer International Publishing: Cham, Switzerland, 2022; pp. 219–249. [CrossRef]
65. Kshetri, N.; Voas, J. Hacking power grids: A current problem. *Computer* **2017**, *50*, 91–95. [CrossRef]
66. Falliere, N.; Murchu, L.O.; Chien, E. W32. stuxnet dossier. *White Pap. Symantec Corp. Secur. Response* **2011**, *5*, 29.
67. Langner, R. Stuxnet: Dissecting a cyberwarfare weapon. *IEEE Secur. Priv.* **2011**, *9*, 49–51. [CrossRef]
68. Chen, T.M.; Abu-Nimeh, S. Lessons from stuxnet. *Computer* **2011**, *44*, 91–93. [CrossRef]
69. Karnouskos, S. Stuxnet worm impact on industrial cyber-physical system security. In Proceedings of the IECON 2011-37th Annual Conference of the IEEE Industrial Electronics Society, Melbourne, VIC, Australia, 7–10 November 2011; pp. 4490–4494.
70. Lindsay, J.R. Stuxnet and the limits of cyber warfare. *Secur. Stud.* **2013**, *22*, 365–404. [CrossRef]
71. Lipovsky, R. Back in BlackEnergy: 2014 Targeted Attacks in Ukraine and Poland. *Retrieved* **2014**, *2*, 2016.
72. Cherepanov, A.; Lipovsky, R. BlackEnergy: What we really know about the notorious cyber attacks. In Proceedings of the Virus Bulletin Conference, Denver, CO, USA, 5–7 October 2016.
73. Cherepanov, A.; Lipovsky, R. Industroyer: Biggest threat to industrial control systems since Stuxnet. *Welivesecurity ESET* **2017**, *12*.
74. Liang, G.; Weller, S.R.; Zhao, J.; Luo, F.; Dong, Z.Y. The 2015 ukraine blackout: Implications for false data injection attacks. *IEEE Trans. Power Syst.* **2016**, *32*, 3317–3318. [CrossRef]
75. Response, S.I. Dragonfly: Cyberespionage attacks against energy suppliers. *Rapp. Tecn* **2014**, *7*.
76. Chen, Q.; Bridges, R.A. Automated behavioral analysis of malware: A case study of wannacry ransomware. In Proceedings of the 2017 16th IEEE International Conference on Machine Learning and Applications (ICMLA), Cancun, Mexico, 18–21 December 2017; pp. 454–460.
77. Hsiao, S.C.; Kao, D.Y. The static analysis of WannaCry ransomware. In Proceedings of the 2018 20th International Conference on Advanced Communication Technology (ICACT), Chuncheon, Korea, 11–14 February 2018; pp. 153–158.
78. Lee, R. *TRISIS Malware: Analysis of Safety System Targeted Malware*; Dragos Inc.: Hanover, MD, USA, 2017.
79. Geiger, M.; Bauer, J.; Masuch, M.; Franke, J. An Analysis of Black Energy 3, Crashoverride, and Trisis, Three Malware Approaches Targeting Operational Technology Systems. In Proceedings of the 2020 25th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA), Vienna, Austria, 8–11 September 2020; Volume 1, pp. 1537–1543.
80. Hemsley, K.E.; Fisher, E. *History of Industrial Control System Cyber Incidents*; Technical Report; Idaho National Lab.(INL): Idaho Falls, ID, USA, 2018.
81. Strom, B.E.; Applebaum, A.; Miller, D.P.; Nickels, K.C.; Pennington, A.G.; Thomas, C.B. *MITRE ATT&CK®: Design and Philosophy*; MITRE Technical Report; The MITRE Corporation: Bedford, MA, USA, 2018.

82. Alexander, O.; Belisle, M.; Steele, J. *MITRE ATT&CK for Industrial Control Systems: Design and Philosophy*; The MITRE Corporation: Bedford, MA, USA, 2020.
83. Roberts, A. *Cyber Threat Intelligence: The No-Nonsense Guide for CISOs and Security Managers*; Apress: Berkeley, CA, USA, 2021.
84. Hutchins, E.M.; Cloppert, M.J.; Amin, R.M. Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. *Lead. Issues Inf. Warf. Secur. Res.* **2011**, *1*, 80.
85. Lockheed Martin Corporation. *Seven Ways to Apply the Cyber Kill Chain with a Threat Intelligence Platform*; Lockheed Martin Corporation: North Bethesda, MD, USA, 2015.
86. Kwon, R.; Ashley, T.; Castleberry, J.; Mckenzie, P.; Gourisetti, S.N.G. Cyber Threat Dictionary Using MITRE ATT&CK Matrix and NIST Cybersecurity Framework Mapping. In Proceedings of the 2020 Resilience Week (RWS), Salt Lake City, UT, USA, 19–23 October 2020; pp. 106–112.
87. Metere, R.; Arnaboldi, L. Automating Cryptographic Protocol Language Generation from Structured Specifications. *arXiv* **2021**, arxiv:2105.09150.
88. Mell, P.; Scarfone, K.; Romanosky, S. Common vulnerability scoring system. *IEEE Secur. Priv.* **2006**, *4*, 85–89. [CrossRef]
89. Fielding, R.T. *Architectural Styles and the Design of Network-Based Software Architectures*; University of California: Irvine, CA, USA, 2000.
90. Tixteco, L.P.; Aguirre, E.; Hdez, A.F.M. DoS attacks flood techniques. *Int. J. Comb. Optim. Probl. Inform.* **2012**, *3*, 3.
91. Gao, P.; Shao, F.; Liu, X.; Xiao, X.; Qin, Z.; Xu, F.; Mittal, P.; Kulkarni, S.R.; Song, D. Enabling efficient cyber threat hunting with cyber threat intelligence. In Proceedings of the 2021 IEEE 37th International Conference on Data Engineering (ICDE), Chania, Greece, 19–22 April 2021; pp. 193–204.
92. Lallie, H.S.; Debattista, K.; Bal, J. A review of attack graph and attack tree visual syntax in cyber security. *Comput. Sci. Rev.* **2020**, *35*, 100219. [CrossRef]
93. Czekster, R.M.; Morisset, C.; Clark, J.A.; Soudjani, S.; Patsios, C.; Davison, P. Systematic review of features for co-simulating security incidents in Cyber-Physical Systems. *Secur. Priv.* **2021**, *4*, e150. [CrossRef]
94. Truong, T.C.; Zelinka, I.; Plucar, J.; Čandík, M.; Šulc, V. Artificial intelligence and cybersecurity: Past, presence, and future. In *Artificial Intelligence and Evolutionary Computations in Engineering Systems*; Springer: Berlin/Heidelberg, Germany, 2020; pp. 351–363.