energies

MDPI

Article

Factors Influencing the Threats for Urban Energy Networks: The Inhabitants' Point of View

Inna Čábelková [1], Wadim Strielkowski [1,*], Frank-Detlef Wende [2] and Raisa Krayneva [2]

[1] Department of Trade and Finance, Faculty of Economics and Management, Czech University of Life Sciences Prague, Kamýcká 129, Prague 6, 165 00 Prague, Czech Republic; cabelkova@pef.czu.cz

[2] Department of Logistics and Marketing, Faculty of Economics and Business, Financial University Under the Government of the Russian Federation, Leningradskiy Prospekt 55, Moscow 125993, Russia; FDVende@fa.ru (F.-D.W.); RKKrajneva@fa.ru (R.K.)

* Correspondence: strielkowski@pef.czu.cz

Received: 26 September 2020; Accepted: 27 October 2020; Published: 29 October 2020

Abstract: Our paper focuses on eliciting the factors that constitute threats and dangers for urban energy networks, information networks, and energy grids in the cities. Moreover, we attempt to determine how these threats are perceived by the inhabitants of those cities. Urban energy networks tend to play an increasing role in achieving energy efficiency and environmental sustainability in large urban centers. Even though they do not necessarily correspond to reality, public opinions can substantially influence the adoption of relevant technologies in populous urban locations. We use the public opinion representative survey data from the Czech Republic (a sample of 1023 respondents) in order to show how people perceive the dangers and threats for urban energy networks from such events as: (i) Extensive and long-term power outage; (ii) service disruption of the Internet, mobile networks or telephone landlines; (iii) cyber-attacks, and (iv) the technological dependence of the state on multinational technological companies. Our results demonstrate that people who live in small rural settlements and medium-sized cities tend to be more afraid of the threats and dangers from urban energy networks such as electricity and Internet outages, compared to people residing in some smaller towns. As far as there would always be a fear of the new technologies and their vulnerabilities, the local governments, mass media, and Internet resources alike should pay more attention to providing the relevant and updated information on the threats to urban energy networks for the general public.

Keywords: urban energy networks; energy grids; public opinion; urban networks; energy security

1. Introduction

Urban energy networks, information networks, and smart energy grids represent the key importance for the proper functioning of the modern cities and large urban centers ensuring their energy efficiency and environmental sustainability [1,2]. Yet, these networks and grids are subjected to a plethora of dangers and threats both imaginary and real, perceived by their inhabitants. A modern-day smart city can be viewed as a dwelling that employs smart lighting, electric transport, as well as smart sensors and similar technologies that utilize the data collected by sensors such as smart meters, and sensors on buildings and on the ground [3,4]. Today's cities are often dependent on extensive urban energy networks that often include renewable energy sources (RES) as well as novel solutions such as peer-to-peer (P2P) energy trading between prosumers alongside traditional carbon sources of energy [5–8]. At the same time, these urban energy networks might be vulnerable to all sorts of attacks and issues [9,10].

Any city that plans to use information technologies (IT) seeks to instrumentalize and integrate its infrastructure and services, to optimize these facilities and to use analytical tools to predict the city's energy consumption and energy consumption in the long term, as well as the effects of weather changes (see e.g., Ceglia et al. [11]). In the context of large urban centers where the city has no single owner for a plethora of services, integrating infrastructure and services into a common platform becomes a very complex task [12,13]. Most power grids around the world still rely on fossil fuels and obsolete infrastructure [14,15]. Smart networks, on the other hand, use the latest technology to meet demand and maximize efficiency [16,17]. With a smart grid, energy customers benefit from a more efficient electricity system, and utilities manage their electricity supply and productivity in a cost-effective way [18]. A utility's smart grid balances demand for electricity with supply. The adoption of smart grid technology is driving the increasing integration of energy systems around the world.

With regard to the above, the installation of distributed energy resources (DER) can prepare cities for a smarter future, but also give consumers greater control over their electricity consumption [19,20]. The solution could lie in the energy-efficient technologies offered by the Internet of Things (IoT).

There is great potential for smart meters, sensors and devices that can be connected together on the Internet of Energy (IoE) in a smart city, but this also makes these cities vulnerable for cyber-attacks and other threats.

While scarcity of key infrastructure resources continues to pose challenges for global cities and urban centers, smart urban technologies can help to improve their safety and resilience. Better connectivity between systems such as smart buildings, smart streets, and smart infrastructure would enable cities to move from "smart cities" to hyper-connected hubs. Various smart city projects would lead to a population of cities providing access to energy in a way that is sustainable for the economy, society, and the environment. This might allow cities to tap into the potential of smart infrastructure, smart buildings, and smart roads as well as energy security and connectivity.

Given all of that above, one would probably agree with us that all the smart energy projects are suitable for all the localities and that the governments should effectively differentiate the applicability of the projects for the locality including the perceptions of the population and the relative importance of the projects to the place from the point of view of both population and the local authorities. In a case when the project does not have the required domestic public support, the chances are high that its outcomes are not going to be used (neither maintained in the best-case scenario or actively destroyed in the worst-case one).

