Vulnerability Exposure Driven Intelligence in Smart, Circular Cities

PAUL-DAVID JARVIS and AMALIA DAMIANOU, BU-CERT, Bournemouth University, UK
COSMIN CIOBANU, EU Agency for Cybersecurity (ENISA), Greece
VASILIS KATOS, BU-CERT, Bournemouth University, UK

In this article, we study the vulnerability management dimension in smart city initiatives. As many cities across the globe invest a considerable amount of effort, resources and budget to modernise their infrastructure by deploying a series of technologies such as 5G, Software Defined Networks, and IoT, we conduct an empirical analysis of their current exposure to existing vulnerabilities. We use an updated vulnerability dataset that is further enriched by quantitative research data from independent studies evaluating the maturity and accomplishments of cities in their journey to become smart. We particularly focus on cities that aspire to implement a (data-driven) Circular Economy agenda that we consider to potentially yield the highest risk from a vulnerabilities exposure perspective. Findings show that although a smarter city is attributed with a higher vulnerability exposure, investments on technology and human capital moderate this exposure in a way that it can be reduced.

CCS Concepts: • **Security and privacy** → *Systems security*; *Vulnerability management;*

Additional Key Words and Phrases: Data-driven Circular Economy, smart cities, maturity model, vulnerability contextualisation

ACM Reference format:
Paul-David Jarvis, Amalia Damianou, Cosmin Ciobanu, and Vasilis Katos. 2022. Vulnerability Exposure Driven Intelligence in Smart, Circular Cities. *Digit. Threat.: Res. Pract.* 3, 4, Article 40 (December 2022), 18 pages.
https://doi.org/10.1145/3487059

1 INTRODUCTION AND MOTIVATION

With the ongoing trend of urbanisation, it is predicted that by 2050, 68% of the world population will live in cities [41]. Such trend will impose considerable strains on the governance on a local authority level and is already challenging the way cities manage their resources.

To address the challenges arising from the accelerating urbanisation and depletion of finite resources, cities are moving toward the adoption of a range of approaches across a number of dimensions, one of which is the technological. More specifically, the technological dimension refers to the use IT and computer network enablers that can support the delivery of sustainability focused business models. The path and journey for a city in becoming *smart* may differ between the cities that may have different problems to solve as well as different starting

This work has received funding from the European Union's Horizon 2020 research and innovation program under the grant agreement no 830943 (ECHO) and the H2020-MSCA-RISE-2017 project, under the grant agreement no 778228 (IDEAL-CITIES).
Authors' addresses: P.-D. Jarvis, A. Damianou, and V. Katos, BU-CERT, Bournemouth University, Fern Barrow, Poole, UK, BH12 5BB; emails: {s5115232, adamianou, vkatos}@bournemouth.ac.uk; C. Ciobanu, EU Agency for Cybersecurity (ENISA), Vasilissis Sofias Str 1, Athens, Greece, 151 24; email: Cosmin.Ciobanu@enisa.europa.eu.

2576-5337/2022/12-ART40
https://doi.org/10.1145/3487059

points. London, for example, had challenges in the transportation sector, whereas Barcelona's main driver was to tackle pollution. In all cases, however, the end state is envisaged to use enabling technologies from the same broad areas: 5G and Software Defined Networks, IoT, and Industrial Systems in general, as well as the adoption of cloud and edge computing paradigms. These technologies would support decision making for planning, managing resources and responding to incidents affecting supply and demand in real time.

At the same time, as the business models promoting sustainability emerge and mature, it became apparent that data-driven Circular Economy is an emerging concept and approach cities should strive to adopt. This in turn led to the realisation that a city becoming *smart* is an intermediary stage rather than an end goal. However, achieving a state where a city is sustainable—or, equivalently, *circular*—carries significant risks if an appropriate risk management plan is not in place. In contrast to traditional cyber systems, smart cities are a melting pot of cyber-physical and socio-technical systems, where risk transfer occurs between the cyber and physical plane, through two main conduits. From a cyber-physical system perspective, the transfer of risk occurs through the IoT nodes (sensors and actuators), whereas from a socio-technical view the risk is transferred from the human nodes. This inevitably leads to a wide attack surface with an increased scope of the impact affecting not only confidentiality, integrity and availability, but also privacy and safety.

From a cybersecurity view, attacks on either direct smart city services or its citizens undermines the users' incentive to adopt and use these services [1]. As smart cities encompass a wide range of technological domains and themes (see, for example, Reference [20] for a comprehensive list of research themes), we argue that vulnerabilities constitute a horizontal theme cutting across most of the other domains. Moreover, a vulnerability is a key component of any risk-based approach as well as for any attack vector when there is a corresponding exploit available. Vulnerability management is therefore critical for any local government and authority who engage in smart city initiatives and the scope should extend beyond the core smart city services and infrastructure, but reach to the end devices; for example, as smart urban services highly depend on mobile communications, there are cases where local authorities are exploring ways in becoming local Mobile Network Operators, primarily due to the 5G rollout. A safe and secure city operating a 5G network would need to consider end to end security along with the QoS aspects and the authority's lack of ability to frame cybersecurity can lead to the failure of developing suitable security policies [14].

Our contribution. To our knowledge, the study of vulnerabilities in a smart cities context is primarily theoretical [24, 27] or has not been extensively explored from an empirical evaluation perspective. In fact, most of the empirical studies on cybersecurity for cities explore practices, capabilities, policies and government involvement [34]. In this article, we attempt to create a baseline to allow the stakeholders of a city to compare their standing and exposure against cities with *similar* profiles and characteristics. This is performed by consolidating and correlating (mostly orthogonal) data from two types of sources: independent studies on the level of achievement and maturity of a city becoming smart, and actual data from available online, potentially vulnerable devices. With regards to the former, we adopted the most to date and accepted surveys and metrics assessing smart cities on a number of dimensions. With regards to the vulnerabilities and exposures we employed and expanded the ENISA 2018-2019 vulnerabilities dataset by extending the date rage of collection of vulnerabilities, including city exposure information. Through a grounded theory approach we correlate such information with the other established third party research using city metrics. We focus on vulnerabilities that correspond to actual devices as captured and indexed by the **Sentient Hyper-Optimised Data Access Network (Shodan)**, an online database that is periodically updated with device exposure information. This approach is twofold; first, it would allow a local authority (who may be also running a smart city data centre) to gather and generate actionable threat intelligence at an operational level that can also help them to conduct a cyber-physical risk assessment. Second, it will help the city to understand the local and wider threat landscape and prioritise its synergies and collaboration efforts with cities that have a similar exposure profile and alike constituencies. By creating the aforementioned baseline, the respective decision maker would be in a position to develop a contextualised narrative by enriching their

position with specific geo-political and social context and therefore make informed decisions on their vulnerability management processes and cybersecurity investment in general. For example, we argue that more *mature* smart cities—that is, in terms of achievement of a smart city agenda—would need to maintain and strictly adhere to vulnerability management plans, as in the opposite case they are open to an assortment of threats, including hybrid ones, that can directly affect the safety and well-being of their citizens.

The rest of this article is structured as follows. In Section 2, we introduce the concept of data-driven Circular Economy for the benefit of the reader who is not familiar with the concept. We particularly focus on data-driven circular cities, as these subscribe to the interconnected networks and cyber-physical systems paradigms, thus elevating significantly the impact of a vulnerability. Section 3 describes and elaborates on the smart/circular city maturity model, to illustrate the need for vulnerability contextualisation. Section 4 describes the proposed approach by detailing the methodology and dataset used, the analysis and discussion on the findings. Section 5 summarizes the main findings and outlines areas for future research.