One of the factors that builds the public attitude to the new technological projects is the perceived threats of the technologies. This paper studies the factors influencing the threats for urban energy networks in smart cities from the point of view of inhabitants.

In this paper, we demonstrate that differences in town/city size, urban/rural is of immense importance for the energy (and all the other types of infrastructural) projects in any country (including the Czech Republic) as it is related to: (1) The quality of the existing energy (and other) infrastructure, and (2) the probability that the future infrastructure will be maintained. Less populous localities typically have poorer existing infrastructure, less public resources to build and maintain new ones, and cannot benefit from the economies of scale. In addition, often the location and the number of people living in this location defines the optimal technology. For example, in locations far from big cities and with few people, individual solar panels might be a more effective source of energy than the centralized entry transmitting systems. Given that in the Czech Republic many villages are located in the mountains, are hardly accessible in winter and the small number of people living there does not make profitable public/or private energy (or internet) infrastructure. In addition, in case of a damage caused by weather conditions, these localities need more resources per inhabitant and more time to fix this damage.

Our paper attempts to determine how the threats and dangers for urban energy networks, information networks and energy grids in the cities are viewed by their inhabitants using a unique representative sample from the Czech Republic, the EU Member State since 2004. Although the

perceptions of the public do not necessarily correspond to reality, this information appears to be crucial for the further promotion of the "smart city" concept and is likely to help the urban planners and policy makers in their endeavors. This becomes very important since the creation of carbon-free sustainable and energy sufficient smart cities became the priority of many countries and governments in the face of the impending global warming and climate change.

The paper is organized as follows: Section 2 outlines the hypotheses related to the perception of dangers and threats to the urban energy and information networks. Section 3 discusses the adequacy and importance of public opinion in technological innovations. Section 4 offers a comprehensive literature review on dangers and threats for smart city technologies in the view of public opinion. Section 5 describes materials and methods. Section 6 presents the empirical model. Section 7 demonstrates the results and provides the discussions of these results. Finally, Section 8 concludes the paper with outcomes, implications, and pathways for further research.

2. Research Hypotheses

Our paper studies the public perception of the four types of vulnerabilities for urban energy networks described above, namely: (i) Extensive and long-term power outage, (ii) long-term outage of the Internet, mobile networks or telephone, (iii) cybernetic, computer attack, and (iv) technological dependence of the state on multinational companies such as Huawei, Facebook, and Google. While the information about the first two can be obtained by the respondents from their own experience, the last two (cybernetic, computer attack, technological dependence of the state on multinational companies) represent a matter of technological and political discussion, which, most likely, the public will learn from other publicly available sources of information such as mass media, Internet, and social networks (or private discussions outside the Internet). Thus, we can formulate the following the following two hypotheses:

1. Perception of the four dangers and threats for urban energy networks is dependent on the size of the settlement the respondents live in;
2. Perception of the four dangers and threats for urban energy networks is contingent upon the exposition to the mass media and other sources of information that may form the opinion.

In the next sections of this paper, we will test these hypotheses using the representative public opinion data from the EU Member State represented hereinafter by the Czech Republic (the EU Member since 2004). Given that the ideas above are likely to be influenced by sociodemographic indicators of the respondents, we also control for age, gender, education, and the subjective standard of living.

3. The Role of Public Perceptions

Nowadays, public perceptions receive increasing attention as far as they can substantially influence the outcomes of governmental policies and technological innovations and have an increasing effect on sustainability of the results [21–23]. In the case of technological innovations financed by the governments, public perceptions can substantially influence whether the projects would have a financial priority and eventually receive the adequate funding. This holds true especially for the localized projects where the infrastructure can be built and financed by the local governmental bodies. Public perceptions and the general knowledge about the projects can substantially influence whether the outcome of the projects would be used by the public and whether they would not be damaged (for example by vandals). Public perceptions and public knowledge are even more important in the case of projects that can substantially influence the quality of life in a given location, attitude to the place they live in, and, eventually, the participation in public life.

However, more often the general public does not have adequate information about the project or technology which eventually can change people's lives. Naturally, most of them are not educated experts in the field and cannot rely on scientifically-proven information. Many of them do not have the adequate education, time, or willingness to collect relevant information even when it is

available, which, in many cases, is not so. Thus, the public is doomed to rely upon the personal experience, if available, or other accessible sources of information such as mass media, Internet, or social networks (both Internet-based on asynchronous). However, in personal experiences, a relevant source of information is rarely available and the stories about experiences of others transferred via social channels can be substantially blurred or changed. The other sources of information such as mass media can distort the information provided by selection of the topics, the style of presentation of information including creating emphases and presenting only some but not all points of view in an attempt to create sensations, either positive or negative ones [24–26].

In this paper, we focus on the public opinions on: (i) Extensive and long-term power outage; (ii) long-term outage of the Internet, mobile networks, or telephone; (iii) cybernetic, computer attack; and (iv) technological dependence of the state on multinational companies such as Huawei, Facebook, and Google. Obviously, the first two phenomena (power or Internet disruptions) represent the issues that one can have personal experience with or are frequently described in the mass media. The inhabitants of small villages are especially vulnerable to energy and Internet outage, since these types of settlements often possess poorer infrastructure and, as the density of the population is lower than in big cities, do not constitute a priority in case of sudden Internet outage. The third phenomenon (cybernetic or computer attack), is even less understandable for many people, as far as it requires to have a computer, frequently used in attacks. Thence, most of the population can get this information from the mass media or sources other than from personal experience. The last one (the dependence of the state on multinational companies), is a matter that does not directly concern the lives of citizens at all, so the only information they can find is in mass media or on the Internet. Both of these sources are vulnerable to disinformation especially in the times of "post-truth" society and given the economic competition between the corporations.

To summarize the arguments above, public opinion often relies upon highly unreliable sources of information. Thus, they do not necessarily correspond to reality. However, public opinions are extremely important especially in the case of technological innovations that can directly influence the quality of life in the localities as far as, in cases where they are not approved, people can efficiently stop or cancel these innovations. Therefore, they represent an extremely important issue for this study.

4. Dangers and Threats for Smart City Technologies in the View of Public Opinion

While the original aim of the smart cities technologies was to address the sustainability, uncertainty, and risks related to the quick urbanization and population increase, environmental change, and fiscal needs [27,28], they also present the newly created uncertainties, threats, and unintended consequences such as enhanced inequality, security and criminal risks, or environmental externalities on the society level [29–32] or technological vulnerabilities such as software imperfections and viruses, data errors, hacks, and criminal attacks on the hardware and software levels [33–37]. Our paper studies four of these threats and uncertainties: (i) Extensive and long-term power outage; (ii) long-term outage of the Internet, mobile networks or telephone; (iii) cybernetic, computer attack; and (iv) technological dependence of the state on multinational companies such as Huawei, Facebook, and Google from the point of view of the citizens as they have to approve and adopt to new city technologies.

The first and most obvious general public vulnerability of any electricity-based technology is the power outage. Currently, the majority of big cities and small villages have experienced a power outage at least once in their recent history. In large cities that are heavily based on electricity consuming technologies, power outage may cause detrimental consequences which are very visible for the general public (see Marx et al. [38] or Anderson and Bell [39] for the consequences of power outage in New York in August 2003; or Li et al. [40] for the Manhattan blackout in July 2019). In small villages or in locations with less resistant electricity networks, power outages might be even more and the costs might be enormous (see the studies by Akter [41] for the town of Dhaka in Bangladesh or Sun et al. [42] for the city of Shanghai in China). In any case, power outage is one of the problems to consider when enforcing smart city technologies. On the other hand, the technologies themselves may help to solve

the problem of power outage as one of their contributions is the distributed generation of power (see Ruiz-Romero et al. [43]) which may, if used correctly, stabilize the energy system especially in locations with less accessible or less secure centralized energy infrastructure.

The second vulnerability of the smart city technologies we focused upon in this paper is the long-term outage of the Internet, mobile networks, or telephone. As far as (as it was mentioned above) one of the main ideas of the smart cities is the Internet of Things [44,45] that can be accessed by the end user via mobile applications of smartphone [46,47] and effectively use the sensors located in phones or smart phones [48], the lack of Internet connection, mobile networks or telephone connections may efficiently shut down the system. This second vulnerability is also apparent to the general public as far as many people already experienced the lack of mobile phone signal in some locations (for example such as the subway lines in the Prague, a capital of the Czech Republic.).

Furthermore, we study public opinions on cybernetic or computer attacks as they represent the next important danger for the technologies used in smart cities. Contrary to the outage of energy, Internet or mobile phone signal, the danger of cyberattacks does not constitute the issue that the average person might have a personal experience with. The computer and energy grids of the smart cities are most vulnerable to cyber-attacks through many supervisory control and data acquisition (SCADA) systems that can be hacked and wirelessly controlled by hackers are widely used in infrastructure to control power substations and electric power flow through the grid [49]. Naturally, there are many more vulnerabilities and types of cyber-attacks (for classification see Garcia-Font et al. [50]), so the future smart cities need to build cybersecurity (Nautiyal et al. [51]).

The technological dependence of the state on multinational companies such as Huawei, Facebook, and Google might represent one of the types of risks smart city technologies, as any other type of technology, are vulnerable to. The grasp of the technological dependency may present a serious argument in political and economic life of the country and, in the worst case, may form the basis of extortion or blackmail of city- or country-level of political or financial elites [52–54].

In the light of the recent political events, there appeared serious concerns about Chinese technology giant Huawei supplying critical infrastructure for the next generation of the 5G mobile networks. The concerns were so serious that some countries refused to purchase this equipment, in others, it triggered off serious debates [55]. The continuous sophistication of Facebook and Google accompanied with the high potential to influence public opinion make these international corporations important players in the future development of the nations and smart cities [56–59].

Obviously, there are many more points of vulnerability of smart city technologies that are outside of the scope of this paper. For the sake of conciseness, we are going to limit ourselves to the four threats that were described above.