2 FROM TRADITIONAL CITIES TO SMART CITIES, TO CIRCULAR CITIES

The transition from a traditional to a smart city is not a new concept; however, it has come to the spotlight during the recent years. Furthermore, many ICT enablers have reached a maturity level that allow the realisation of the smart city concept. The **International Telecommunication Union (ITU)** alone in a recent survey captured over 100 definitions for the term [42].

The term *smart city* is not the only one to describe a technologically evolved environment. There are many other terms, like wired city, connected city, intelligent city, digital city, and so forth [31]. Alongside these definitions, a stream of research focuses on defining not only the dimensions that would characterise a city smart, but also to measure the level of achievement across these dimensions, that is captured and described under a maturity model.

From a systems perspective, a city can be viewed as a complex system that is continuously evolving, with all of its components being organised and interconnected to perform particular functions or purposes. A smart city can be viewed as a system of systems [23], a **Socio Technical System (STS)** [6] and a **Cyber Physical System (CPS)** [36]. An STS comprises of the users and/or human assets, who interact with the city infrastructures in meaningful ways, to receive a service or to contribute to a city's function. User/human interactions are related to the exchanging of information between both the physical and the cyber plane. Furthermore, users interact with each other.

However, a Cyber Physical System consists of computation and control components on the one hand and physical devices and intelligent assets on the other. The intelligent assets can have varying levels of "importance" in the system, assuming different roles and offering services of different levels of criticality. CPS are mostly implemented for critical infrastructures and industrial control systems; however, during the past few years they have been adopted to many other domains including smart cities. A citywide deployment of a CPS must be conducted in a way to ensure sustainability, safety, and security.

A particular milestone for massive CPS deployments is the establishment of the IoT paradigm rooted in 2008, which marked the introduction of technologies like embedded systems and wireless networks. In essence, smart devices, sensors, and actuators are employed to produce, collect and exchange information using wireless networks; at the same time machine learning approaches were introduced and employed [2] to create added value out of the produced big data.

In general, smart city is a concept that primarily refers to the adoption of technological enablers to enhance the quality of services that the city provides, with the overall aim to improve the citizens' quality of life. According to Reference [31], the majority of smart cities projects include four main attributes that are common, namely sustainability, quality of life, smartness, and urbanisation [38].

It is argued that the adoption of technological enablers in a citywide scale is a key direction for achieving sustainability. Some of the major challenges that come along with urbanisation include the waste management,

air and noise pollution, adequacy of resources, traffic issues, citizens health and mental issues, transportation, and so on. The use of technological approaches has changed the conventional concept of a city. Moreover, various studies [19, 38] that have as main topic the correlation between urbanisation and smart cities, came to a conclusion that the new opportunities through the usage ICT influence positively the urban wealth.

2.1 Data-driven Circular Economy

As discussed, a smart city should be the epitome of sustainability, since any deviation from this would entertain scenarios of dystopian futures. Since sustainability is one of the main business and societal drivers for transforming a city into a smart one, there is a requirement to develop a suitable agenda and accompanied business models. The **Circular Economy (CE)** paradigm is viewed as the sustainability approach, whereas ICT may provide the means.

The term *Circular Economy* is used to describe the economic model where everything has value and nothing is wasted. This means that assets like materials, devices, services, and generally resources are not disposed after the first usage, but they are used again and again for a variety of purposes. The main goal of Circular Economy is to maintain their utility without producing new assets or wasting them before the end of their lifecycle [12]. The main idea behind Circular Economy is to design products in a smart way so as to be used during their whole lifecycle, be re-used and re-paired to extend this lifecycle and re-manufactured to create new products [12]. Information and Communication Technologies can facilitate Circular Economy as it can provide useful information on assets, their location, the condition, and the performance of assets, in real-time and over time.

According to the Ellen MacArthur Foundation, "A Circular Economy is one that is restorative and regenerative by design, and that aims to keep products, components and materials at their highest utility and value at all time. It distinguished between technical and biological cycles as an attempt to minimise leakage and wastage" [32]. Adopting nature inspired "techniques" on waste recycling/upcycling and reuse, Circular Economy is built on the premise that every material can be reused in this way to be functional again as it will have the opportunity to be regenerated and restored. Some of the main benefits of Circular Economy involve substantial net material savings, reduced exposure to price volatility, increased economic development, increased innovation and job creation potential and increased resilience in living systems and in the economy [32]. To achieve the aforementioned highest utility and value, one would need to enable and maintain information flows, so that timely and fine-grained decision making can take place. This in turn leads to accepting that a CE model would need to be data driven to achieve its goals:

Definition 1. Smart, or data-driven Circular Economy is the utilization of reactive, adaptive, autonomous or collaborative objects and systems for economic and environmental value creation [26].

In a data-driven CE ecosystem, the management of finite resources and intelligent assets is coordinated by data flows. Data in turn are also considered to be assets and of a high value. Reciting Clive Humby, who back in 2006 coined the phrase "data is the new oil" in an effort to stress that data have become the most valuable resource, it can be seen that CE would need to be data enabled, or alternatively data driven, to be able to deliver what it evangelises.

The interplay of CE with the intelligent assets and particular IoT devices leads to the creation of data structures and patterns, to enable a "circular-by-design" approach. Currently, the prevailing pattern for managing an asset is that of `Location, Condition, Availability`. From these three properties, `Location` and `Availability` refer to the geolocation and the state of the asset. These two properties have already proven sufficient to leverage highly profitable data-driven CE business models, such as in the case of Uber and AirBnB. The `Condition` property is more esoteric to CE itself as it is used to describe the state the respective asset is in terms of its lifecycle. An example definition of this property is `{Condition::good|require_repair|recycle}`. A complete treatment of this concept is presented in Reference [29].

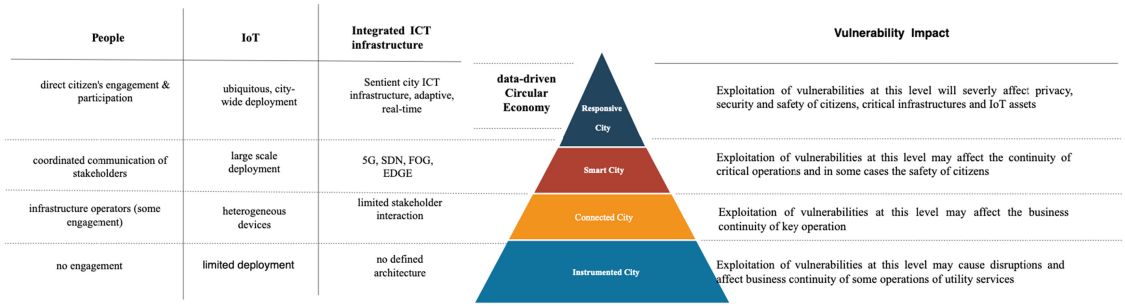

Fig. 1. A maturity model for a smart, circular city (adapted from Reference [12]).

3 A SMART CITY MATURITY LEVEL

A maturity model helps in structuring and streamlining the "CE readiness" of a city against a set of dimensions. Maturity models are widespread in the field of organisational performance as they identify organisational strengths and weaknesses as well as providing benchmarking information. Popular maturity models include OPM3, CMMI, P3M3, PRINCE, BPMM, and Kerzner's Project Management Maturity Model [22]. These models may differ in terms of factors, number of levels as well as application domains [22].

In this work, we adopt the maturity model for smart circular cities as described in Reference [12]. This maturity model is suitable for illustrating the technological roadmap for a city adopting a CE agenda. In Figure 1, the maturity model paired with the potential impact of vulnerabilities in the respective level is outlined.