Smart city technologies usually fall into the domain of local communities and local politics, although they might be centrally coordinated. The cities on the different levels may adopt different goals, procedures, and outcomes of the smart city concept in their given location. In the Czech Republic, the cities, in terms of priorities of smart cities technologies, fall into three main clusters: (i) Large cities (above 150,000 inhabitants) perceive the smart city programs which are the communitarian programs that bring better quality of life as the main priority; (ii) cities over 40,000 inhabitants prefer to focus on transportation solutions; and (iii) cities having between 40,000 and 15,000 inhabitants concentrate more on smart lightning, parking availability, and management of traffic flow (see Maryska et al. [60]).

In general, one would probably agree that the efficient participation of the citizens at the smart city projects is one of the main pre-requisites for the success of any smart energy project (see Vácha, et al. [61]). The anecdotal evidence of the lack of participation in the Czech Republic comes from the Usti nad Labem, where extremely expensive smart benches priced at 60,000 Czech crowns (approximately 2400 EUR) were installed in the city park but were never used and were subsequently destroyed by the city vandals [62]. Similarly, the smart bench in Prague 6 district ceased to operate because no one took care of it [63]. Thus, it is important to monitor the public opinions on smart city projects which may vary according to the size and type of settlements. Beside the selection of smart city projects which is

dependent on the size of the city, the vulnerabilities of the energy grids in smart cities might become a factor that can shape up form public opinion and public support for these projects.

5. Materials and Methods

5.1. Participants and the Survey

The data used for the empirical model presented in this study was collected in June 2019 via the survey questionnaire conducted by the Czech Institute of Sociology [64]. A total of 1023 respondents (aged 15–92 years, $M \pm SD$: 47.59 ± 16.88; 18.8% with higher education, 51.30% women, Pearson correlation age-education 0.036, Sig. 0.252; higher education in women 18.9%; higher education in men 19.0%) completed the questionnaire voluntarily and anonymously under the supervision of 177 experienced interviewers. All participants of the study in question were residing in the Czech Republic. The method of sampling relied on representative sampling with quotes. The quotes included geographical position, age, gender, and education of the respondents. According to the quotes, the data sample is representative for the Czech Republic. The representativity was controlled for geographical position, age, gender, and education. The data was kindly provided by the Czech Social Science Data Archive for non-commercial use.

5.2. Indicators

Indicators of the Perceived Dangers

The questions on the perceived dangers were formulated in the following way:

"How big a threat do you think the following phenomena currently pose in the Czech Republic? Use a range from 0 to 10, where 0 means absolutely no threat and 10 absolutely vital threat:

- *Extensive and long-term power outage;*
- *long-term outage of the Internet, mobile networks or telephone;*
- *cybernetic, computer attack; and*
- *technological dependence of the state on multinational companies such as Huawei, Facebook, Google, etc."*

Obviously, this question represents a combination of two ideas: (1) How dangerous are the phenomena above in general, and (2) how important is the current and immediate danger. For example, people living in small hypothetical villages with no Internet connection and with a little use of electricity would not consider the Internet or electricity outage to be a danger, neither would they know much about cybernetic or computer attacks. On the other hand, people living in cities are heavily dependent on electricity and frequently use Internet. Thus, they may consider the outage of Internet and electricity to be extremely dangerous. Technologically advanced Internet users might have more knowledge of technological dependence and cyber-attacks. One could argue that these people are more concentrated in the main agglomerations and the big cities. However, there is also a trend to work from home (which became especially relevant during the COVID-19 pandemic and lockdowns) which might be located anywhere where they can have electricity and Internet, which, in the Czech Republic represent the area of almost the whole country except for some recreational locations in the mountains. While the relocation of technologically-advanced Internet users becomes a trend, one could also argue that given the speed of urbanization and intense migration of people to cities and bigger towns all over the world (including the Czech Republic), the idea that significant numbers of computer specialists live in villages might not be viable.

The second half of the interpretations of the questions above requires a discussion of whether the danger is real, and how acute it is in the Czech Republic at the moment. Here, the respondents may rely on possible personal experience (blackouts are very rare in the Czech Republic, are usually short-term

and caused by weather conditions), or the information from all available sources of information about the society level social life they may use such as mass media, Internet, and discussion groups. In this study, we cannot divide the question into these two parts presented above, thence we will analyze them simultaneously.

5.3. Data Transformations

The original encoding of the data on subjective dangers was conducted on the scale from 0 to 10 (0—no danger, 10—acute danger) which presented a problem of having very few respondents in some categories (3% and less). In order to increase the number of respondents in the categories, the data were recoded into 5 categories that are presented in the following table (see Table 1).

Table 1. Recoding of the variables representing dangers of extensive and long-term power outage, long-term outage of the Internet, mobile networks or telephone, cybernetic, computer attacks, technological dependence on multinational companies such as Huawei, Facebook, and Google.

Old Category	New Category	Interpretation
0, 1	1	No danger
2, 3	2	
4, 5, 6	3	
7, 8	4	
9, 10	5	Vital danger

Source: Own results.

This new coding preserves the symmetricity of data at the expense of the equal subjective width of the categories (the middle category 3 comprises three former categories, while the other new categories include only two of them). However, the ordinal regression analysis employed in the empirical part of this paper does not take into account the equality of the subjective sizes of the categories (the latter would be characteristic for interval data, not the ordinal ones) and only requires the ordinality of the categories in the sample. Thus, the recoding presented above can be considered plausible.

The alternative approach to employing this type of data would work with the variable ranging from 0 to 10 being a continuous variable and would employ linear regression analysis instead of the ordinal one. While some authors would resort for this solution, for the authors of this paper the idea of ordinality and possibly unequal distances even between the former categories characteristic for ordinal data presented a bigger problem when using the linear regression. Hence, the reduction of the number of categories was chosen. The resulting distribution of the respondents is presented in the following table (Table 2).

Table 2. The distribution of the respondents over 5 categories on the perceived dangers, (%).

Variable	1—No Danger	2	3	4	5—Vital Danger	Missing
Long term energy outage	13.2	27.2	32.9	14.5	8.0	4.2
Long term internet outage	13.2	26.1	33.3	14.2	6.5	6.7
Cyber-attacks, computer attacks	7.4	20.9	34.3	19.2	11.0	7.1
Technological dependence on transnational companies	6.2	14.6	35.4	20.7	13.4	9.8

Source: Own results.

From Table 2 it follows that long-term Internet and energy outage present similar subjective dangers for our representative sample of respondents from the Czech Republic as for the distribution of responses −21 to 22% of the respondents view them as rather vital or vital dangers. Computer attacks, cyber-attacks, and technological dependence on transnational companies present a bigger subjective danger −30 to 34% of the respondents view them as rather vital or vital dangers. Pearson correlation coefficients of perceived dangers are shown in Table 3 that follows.

Table 3. Pearson correlation coefficients of perceived dangers.

	Energy Outage	Internet Outage	Computer Attack
Internet outage	0.605 **		
Computer attack	0.500 **	0.666 **	
Technological dependence	0.269 **	0.276 **	0.322 **

Note: ** Correlation is significant at the 0.01 level (2-tailed). All the *p*-values were less than 0.000. Source: Own results From the Table 3 it follows that the perceived dangers are significantly correlated.

5.4. Indicators for Exposition to Mass Media and Other Sources of Information

Generally, exposure to the sources of information presented by mass media may mean several things. People follow mass media (including TV) in order to listen to music, watch movies, and visit social networks for communicating with their friends or for exposing bright parts of their lives to the sights of outer community, etc. All these activities do not represent what we usually define as mass media and others as a source of information about what is currently going on in society. Due to this reason, the question on the exposition to mass media and other sources of information were formulated in the following way: How often do you follow the issues relevant for society as a whole in the following media sources? For the full results see Table 4 that follows.

Table 4. Indicators—exposition to mass media and social discussion platforms when following social life. Frequency table (%).

How Often Do You Follow Social Life Via:	At Least Once a Day, %	Several Times a Week, %	Once a Week, %	Less than Once a Week, %	Never, %	Missing, %
TV	45.0	32.5	10.3	7.7	4.3	0.2
Printed newspapers and magazines	7.8	26.6	19.7	24.8	20.8	0.3
Radio	21.7	28.3	14.8	16.8	18.0	0.4
News webs on Internet	21.6	28.7	13.5	10.3	25.1	0.9
Internet discussions and blogs	7.1	14.3	12.7	16.6	48.1	1.2
Social networks (for example Facebook, Twitter, or Instagram	13.7	13.2	9.7	15.1	47.3	1.1
Discussions outside of Internet	6.3	19.1	19.2	26.5	27.8	1.1

Source: Own results.

From Table 4 it becomes quite clear that the most frequently watched media is, (as expected) TV which is followed by radio and news sources on the Internet. Printed newspapers and magazines together with Internet discussions and blogs including social networks represent the next three frequently followed sources of information. Quite surprisingly, almost 1/3 of the respondents never participate in the discussions outside the Internet.

5.5. Indicator of the Size of the Settlement

The question is formulated in the following way: "If you look at the IDE.19 (The card IDE.19 included: (1) Big city, (2) suburbs of a large city or seat in the immediate vicinity, (3) medium-sized city, (4) small town, (5) large village, (6) small village, settlement, solitude, (7) other type of seat, (8) does not know, (9) no answer, (10) denied to answer) card, how would you mark the place where you live?"

(1) Big city, (2) suburbs of a large city or seat in the immediate vicinity, (3) medium-sized city, (4) small town, (5) large village, (6) small village, settlement, solitude, (7) other type of seat

Due to small number of observations (less than 1.6%) in the category (2), the categories (1) and (2)—big cities and suburbs—were recoded as category 1. Similarly, we had to recode category (6) and (7), due to small number of observations in the category (7) (0.9%). The resulting distribution of the respondents is presented in Table 5.

Table 5. The distribution of the respondents in different sizes of settlements (%).

Town Size	Big City	Medium-Size City	Small Town	Large Village	Small Village	Missing
% of the respondents	28.6	23.2	25.5	10.8	11.3	0.5

Source: Own results.

5.6. Socio-Demographic Indicators

We control for age, education and gender, and the subjective standard of living of the household. The question for the latter was formulated as the following (in parenthesis we present the distribution of the respondents): Do you consider the standard of living of your household as: 1. Very good (8.4%), 2. rather good (44.7%), 3. neither good nor bad (36.6%), 4. rather bad (8.9%), 5. very bad (1.3%)?