According to this maturity model, the progression from an instrumented to a responsive city involves the following stages [12]:

- **The Instrumented City.** This is the first stage of the transition, where the city embeds constellations of sensors and devices on the physical infrastructures (e.g., bridges, street lights, gas pipes, the grid). At this stage, the devices perform basic tasks for specific purposes. Almost every device in a city environment is equipped with sensors that perform constrained tasks and has been employed for narrow and specific purposes.
- **The Connected City.** This is the stage where connectors between the different constellations are in place. The existence of these connectors does not necessarily involve any actual exploitation or systematic utilisation of the available data. The stakeholders are still constrained at this stage, consuming data within their respective sector or domain, despite the increased heterogeneity of the data.
- **The Smart City.** This refers to the stage where all assets are fully interconnected and actionable information is available to the stakeholders who can reach high levels of situational awareness. The activities of a smart city environment take place as "back office" operations. Infrastructure operators, utility and service providers can perform intelligent processing and the local government stakeholders can perform global processing and maintain an overview of the city's operations. A smart city is a heterogeneous environment, with different purpose devices and technologies can be used by various users, stakeholders and citizens. Citizens and visitors can use their personal devices, such as smartphones and tablets. For this reason, the amount of data that is produced is vast and facilitates different aspects and services of a city.
- **The Responsive City.** This stage could be considered as the city's "self-actualisation" level, in resemblance to Maslow's hierarchy of needs. A responsive city could be considered as a stage where every part of the city is in a complete sync with its counterparts. This means that humans, intelligent assets and all the other components have access to information in real time, which will be in an appropriate and accessible format. In this way, intelligent assets and smart city infrastructures will be in a position to dynamically reconfigure network and physical structures when it is necessary to address the citizens needs, by

balancing supply and demand. Ultimately, the city is able to adjust itself depending on the circumstances, as living organisms do. A representative use case is the increased gatherings of people, such as social events or incidents, where the safety of citizens and visitors is at stake. Furthermore, the city itself can address and respond to the needs of people before these needs are expressed and avoidance of difficulties, before they take place. Offering capabilities to the city's assets to participate in real-time decision making by reconfiguring its resources to meet the needs of the stakeholders and beneficiaries, defines in essence the *sentient city*.

It is fairly evident that reaching the responsive city level of maturity would require—from a technological perspective—to achieve high levels of connectivity and integration with software services that are delivered in the whole vertical. A representative example is Software Defined Networks, where the network resources and topology is fully defined and controlled by software. As such, the impact of a vulnerability being exploited at a particular maturity level is expected to increase, as one traverses from a lower to a higher level. This suggests that a vulnerability will carry a larger amount of risk, the higher the maturity level this vulnerability will be placed on. More formally, if $R_m(\cdot)$ is some risk calculation function with m denoting the maturity level, then for a particular vulnerability v the following should hold:

$$R_i(v) \leq R_j(v)$$

for $i < j$. This means that if two cities have an identical vulnerability profile, then the city with the highest maturity will also have the highest risk. This is captured in some quantitative vulnerability measurement systems such as the **Common Vulnerability Scoring System (CVSS)** [17, 28], where the resulting severity of a vulnerability can be adjusted and subject to the so-called environmental variables. To the best of our knowledge, the development of a methodology for producing a suitable vulnerability scoring system with an environmental metric group for a smart city infrastructure remains a research challenge, see, for example, Reference [45] where although a concise threat and risk model for smart cities is proposed, there is limited evidence on how the environmental CVSS score dimension is populated. In fact, the CVSS measurement system itself has received criticism from the research and practitioner communities [18, 21] with alternatives being proposed (see, for example, Reference [39]) but despite its shortcomings, it has still been applied to and validated through a variety of contexts and scenarios [10]. In any case, the two main characteristics of a risk-based approach for a vulnerability-driven assessment system would require a vulnerability measuring system and a risk methodology that considers interdependent networks [35]. While these aspects are outside the scope of this work, we argue that the narratives included in the proposed approach could be adapted to develop a suitable risk management approach informed by vulnerability exposure.

In the remainder of this article, we conduct an empirical evaluation of the current state of vulnerabilities as these exist in cities. We explore the existence of potential differences or patterns of vulnerabilities in a collection of cities that can be used to infer practices, behaviours, and other risk factors.

4 ACTIONABLE THREAT INTELLIGENCE THROUGH VULNERABILITY MANAGEMENT

4.1 Datasets: Limitations of Research

For this research, datasets from two primary domains were considered. The first domain covers the independent factors or variables of the study and is primarily composed from the descriptors of cities as expressed by the cities in motion research [7]. The dependent variables are primarily covered from the cybersecurity dataset. To this end, we extended the ENISA vulnerabilities 2018–2019 dataset [15, 16]. This dataset comprised contextualised vulnerability data from a number of sources. Starting from the curated list of vulnerabilities in the NVD database, these were enriched with tactics and techniques as specified by the ATT&CK framework[1] as well as the exploit

[1] https://attack.mitre.org.

Table 1. Dataset Description

Vulnerabilities		City metrics	
source	features	source	features
NVD [33]	CVE, CVSS	Cities in Motion [7]	Ninety-six variables over nine indicator categories, including population, human capital, technology, city in motion score
Shodan	#vulnerable devices, geolocation	IMD [8]	adoption of digital technologies, citizen perceptions, smart city ranking
MITRE [30]	CWE	C40 [11]	leading CE cities

database.[2] Although the original ENISA dataset contained also information from Shodan on the number of exploits, it did not include information on the actual exposure—that is, a view of actual devices that are potentially vulnerable to a particular exploit. For the purpose of this research, we extended the ENISA dataset to contain such information.

Moreover, the geolocation of the IP addresses of the vulnerable devices was used to pivot between the vulnerability and city/country domain data. As such, we ended up with a dataset of vulnerabilities attached to devices that in turn were mapped to geographical locations. Hence, the accuracy of geolocation is limited and bounded by Shodan's geo-mapping process. To this end, to avoid ambiguity on the city data and overcome any city synonyms, the queries for the geolocation searches consisted of the (country, city) tuple.

A noteworthy limitation of this research is the fact that there was no identification information on the type of service or direct attribution of ownership of the vulnerable devices. This means that we observe the city as a whole rather than distinguishing the different services, sectors (e.g., separation between critical infrastructure and household devices and so forth); such information is crucial in a fully blown interconnected networks approach. In addition to this, the collection does not cover IPv6, and as such a potentially substantial volume of IoT devices was not taken into consideration. This may affect the actual results of relatively more mature smart cities and especially those that have already deployed 5G, so we accept that the findings in the present study represent the best case scenario and the lower bound of the attack surface. In addition, exclusion of IPv6 would limit the scope to more "traditional" and core services. Nevertheless, this limitation, together with the geolocation approach shows the need for a city's NOC/SOC equivalent to invest in asset discovery and a register that from a practical perspective this is a non-trivial task. Furthermore, any IP addresses exposing devices through VPN or TOR networks were not filtered out, as these were not expected to introduce any significant bias in the analysis.

It should be noted that, as with all exercises of joining data from different sources, the end dataset may have sparse entries. Although there are approaches to increase the sample population of a given feature with a low number of data points (see, for example, ML-based dataset imputation applied on the ENISA dataset [37]), this was not required for this study. A summary of the features of the resulting dataset used is presented in Table 1. In addition to the vulnerabilities and city data, we also employed ITU's Global Cybersecurity Index, GCI [43]. This metric reflects a country's commitment to cybersecurity and is compiled from 25 measured indicators across five pillars: legal, technical, organisational, capacity building, and cooperation.

Another limitation of this study is the volatility of the results due to the nature of the live vulnerability exposure data. More specifically, the data recorded from Shodan, a search engine designed to gather and index information about internet-connected devices and systems, represent a snapshot in a particular time. Shodan's command line interface allows users to develop scripts in Bash language to automate the collection of results.

[2] https://www.exploit-db.com/about-exploit-db.