6. Empirical Model

6.1. Methods of Analysis

In order to study the differences in the perceived dangers to urban energy networks with respect to the size of the settlement the respondent lives in, we employ a one-dimensional ANOVA analysis with LSD post-hoc tests and ordinal regression analysis. The ANOVA enables to study the differences between all the pairs of possible sizes of settlements. In its turn, the ordinal multinomial regression analysis enables us to filter out the effects of the third variables.

ANOVA Analysis

The results of the ANOVA analysis (the perceived dangers with respect to the subjective town size) are presented in Figure 1 that follows.

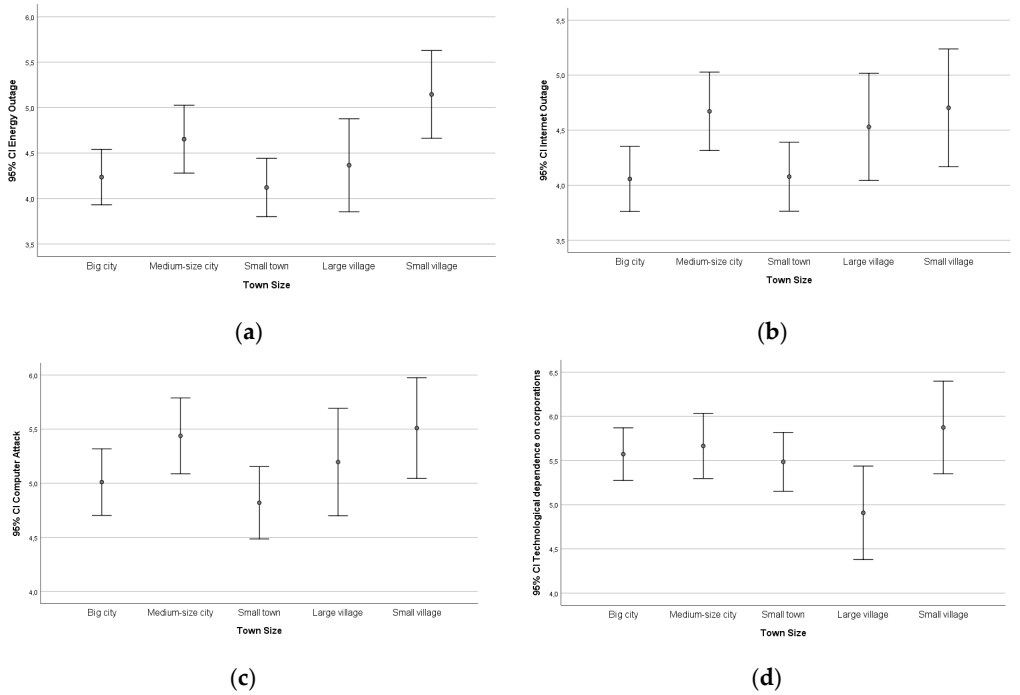

Figure 1. The perceived dangers with respect to the subjective town size. Means and confidence intervals. (**a**) Means and 95% confidence intervals for energy outage versus town size; (**b**) means and 95% confidence intervals for Internet outage versus town size; (**c**) means and 95% confidence intervals for computer attack versus town size; and (**d**) means and 95% confidence intervals for technological dependence versus town size. Source: Own results.

One can note that for the graphs above the original variables ranged from 0 to 10 for the perceived dangers were used. Thus, some upper boards of confidence intervals are above 6 (the transformed variable ranges from 1 to 5). Levene variance test failed to reject the similarity in variances across the categories. Thus, we can use the p-values of tests that follow that assume that there were no significant differences in variances.

From the Figure 1 it follows that small village and medium-size city both seem to differ from some other sizes of settlements. In order to study the statistical significance of the differences, the one-dimensional ANOVA analysis with LSD Post-Hoc tests were conducted. As a result, ANOVA Sig. for the mean differences equal to: For Energy Outage 0.003; for Internet Outage 0.0016; for Computer Attack 0.128; and for Technological dependence on corporations 0.058. Thus, there is statistical difference between the categories of town size in the case of energy and internet outage on 5% significance levels. The danger of technological dependence was on the edge of statistical difference (Sig = 0.058).

Here, we do not present the results of post hoc tests for the dangers of computer attacks and technological dependence as the ANOVA Sig. for these two variables were above the significance levels (greater than 0.05). Levene variance test failed to reject that there were no differences in variances across the categories.

The results of post hoc tests presented in Table 6 support the significant differences between the respondents living in the towns (villages or cities) of different sizes. From the one-dimensional ANOVA it follows that the relationship of the perceived dangers and the size of the cities is not uniform or linear. Specifically, the following conclusions can be made:

- People living in big cities are less afraid of Internet and electricity outage than people living in medium-sized cities;
- People living in small towns are less afraid of Internet and electricity outage than people living in medium sized towns;
- People living in the small towns are less afraid of Internet and electricity outage than people living in small village;
- People living in large village are less afraid of electricity outage than people living in small village; and
- People living in small village are more afraid of Internet and electricity outage than people living in big cities and small towns.

In other words, the people who are most afraid of electricity and Internet outage tend to live in small villages (the smallest category of settlements) and medium-sized cities compared to people living in some but not all town sizes.