The scripts that were created to automatically scrape the data contained several queries needed to collect the desired data. Apart from the queries to retrieve port, device type, product type and protocol, the following four queries were the most important:

- **vuln:** This query returns devices vulnerable to a given vulnerability such as MS17-010 or CVE-2017-15906.
- **count:** This query returns the total amount of devices. For example, in November 2020, 7,647,885 devices were vulnerable to CVE-2017-15906.
- **country:** This query returns the number of devices from a specific country.
- **city:** This query returns the number of devices from a specific city.

For the purpose of this study, the vulnerability data were used to explore whether potentially significant relationships may exist between these types of data and other, orthogonal dimensions (such as behavioural and economic variables). In a real-life deployment, it would be more appropriate to collect and maintain historical vulnerability data to run longitudinal research that is expected to provide actionable information of a higher quality. To this end, other vulnerability exposure databases can be considered such as Censys[3] and Zoomeye[4]; it is noteworthy that the latter contains historical exposure information. In addition, as the exposure metric is based on Shodan's methodology of assigning CVEs to devices and services, the accuracy of the results and findings are bounded by Shodan's disclaimer of implied vulnerabilities.

Last, with regards to the quantitative measures of vulnerabilities, this study inherits the limitations and issues surrounding the CVSS scoring convention. Specifically, although the CVSS approach is in principle founded on widely acceptable methodologies and is considered trustworthy [21], its use and applications introduce conflicts with regards to the assignment of the actual values and ground truth. Indicatively, the National Vulnerability Database that can be viewed to maintain an authoritative record of CVSS scores shows a substantially low correlation of some of impact measures (Confidentiality, Integrity, Availability) between CVSS version 2 and version 3. More specifically, the correlation of integrity and availability between the two versions were found to be 0.34 and 0.38, respectively [15].

4.2 Analysis and Findings

The analysis that follows is twofold. First, we use the available datasets as means for evaluating whether these published, available data are aligned with, or can interpret or support assumptions and policy directions as stated in the recent literature. Secondly, we present a series of approaches smart city stakeholders could adopt when developing vulnerability management capabilities.

The analysis also follows a top-down approach. We initially analyse data on a city aggregate level and evaluate the counties vulnerability exposure by considering additional macroeconomic measures. We then move on to city comparisons and finally we focus on the cities themselves.

To develop meaningful comparisons, we use the population variable to normalise the vulnerability data. There are two approaches for doing this, namely dividing the vulnerability variables by the population, or adding the latter to the set of independent variables in the regression model(s). Furthermore, we define the vulnerability exposure E_c of a city or country c as

$$E_c = \sum_{v \in V_c} |v| * b_v,$$

where V_c is the multiset of discovered vulnerabilities for c and b_v is the CVSS base score of vulnerability v. As the vulnerability exposure failed the **Kolmogorov-Smirnov (K-S)** normality test, we consider the natural logarithm values $ln(E_c)$ instead, as this variable follows a normal distribution (K-S significance: 0.604), which allows the construction and testing of the regression models.

[3] https://censys.io/.
[4] https://www.zoomeye.org/.

Table 2. Country Regression Model

Model Info			**Model Fit**				
Observations:177			$F(3,173) = 27845$, $p = 0.000$				
Dependent variable: log_exposure			$R^2 = 0.326$				
Type: OLS			Adj. $R^2 = 0.314$				
	Coefficients					**Collinearity stats**	
	B	std. error	β	T	p	Tolerance	VIF
intercept	11.177	0.268		41.640	.000		
GDP	2.973e-005	0.000	0.218	2.917	.004	0.699	1.431
GCI	3.939	0.852	0.353	4.623	.000	0.667	1.498
population	3.501e-009	.000	0.210	3.232	.001	0.921	1.086

4.2.1 Scope: Country. A country level study can facilitate the contextualisation of the vulnerabilities exposure as this can bring in country indices and factors, which to an extent encapsulate the historical efforts and profile of the country on geo-pollitical matters. Analysis on a country level can be a good reference and baseline to build a pragmatic cyber situational awareness capacity. For instance, a city's investment budget is normally comprised of funding external to the city (funding of national or international origin such as from international research bodies or other organisations) as well as through income from its primary stakeholders (citizens, businesses) in the form of a tax. Assuming that the GDP of a country is a factor that relates to the cybersecurity investment and capacity [9, 13].

Table 2 summarizes the results of the regression analysis on the vulnerabilities exposure against the independent variables, GDP, GCI, and population. The **Variance Inflation Factors (VIF)** are all less than 10—or, alternatively the Tolerance values are greated than 0.1—showing that there is no co-linearity between the interpretive variables. The adjusted R^2 is significant, where it is shown that the Global Cybersecurity Index is the strongest of the three in explaining the level of exposure. More specifically, although the GDP and population result in the increase of the attack surface, the GCI also follows a positive correlation overall. In essence, as the GDP increases so does the investment in networked devices, but countries do also seem to invest in improving their cybersecurity capabilities at the same time, as captured by the GCI. However, this does not suggest that *all* countries follow such practice; outlier countries who are on a low GCI score with high exposure may not have an effective vulnerability management plan. At the time of writing, the countries with the highest exposure and lowest GCI are Cape Verde, Palau, and Eritrea. Interestingly, at the time of writing (Q1 of 2021), the government of Cape Verde approved the establishment of a national CSIRT and a National Cybersecurity Centre together with the introduction of a legislative framework [40]. This is a timely development, as a country with a high exposure and a low cybersecurity investment can potentially be an easy target and the adoption of security controls and measures is imperative.

It should be highlighted that the regression model described above is vulnerability management practices agnostic; a high GCI score indicates that there *may* be a vulnerability management scheme in place, but there is no explicit metric for that—other than the generic technical and capacity building pillars. As such, the government of a country could use this model to benchmark their position and compare where their actual exposure against the estimated value. This in turn would allow them to strategise and prioritise on a vulnerability management program.

Another metric showing the cybersecurity effort in relation to the exposure is the log of the ratio between E_c and GCI. This metric is normally distributed (Shapiro–Wilk test significance: 0.056), with a mean of 14.685, standard deviation of 2.28 and within the range of [9.73, 20.92]. Countries placed on the low end of the distribution have potentially over-invested in cybersecurity considering their actual attack surface, whereas countries with a value close to 20 may be overexposed.

	N	#CVE	mean	std
plain	87	16.8m	7.580	0.463
circular	5	6.2K	7.533	0.186
smart	91	22m	7.541	0.239
both	11	7m	7.339	0.175

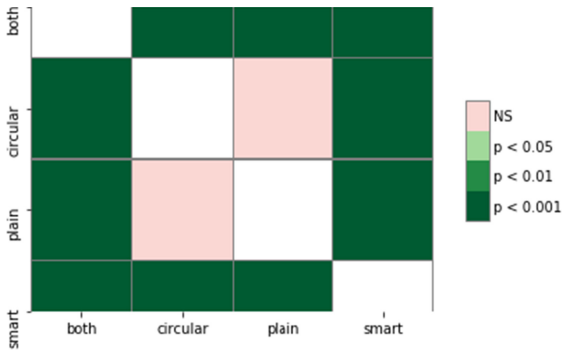

Fig. 2. Pairwise comparisons of the four city classes.

4.2.2 Scope: City. Moving on to a cities view, a broad analysis considers the cities based on their current maturity level and agendas. To this end, we considered four classes of cities:

Class 1: the `plain` city, referring to those cities that have not indicated progress or intention to implement a smart city agenda;
Class 2: the `circular` city, referring to cities that have a CE agenda, but have not explicitly considered to implement this adopting a clear data-driven approach;
Class 3: the `smart` city, referring to cities that are evaluated and included in the IMD or Cities in Motion study;
Class 4: the `both` city, referring to cities that are smart and also have a CE agenda, as specified in the C40 dataset.