While the reasons of people living in small villages being afraid these things are obvious (these settlements are usually in locations that are more difficult to reach and, due to lower number of inhabitants, have worse access to the infrastructure), the reasons behind worries of people from medium-size cities are less clear. Except for the phenomenon of the middle-sized city, the total trend seems to yield more worries in smaller cities.

The above analysis highlighted the main trends of the relation of the subjective town size the respondents live in and the perceived dangers of long-term energy outage, long-term Internet outage, cyber-attacks, computer attacks, and technological dependence on transnational companies. However, the analysis above did not consider the differences between the people living in the different sized settlements. The model presented in the next section relieves this limitation.

Table 6. Results of LSD post hoc tests. Sig. of the differences in the perceived danger of energy and Internet outage between the categories of town size.

		Energy Outage		Internet Outage	
		Mean Difference	**Sig.**	**Mean Difference**	**Sig.**
Big City	Medium-size city	−0.203 *	0.041	−0.278 **	0.004
	Small town	0.022	0.821	−0.049	0.605
	Large village	−0.084	0.515	−0.174	0.169
	Small village	−0.414 **	0.001	−0.305 *	0.016
Medium-size city	Big City	0.203 *	0.041	0.278 **	0.004
	Small town	0.225 *	0.027	0.228 *	0.023
	Large village	0.120	0.370	0.104	0.428
	Small village	−0.211	0.105	−0.027	0.836
Small town	Big City	−0.022	0.821	0.049	0.605
	Medium-size city	−0.225 *	0.027	−0.228 *	0.023
	Large village	−0.106	0.419	−0.125	0.333
	Small village	−0.436 **	0.001	−0.256 *	0.047
Large village	Big City	0.084	0.515	0.174	0.169
	Medium-size city	−0.120	0.370	-e0.104	0.428
	Small town	0.106	0.419	0.125	0.333
	Small village	−0.330 *	0.032	−0.131	0.394
Small village	Big City	0.414 **	0.001	0.305 *	0.016
	Medium-size city	0.211	0.105	0.027	0.836
	Small town	0.436 **	0.001	0.256 *	0.047
	Large village	0.330	0.032	0.131	0.394

Note: ** Significant at the 0.01 level (2-tailed).* Significant at the 0.05 level (2-tailed), Source: Own results.

6.2. Ordinal Regressions

We computed a set of ordinal multinomial regression analyses with the purpose to study the factors associated with the levels of perceived dangers that include: (1) Extensive and long-term power outage, (2) long-term outage of the Internet, mobile networks or telephone, (3) cybernetic, computer attack, (4) technological dependence of the state on multinational companies such as Huawei, Facebook, and Google. The main model is presented below (Formula (1)). This model was computed four times for different indicators of threats and dangers using the following Formula (1):

$$Danger_i = logit\ (a_0 + a_{1\text{-}7}Info + a_{8\text{-}11}TownSize + a_{12}StLiv + a_{13}Age + a_{14}Gender + a_{15}Edu + \xi \quad (1)$$

where:

$Danger_i$ stands for the answers to one of the following questions:

How big a threat do you think the following phenomena currently pose in the Czech Republic? (1) Extensive and long-term power outage, (2) long-term outage of the Internet, mobile networks or telephone, (3) cybernetic, computer attack, and (4) technological dependence of the state on multinational companies such as Huawei, Facebook, and Google.

Info—stands for the exposition to the country level social life in the mass media and other sources of information (TV, printed newspapers and magazines, radio, news webs on internet, Internet discussions and blogs, social networks, and discussions outside of Internet);

TownSize—town size dummies for: (1) Big city; (2) medium-size city; (3) small town; (4) large village; and (5) small village. The ordinal variable *TownSize* was split into 5 dummies for different types of the settlements the respondents live in. Small village dummy was omitted and used as a reference variable.

StLiv—Subjective standard of living

Age, Gender, Edu—age, gender, and education.

7. Results and Discussions

The results of ordinal regression analyses that was carried out in accordance with the empirical model described above are presented in Table 7.

Table 7. The results of ordinal regression analysis for the factors associated with perceived dangers of energy outage, Internet outage, computer attacks and technological dependence of multinational corporations.