As it is advocated that CE cannot be delivered without the data-driven dimension employing technological ICT enablers [3, 5], we argue that cities that have a set CE agenda, have also a more definitive and mature technological roadmap than other cities.

Figure 2 summarises the pairwise vulnerability means comparisons of the different classes of cities. In all cases the average CVSS base score revolves around the mid 7s with the `plain` cities exhibiting the highest mean and standard deviation. With regards to these comparisons, all cities show significant differences except `plain` and `circular cities` where their differences were not significant.

However, this first exploratory analysis is limited as a comparison of means is a static approach. In addition, the sample of the cities with a circular only agenda is relatively small ($N = 5$) so we consider a further class `motion` that contains all cities that are showing early signs of "smartness" (very low in the maturity scale), yet clearly higher than the `plain` cities who have not declared any smart city initiatives. The city type remains an ordinal, discrete variable with the ascending order of `plain, motion, smart, both` and in this case includes all cities that have been included in the independent studies and respective datasets. Such arrangement allows the construction of the following hypotheses:

H_1 The city type moderates the vulnerability exposure such that it is higher for smarter cities than plainer cities.
H_2 The vulnerability exposure in cities increases with their population.
H_3 The vulnerability exposure in cities decreases with their level of technology.

The focus of H_1 is on the overall exposure rather than the severity score. This is an assumption stemming from the fact that smarter cities become more dependable on technology; technology is more pervasive in smart cities and the cyber attack surface is expected to be bigger than in a plain city. However, for H_3 we assume that a high technology score will have a negative relation with exposure. This is also in agreement with the particular definition of this indicator in the Cities in Motion study, as it includes indicators that measure innovation, the web

Table 3. City Regression Model 1

Model Info			**Model Fit**		
Observations:170			$F(3,166) = 16727$, $p = 0.000$		
Dependent variable: exposure			$R^2 = 0.231$		
Type: OLS			Adj. $R^2 = 0.217$		
	Coefficients				
	B	std. error	β	T	p
intercept	793555.776	743060.891		1068	.287
population	.187	.038	0.348	4891	.000
technology	−20047.553	4737.873	−.304	−4231	.000
city_type	775686.647	276255.132	.196	2808	.006

Table 4. Regression Model 2

Model Info			**Model Fit**		
Observations:171			$F(6,164) = 16290$, $p = 0.000$		
Dependent variable: exposure			$R^2 = 0.372$		
Type: OLS			Adj. $R^2 = 0.349$		
	Coefficients				
	B	std. error	β	T	p
population	.190	.040	.414	4746	.000
technology	−19471.425	4977.282	−.543	−3.912	.000
motion	1706746.558	621010.315	.278	2.748	.007
smart	2175288.130	496238.743	.405	4.384	.000
plain	2180776.000	763190.887	.220	2.857	.005
both	5468921.448	975307.816	.364	5.607	.000

index measuring the economic, social and political benefit obtained from the Internet as well as the registered users on social media, broadband speed, WiFi coverage and so forth. On face value, some of these indicators may be expected to increase exposure, but we also expect that a high technological achievement also requires talent and expertise in cybersecurity in providing a secure and safe infrastructure to the citizens. Nevertheless, as technology is one of many factors that is expected to influence the vulnerability exposure, it may not be sufficient to "drag" exposure down; it is well accepted that cybersecurity cannot be addressed by solely technical means and other factors (such as human aspects when the subject of the study is a socio-technical system) need to be taken into consideration.

In Tables 3 and 4, the regression results are presented. In model 1, the independent variable `city_type` refers to the four city classes (with `circular` being replaced by `motion`). This variable is exploded to its different types in model 2 to validate H_1. Note that there is no intercept in this model to avoid multicollinearity due to the explosion of the type variable.

The results are significant and confirm the hypotheses H_2 and H_3. For H_2 in particular, we can see that it also holds by observing the β coefficients that confirm the order of the city types in accordance to our initial hypothesis, with the smarter cities being more exposed than the plainer cities. This in turn confirms also the fact that technology alone is not sufficient to address cybersecurity issues.

Figure 3 shows the results of hierarchical clustering (Ward's method) of vulnerabilities on the cities that have declared a smart and circular agenda (class `both`). This information can be actionable in two ways. First, it would allow the local authorities to prioritise and team up with those authorities of the cities that seem to have similar

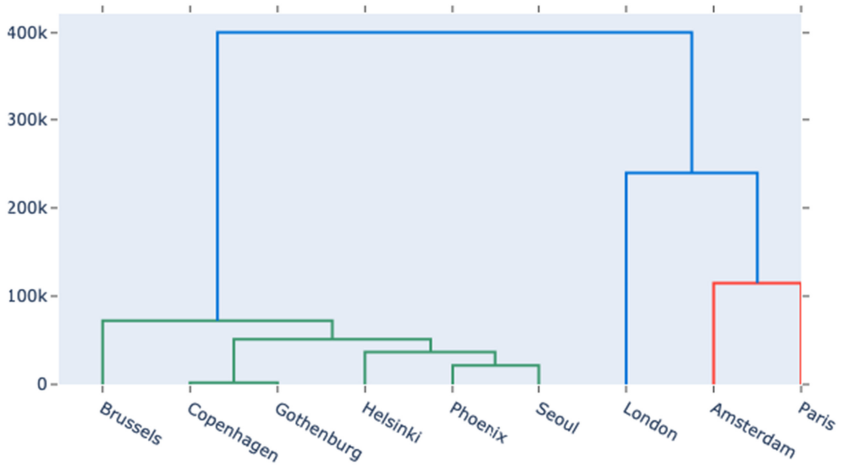

Fig. 3. Hierarchical clustering of cities having a smart and CE agenda (class:both).

vulnerabilities and exposure profile. Such intelligence could contribute to information sharing and operational cooperation activities. Assuming that CSIRTs on a local authority level are established—say, through forming their own local authority CSIRT network - the councils could form operational cooperation structures with selective peers. At the time of writing, the closest CSIRTs to supporting a local authority are primarily operators of essential services (such as healthcare, transport, utiliy services and so forth, see ENISA's CSIRT interactive map[5]). Second, any attacks mounted to a city of a similar vulnerability profile could act as an early warning for the unaffected yet *similar* city. The absence of geo-political contextualisation of the data at this level would restrict the benefit of this approach to thwarting scatter-gun type of attacks, such as Mirai and Wannacry, which had devastating consequences not to the economy but also to safety. In essence, such an approach would help a local authority to effectively triage across the hundreds of cities and establish information sharing with peer authorities for the purpose of increasing their situational awareness and improving their responses to cybersecurity incidents. As an example on how the vulnerability exposure information can be leveraged from the clusters shown in Figure 3, Paris and Amsterdam are grouped under the same cluster and as such exhibit similarities on potential vulnerabilities. This would trigger an additional analysis and study to see why these two cities are grouped together and an example direction would be to inspect the exposure profiles against the types of devices, protocols and whenever possible, sectors. Both Amsterdam and Paris have made significant progress in smart building infrastructures, with Amsterdam maintaining the most celebrated circular office building to date. "The Edge," is designed and built for the headquarters of Delloite in Amsterdam and is considered the most intelligent office building in the world [44] with 28K sensors, and a state of the art data centre, constantly monitoring and controlling the internal environment. Paris, however, has a concentration of almost half of innovative startups in the smart building industry [4].

Table 5 contains the results of a factor analysis performed on the top 20 cities with the highest exposure and potential exploitability to vulnerabilities. The analysis produced three factors (groups) in total, with a significantly high alpha (over 0.7) in all cases, showing strong internal consistency and that the respective dimensions (cities in our case) can be reduced and represented by their assigned groups (factors).

In Table 6, the weakness profile of the four city classes is shown. Although there seem to be differences in the distribution of the weaknesses across the classes, this is an oversimplified overview offering a coarse level comparison between these city classes and needs to be further contextualised and substantiated to extract

[5]https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map.

Table 5. Factor Analysis (Loadings) of Top 20 Cities with the Most Potential Vulnerabilities

Factor 1		Factor 2		Factor 3	
Ashburn	0.7724	Sydney	0.7245	Chicago	0.9596
Tokyo	0.6910	Central	0.8390	Miami	0.8154
London	0.9050	Incheon	0.8180	Buffalo	0.9574
Dublin	0.8811	Johannesburg	0.9552		
Columbus	0.8197				
Singapore	0.8458				
Amsterdam	0.9710				
Mumbai	0.8992				
Paris	0.8611				
Montreal	0.7529				
Moscow	0.7682				
Dallas	0.7713				
Nuremberg	0.9840				
Cronbach's alpha	0.9614		0.9335		0.9130
Bartlett's sphericity test:		chi square: 24144.232		p-value: 0.000	

Table 6. Weakness Profile per City Class

CWE		plain	circular	smart	both
20*:	Improper Input Validation	✓		✓	
399:	Resource Management Errors	✓			✓
119*:	Improper Restriction of Operations within the Bounds of a Memory Buffer	✓	✓		
384:	Session Fixation	✓			✓
416*:	Use After Free	✓			
787*:	Out-of-bounds Write	✓	✓		
287*:	Improper Authentication	✓	✓	✓	
476*:	NULL Pointer Dereference	✓	✓	✓	
732*:	Incorrect Permission Assignment for Critical Resource		✓		
444:	Inconsistent Interpretation of HTTP Requests		✓		
126:	Buffer Over-read			✓	
200*:	Exposure of Sensitive Information to an Unauthorized Actor			✓	
320:	Key Management Errors				✓
362:	Concurrent Execution using Shared Resource with Improper Synchronization				✓
390:	Detection of Error Condition Without Action				✓
400*:	Detection of Error Condition Without Action				✓
	*In top 25 most dangerous software weaknesses list [30]:	75%	83%	80%	16%

actionable information. A metric prescribing the percentage of most dangerous weaknesses (as agreed by the community) would offer opportunities for comparison, which can also be performed on a city level granularity, comparing like-to-like cities (in terms of economic or other maturity dimensions). Interestingly, the cities that have both a smart and circular agenda have the least percentage of most dangerous weaknesses. This finding, is in agreement with the results in Figure 2, where the `both` class shows the lowest mean across all cities, although the weakness profile data refer to unique counts of a particular weakness per city rather than the totals (as in the case of the mean CVSS base scores).

Table 7. Backward Regression Results

Model Info			**Model Fit**		
Observations:173			$F(3,169) = 5738$, $p = 0.000$		
Dependent variable: exposure			$R^2 = 0.163$		
Type: OLS			Adj. $R^2 = 0.148$		
	Coefficients				
	B	std. error	β	T	p
intercept	1849657.449	599408.291		3.086	.002
human_capital	−13431.430	4856,886	−.204	−2.765	.006
smart	1103603.507	501319.562	.166	2.201	.029
both	4214523.878	1036497.640	.296	4.066	.000

4.2.3 Scope: Human Aspects. Notwithstanding the fact that the scope of software vulnerabilities and exposures lies within the realm of interconnected devices, an analysis of a sociotechnical basis is a fundamental approach when assessing factors that are potentially capable of moderating and regulating these vulnerabilities from a non-technical approach. To this end, Table 7 shows the results of a backward stepwise regression with exposure being the dependent variable; the initial dependent variables were human_capital, social_cohesion, technology as defined in Cities in Motion as well as the three city classes: plain, smart, and both. The circular class was omitted again due to the low number of observations. Interestingly, the backward regression completed after four rounds (models) where in every round a variable was removed. The end result included human_capital, smart, and both. This is a remarkable result showing that smart cities, smart cities with a CE agenda and human capital are significant in predicting the vulnerability exposure, even more important that technology maturity. From the β coefficients, smart and circular cities are more vulnerable than smart cities (with no circular agenda), showing indeed that smart, circular cities are likely to be more technologically "hungry," highlighting the data-driven nature of CE, but at the same time are more exposed. This finding can also be used to validate, to some extent, the adopted maturity model for smart, circular cities. Moreover, the negative sign of the β coefficient for human capital shows an inverse relationship between this factor and vulnerability exposure. Although not surprising, the significance of this finding is appreciated if we look into the rationale and indicators of the human capital construct. From the Cities in Motion study (Reference [7], p. 11): "The main goal of any city should be to improve its human capital. A city with smart governance must be capable of attracting and retaining talent, creating plans to improve education, and promoting both creativity and research."

Moreover, the human capital variable is comprised of 10 indicators most of which focus on education and culture, such as number of universities that are in the top 500 list, expenditure on education per capita, international movement of higher-level students, but also number of theatres per city, expenditure on leisure and recreation. All in all, informed by this model we would dare to argue that a "sophisticated city is a (potentially) secure city."

Interestingly, all the above empirical findings can be summed up by the position of Reference [27], referencing [14, 25]: "considering the way humans, government, and technology interact, security education is desirable to strengthen the knowledge of government officials and citizens with regard to cybersecurity issues." Such positions reinforce the complex and interdisciplinary nature of cybersecurity; starting from studying the vulnerabilities and an exposure of a particular conurbation that, in essence is dependent of and defined by a wealth of factors, we discover significant relationships and dependencies of the exposure and many of these factors. The latter are both technological and human, as measured by the independent studies. Having created a model showing the expected exposure of a city and comparing this against the actual exposure (as measured by services like Shodan, which was used in this current study), would allow the city's planners, stakeholders and policy makers to reflect on their particular case by factoring in their own geo-political context and take informed decisions on the required cybersecurity investment and vulnerability management and incident response capabilities in particular.

It is also worth reporting that the regression was also ran with `exposure_per_person` being the dependent variable. In this case, the most significant model contained the factors `technology, both` and `plain`. In other words, if the size of the population is used to normalise the vulnerability exposure, then the technology factor becomes more prevalent.

5 CONCLUDING REMARKS AND OUTLOOK

Extending the scope of data by including feeds from sources orthogonal to cybersecurity can offer added value to cyber threat intelligence and increased situational awareness. We demonstrated that the injection of open data from published smart city studies into the vulnerabilities domain can offer insights into the factors affecting the vulnerability exposure of a particular socio-technical ecosystem. In particular, this work focused on smart cities and to this end the vulnerability exposure was considered against a smart city maturity model to enable the development of a meaningful and contextualised risk-based approach using vulnerability impact and exposure data.

Although the datasets used were from independently conducted studies or sources, we observed statistically significant relationships. The underlying hypotheses were confirmed and there were no instances where the data contradicted widely accepted beliefs and positions of the cybersecurity community, such as the increased exposure of an advanced smart city and the fact that investing on the human capital is key to reducing the cybersecurity risks.

The proposed approach has a wide range of research directions and practical implications. Cities are challenged in the ways they fundamentally operate; their governance and business models are substantially revised to meet the expectations of their citizens who are congruent to end users of the introduced ICT infrastructures. In such deployments of devices on a massive scale, cyber situational awareness and incident response capabilities would need to be adequately defined from the outset. As such, identifying a common ground between cybersecurity approaches and local governance is a significant activity. Practices such as establishing a city level CSIRT and coordination with other peer CSIRTs, cyber certification schemes for smart city products and services are a few examples of activities for improving the risk posture and controlling the vulnerability exposure of a city.

Short-term future research involves the development of an integrated model of vulnerabilities in smart, circular cities by performing structured equation modelling on the indicators of the non-vulnerability related data, such as those described in the Cities in Motion and the IMD world digital competitiveness data that include the citizens' perceptions and adoption of smart city technologies. From the vulnerabilities perspective, further enrichment of the data with standardised CTI indicators such as ATT&CK's techniques and tactics, CAPEC and so forth, is expected to offer additional insights on the city's exposure and facilitate more efficient decision making.

A limitation of this research is the coarse level of granularity on the city data and absence of context, since every city and country have their own distinct paths and trajectories in the geo-political plane. Although from a vulnerabilities and exposure perspective there may not be significant discriminators; however, from a risk perspective there can be considerable contrasts. To appreciate the subtle differences, we can distinguish between scatter-gun type of attacks (such as Wannacry), and targeted, specific attacks (such as Stuxnet or the more recent ransomware attacks on critical infrastructures, see the Colonial Pipeline attack) that are lately also acknowledged as hybrid threats. Scatter-gun type of attacks do not discriminate by geographic location and the underlying probability of a successful attack would be comparable across all cities matching the *right* vulnerability profile. In this case the impact of the (same type of) attack would be different, depending on the city maturity level, and the models proposed in this research can be used to both understand how a city performs against a baseline of alike cities, but also to develop an incident response plan and decide on the prioritisation of information sharing with other peer cities. With regards to the targeted attacks, the stakeholders should again compare their position relative to the baseline and factor in their geo-pollitical parameters to assess whether their standing is adequate given their context. A medium-term research direction that would allow the development of a incident response and vulnerability management plan involves the introduction of sector specific device information to further enrich the vulnerabilities descriptions. This will enable the study of vulnerabilities using theory and approaches from

the interdependent networks domain. From an operational level, it will allow further interpretation and consequently obtain more added value from the critical weaknesses (Table 6). Defining the boundaries of the different constellations of subsystems and performing segmentation of the constituencies would allow the definition of different risk areas (such as core critical infrastructure components to mobile ad hoc Machine-to-Machine as well as end user/citizen realms) that in turn would enable the creation of more efficient resource management capabilities and finer-tuned incident response capacity.

Last, enriching the datasets with finer-grained contextual and qualitative information (such as the geo-political context) would enable a tighter coupling of the triptych comprised of vulnerability management, risk assessment and incident response processes. The impact and severity quantification of the vulnerabilities would better be reflected in the quantitative descriptors, such as the CVSS scores. As a future research activity, the first step for capturing the different impact levels of a given vulnerability across the different cities would be through the adjustment of the `environmental` scores depending on the smart city maturity level; this can be estimated by using the regression models as presented in this work. Having an agreed or expected environmental score for a given maturity level, it would be possible to allow some automated adjustments of a CVSS final score. In principle, the higher the maturity level, the higher the CVSS environmental scores should be. However, by introducing the city's geo-political context, it would be possible to further tweak and refine the final score. This would make the vulnerability severity and impact scoring system appropriate for feeding into the risk assessment process. The residual risk in turn would then be considered for developing effective and appropriate incident response capabilities. By maintaining the view of a smart city being an interconnected network running critical infrastructures with a variety of stakeholders, the residual risk could be used for making a business case of deploying CSIRTs on a city or local authority level. From a governance perspective we envisage such CSIRTs to be placed below the respective National CSIRTs and at the same level of Law Enforcement entities and utility providers, forming information sharing and cooperation networks on such layer. This would not only allow the development of attainable and realistic vulnerability management processes, but would foster effective incident response capabilities.

REFERENCES

[1] Yas A. Alsultanny. 2014. Evaluating users intention to use e-overnment services. *Environment* 3, 5 (2014).

[2] Leonidas G. Anthopoulos. 2017. The rise of the smart city. In *Understanding Smart Cities: A Tool for Smart Government or an Industrial Trick?* Springer, 5–45. DOI: https://doi.org/10.1007/978-3-319-57015-0

[3] Maria Antikainen, Teuvo Uusitalo, and Päivi Kivikytö-Reponen. 2018. Digitalisation as an enabler of circular economy. *Proc. CIRP* 73 (2018), 45–49. *10th CIRP Conference on Industrial Product-Service Systems*, IPS2 2018, 29-31 May 2018, Linköping, Sweden. DOI: https://doi.org/10.1016/j.procir.2018.04.027

[4] Sevinç Ar. 2021. Circular Economy Models for Smart City Assets. Retrieved November 14, 2020 from https://www.ideal-cities.eu/wp-content/uploads/2019/10/IDEAL-CITIES-D2.1.pdf.

[5] Ioannis Askoxylakis. 2018. A framework for pairing circular economy and the Internet of Things. In *Proceedings of the IEEE International Conference on Communications (ICC'18)*. IEEE, 1–6. DOI: https://doi.org/10.1109/ICC.2018.8422488

[6] Gordon Baxter and Ian Sommerville. 2011. Socio-technical systems: From design methods to systems engineering. *Interact. Comput.* 23, 1 (2011), 4–17. DOI: https://doi.org/10.1016/j.intcom.2010.07.003

[7] P. Berrone and J. E. Ricart. 2019. IESE Cities in Motion Index. Retrieved November 14, 2020 from https://media.iese.edu/research/pdfs/ST-0509-E.pdf.

[8] Arturo Bris and Christos Cabolis. 2020. IMD World Digital Competitiveness Ranking 2020. Retrieved November 14, 2020 from https://www.imd.org/globalassets/wcc/docs/release-2020/digital/digital_2020.pdf.

[9] Andrea Calderaro and Anthony J. S. Craig. 2020. Transnational governance of cybersecurity: Policy challenges and global inequalities in cyber capacity building. *Third World Quar.* 41 (2020), 1–22. DOI: https://doi.org/10.1080/01436597.2020.1729729

[10] Pengsu Cheng, Lingyu Wang, Sushil Jajodia, and Anoop Singhal. 2012. Aggregating CVSS base scores for semantics-rich network security metrics. In *Proceedings of the IEEE 31st Symposium on Reliable Distributed Systems*. IEEE, 31–40. DOI: https://doi.org/10.1109/SRDS.2012.4

[11] C40 Cities. 2020. Municipality-led Circular Economy Case Studies. Retrieved November 14, 2020 from https://www.c40.org/researches/municipality-led-circular-economy.

[12] Ideal Cities. 2019. Construction & Smart Building. Retrieved April 14, 2021 from https://www.chooseparisregion.org/industries/construction-smart-building.
[13] Sadie Creese, William H. Dutton, Patricia Esteve-Gonzalez, and Ruth Shillair. 2020. Cybersecurity capacity building: Cross-national benefits and international divides (unpublished).
[14] Hans de Bruijn and Marijn Janssen. 2017. Building cybersecurity awareness: The need for evidence-based framing strategies. *Govern. Inf. Quart.* 34, 1 (2017), 1–7. DOI: https://doi.org/10.1016/j.giq.2017.02.007
[15] ENISA. 2019. State of Vulnerabilities 2018/2019—Analysis of Events in the Life of Vulnerabilities. Retrieved November 20, 2020 from https://www.enisa.europa.eu/publications/technical-reports-on-cybersecurity-situation-the-state-of-cyber-security-vulnerabilities/download/fullReport.
[16] ENISA 2020. The 2018-2019 ENISA Vulnerabilities Dataset. Retrieved November 10, 2020 from https://github.com/enisaeu/vuln-report.
[17] FIRST 2020. Common Vulnerability Scoring System. Retrieved November 10, 2020 from https://www.first.org/cvss/.
[18] L. Gallon. 2010. On the impact of environmental metrics on CVSS scores. In *Proceedings of the IEEE 2nd International Conference on Social Computing*. 987–992. DOI: https://doi.org/10.1109/SocialCom.2010.146
[19] British Standards Institution. 2014. The Role of Standards in Smart Cities. Retrieved November 14, 2020 from https://www.bsigroup.com/LocalFiles/en-GB/smart-cities/resources/The-Role-of-Standards-in-Smart-Cities-Issue-2-August-2014.pdf.
[20] Elvira Ismagilova, Laurie Hughes, Yogesh K. Dwivedi, and K. Ravi Raman. 2019. Smart cities: Advances in research–An information systems perspective. *Int. J. Inf. Manage.* 47 (2019), 88–100. DOI: https://doi.org/10.1016/j.ijinfomgt.2019.01.004
[21] Pontus Johnson, Robert Lagerström, Mathias Ekstedt, and Ulrik Franke. 2016. Can the common vulnerability scoring system be trusted? A bayesian analysis. *IEEE Trans. Depend. Sec. Comput.* 15, 6 (2016), 1002–1015. DOI: https://doi.org/10.1109/TDSC.2016.2644614
[22] Mohammad Khoshgoftar and Omar Osman. 2009. Comparison of maturity models. In *Proceedings of the 2nd IEEE International Conference on Computer Science and Information Technology*. IEEE, 297–301. DOI: https://doi.org/10.1109/ICCSIT.2009.5234402
[23] Duncan Ki-Aries, Shamal Faily, Huseyin Dogan, and Christopher Williams. 2018. System of systems characterisation assisting security risk assessment. In *Proceedings of the 13th Annual Conference on System of Systems Engineering (SoSE'18)*. IEEE, 485–492. DOI: https://doi.org/10.1109/SYSOSE.2018.8428765
[24] Rob Kitchin and Martin Dodge. 2019. The (in) security of smart cities: Vulnerabilities, risks, mitigation, and prevention. *J. Urb. Technol.* 26, 2 (2019), 47–65. DOI: https://doi.org/10.1080/10630732.2017.1408002
[25] David Klaper and Eduard Hovy. 2014. A taxonomy and a knowledge portal for cybersecurity. In *Proceedings of the 15th Annual International Conference on Digital Government Research*. Association for Computing Machinery, New York, NY, 79–85. DOI: https://doi.org/10.1145/2612733.2612759
[26] David J. Langley, Jenny van Doorn, Irene C. L. Ng, Stefan Stieglitz, Alexander Lazovik, and Albert Boonstra. 2021. The internet of everything: Smart things and their impact on business models. *J. Bus. Res.* 122 (2021), 853–863. DOI: https://doi.org/10.1016/j.jbusres.2019.12.035
[27] Zhen Li and Qi Liao. 2018. Economic solutions to improve cybersecurity of governments and smart cities via vulnerability markets. *Govern. Inf. Quart.* 35, 1 (2018), 151–160. DOI: https://doi.org/10.1016/j.giq.2017.10.006
[28] Peter Mell, Karen Scarfone, and Sasha Romanosky. 2006. Common vulnerability scoring system. *IEEE Secur. Priv.* 4, 6 (2006), 85–89. DOI: https://doi.org/10.1109/MSP.2006.145
[29] Andreas Miaoudakis, Konstantinos Fysarakis, Nikolaos Petroulakis, Sofia Alexaki, George Alexandirs, Sotiris Ioannidis, George Spanoudakis, Vasilis Katos, and Christos Verikoukis. 2020. Pairing a circular economy and the 5G-enabled Internet of Things: Creating a class of "Looping Smart Assets." *IEEE Vehic. Technol. Mag.* 15, 3 (2020), 20–31. DOI: https://doi.org/10.1109/MVT.2020.2991788
[30] MITRE 2020. 2020 CWE Top 25 Most Dangerous Software Weaknesses. Retrieved November 10, 2020 from https://cwe.mitre.org/top25/archive/2020/2020_cwe_top25.html.
[31] Saraju P. Mohanty, Uma Choppali, and Elias Kougianos. 2016. Everything you wanted to know about smart cities: The internet of things is the backbone. *IEEE Consum. Electr. Mag.* 5, 3 (2016), 60–70. DOI: https://doi.org/10.1109/MCE.2016.2556879
[32] Andrew Morlet, Jocelyn Blériot, Rob Opsomer, Mats Linder, Anina Henggeler, Alix Bluhm, and Andrea Carrera. 2016. Intelligent assets: Unlocking the circular economy potential. *Ellen MacArthur Found.* (2016), 1–25.
[33] NVD 2020. National Vulnerability Database. Retrieved November 13, 2020 from https://nvd.nist.gov.
[34] Benjamin Preis and Lawrence Susskind. 2020. Municipal cybersecurity: More work needs to be done. *Urb. Affairs Rev.* (2020). DOI: https://doi.org/10.1177/1078087420973760
[35] Iztok Prezelj and Aleš Žiberna. 2013. Consequence-, time- and interdependency-based risk assessment in the field of critical infrastructure. *Risk Manage.* 15, 2 (2013), 100–131. DOI: https://doi.org/10.1057/rm.2013.1
[36] Ragunathan Rajkumar, Insup Lee, Lui Sha, and John Stankovic. 2010. Cyber-physical systems: The next computing revolution. In *Proceedings of the Design Automation Conference*. IEEE, 731–736. DOI: https://doi.org/10.1145/1837274.1837461
[37] Shahin Rostami, Agnieszka Kleszcz, Daniel Dimanov, and Vasilios Katos. 2020. A machine learning approach to dataset imputation for software vulnerabilities. In *Proceedings of the International Conference on Multimedia Communications, Services and Security (Communications in Computer and Information Science)*, A. Dziech, W. Mees, and A. Czyżewski (Eds.), Vol. 1284. Springer, Cham, 25–36. DOI: https://doi.org/10.1007/978-3-030-59000-0_3

[38] Bhagya Nathali Silva, Murad Khan, and Kijun Han. 2018. Towards sustainable smart cities: A review of trends, architectures, components, and open challenges in smart cities. *Sust. Cit. Soc.* 38, 1 (2018), 697–713. DOI: https://doi.org/10.1016/j.scs.2018.01.053

[39] Georgios Spanos and Lefteris Angelis. 2015. Impact metrics of security vulnerabilities: Analysis and weighing. *Inf. Secur. J.* 24, 1-3 (2015), 57–71. DOI: https://doi.org/10.1080/19393555.2015.1051675

[40] Telecompaper. 2021. Cape Verde to Set Up Computer Security Incident Response Team. Retrieved May 12, 2021 from https://www.telecompaper.com/news/cape-verde-to-set-up-computer-security-incident-response-team-1370871.

[41] UN 2018. 68% of the World Population Projected to Live in Urban Areas by 2050, Says UN. Retrieved November 10, 2020 from https://www.un.org/development/desa/en/news/population/2018-revision-of-world-urbanization-prospects.html.

[42] International Telecommunication Union. 2014. Smart Sustainable Cities: An Analysis of Definitions. Retrieved November 14, 2020 from https://www.itu.int/en/ITU-T/focusgroups/ssc/Documents/Approved_Deliverables/TR-Definitions.docx.

[43] International Telecommunication Union. 2018. Global Cybersecurity Index (GCI). Retrieved May 12, 2021 from https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf.

[44] Anastasia Vayona and Giorgos Demetriou. 2020. Towards an operating model for attribution in circular economy. In *Proceedings of the 16th International Conference on Distributed Computing in Sensor Systems (DCOSS'20)*. IEEE, 490–495.

[45] Paul Wang, Amjad Ali, and William Kelly. 2015. Data security and threat modeling for smart city infrastructure. In *Proceedings of the International Conference on Cyber Security of Smart Cities, Industrial Control System and Communications (SSIC'15)*. IEEE, 1–6. DOI: https://doi.org/10.1109/SSIC.2015.7245322

Received 30 November 2020; revised 13 June 2021; accepted 16 September 2021