	Energy Outage		**Internet Outage**		**Computer Attack**		**Technological Dependence**	
	Estimate	**Sig.**	**Estimate**	**Sig.**	**Estimate**	**Sig.**	**Estimate**	**Sig.**
Threshold = 1	−2.466 ***	0.000	−3.146 ***	0.000	−3.763 ***	0.000	−2.065 ***	0.000
Threshold = 2	−0.875 *	0.032	−1.572 ***	0.000	−2.094 ***	0.000	−0.663	0.118
Threshold = 3	0.715	0.079	0.095	0.819	−0.461	0.265	1.115 **	0.009
Threshold = 4	1.921 ***	0.000	1.511 ***	0.000	0.842 *	0.044	2.405 ***	0.000
Sources of information								
TV	0.055	0.390	−0.163 *	0.014	0.020	0.753	0.001	0.989
Printed newspapers and magazines	−0.132*	0.018	−0.093	0.103	−0.058	0.304	0.181 *	0.002
Radio	−0.026	0.592	0.004	0.939	−0.078	0.115	−0.054	0.287
News servers on internet	0.010	0.852	−0.065	0.238	−0.112 *	0.042	−0.097	0.085
Internet discussions and blogs	−0.167*	0.014	−0.283 ***	0.000	−0.092	0.176	0.013	0.849
Social networks (for example Facebook, Twitter, or Instagram	0.116	0.054	0.188 **	0.002	0.107	0.074	−0.041	0.503
Discussions outside of Internet	0.062	0.256	0.089	0.108	−0.083	0.136	0.042	0.456
Subjective size of the settlement								
Big city	−0.696 **	0.001	−0.462 *	0.031	−0.351	0.096	−0.139	0.526
Medium-size city	−0.371	0.084	−0.093	0.673	−0.062	0.777	−0.052	0.820
Small town	−0.803 ***	0.000	−0.399	0.066	−0.421 *	0.050	−0.209	0.350
Large village	−0.560 *	0.026	−0.168	0.514	−0.262	0.302	−0.605 *	0.022
Socio-demographics								
Age	−0.003	0.441	−0.014 **	0.002	−0.010 *	0.024	0.002	0.635
Standard of living of the household	0.284 ***	0.000	0.219 **	0.006	0.144	0.067	0.167 *	0.037
Gender (man)	−0.169	0.158	0.002	0.986	−0.090	0.456	−0.139	0.259
Education elementary	−0.215	0.357	0.296	0.214	0.206	0.392	0.137	0.576
Education secondary w/o state exam	−0.105	0.548	−0.071	0.685	0.056	0.750	0.091	0.610
Education secondary with state exam	−0.079	0.640	0.012	0.942	0.232	0.168	0.206	0.227
R^2, model significance and number of observations								
R^2 Cox and Snell	0.047		0.065		0.045		0.034	
R^2 Nagelkerke	0.050		0.069		0.047		0.036	
R^2 McFadden	0.016		0.023		0.015		0.012	
Sig.		0.000		0.000		0.001		0.021
N	944		918		915		889	

Note: Ordinal regression, link function logit. *** Significant at the 0.001 level (2-tailed). ** Significant at the 0.01 level (2-tailed). * Significant at the 0.05 level (2-tailed). Reference variables: Women, higher education, small village. The thresholds are 1 through 4 and they represent the analogue to intercepts in linear regression, the points where the respondents may be assigned to the next category in ordinal dependent variable. Given that dependent variable reaches 5 different outcomes, there are four thresholds from each of which the predicted value of dependent variable, which is continuous in logit function, is assigned to the next discreet value of the ordinal dependent variable which is discrete. Source: Own results.

7.1. Size of the City vs. Perceived Dangers

- The effect of the size of the city on the perceived dangers is most visible in the case of energy outage. Here, respondents living in big cities small towns and large villages perceive the energy outage as less vital danger compared to villages.
- Similarly, people living in big cities are less afraid of Internet outage compared to small villages.
- People living in small towns are less afraid of cyber-attacks than people living in small villages. This result does not correspond with the results of ANOVA analysis presented above as far as the ANOVA analysis did not find significant differences in the fear of commuter attacks with respect to the town size. However, the "no significant difference" statistical outcome does not necessarily mean that there is not difference, but just that no difference was shown by our method and data. In addition, ANOVA analysis did not control for the sources of information and socio-demographic variables.
- People living in large villages are less afraid of technological dependence of multinational corporations than people living in small villages. Similarly to the previous case, this result does not correspond to the ANOVA analysis presented above, as far as in ANOVA we did not find significant differences between the categories of the settlements. Similar notes as in the previous case apply.

7.2. The Mass Media and Other Sources of Information

- The more the respondents watch TV, the more they believe that Internet outage represents a vital danger.
- The more the respondents read printed newspapers and magazines, the more they believe that energy outage is a vital danger and the less they consider technological dependence on the corporation is a vital danger.
- The more the respondents use news servers on the Internet as a source of information about social life, the more they believe that computer attack poses a vital danger.
- Internet discussion groups and blogs seem to evoke negative expectations on the energy and internet outage—the more people use them, the more they feel endangered by the energy and Internet outage. The interpretation may be very simple and need not necessarily concern the content that the respondents read or watch. The sole fact that the Internet or electricity outage might disable them from using this information channel (Internet discussions and blogs) is likely to make them more fearful of the disruption of electricity or Internet.
- In the light of the previous result, it seems surprising that people using social networks (such as Facebook or Instagram) are likely to see less danger in Internet outage (the energy outage is at the edge of significance, but, if significant the relationship would be also positive). We offer three explanations for this phenomenon. The first is that social networks attract certain types of people who are generally less worried as for what may happen. Actually, 47% of our respondents never use social networks (see Table 4). Secondly, given the relative stability of access to social networks, they might not have an experience of not being able to access them. Thirdly, the content they follow there is in many cases positive and aimed at showing off, which disables these sources of information from presenting more serious ideas that might case something dangerous to happen.

As far as, most likely, few people have personal experience with the threats to urban energy and information networks, the role of mass media is alarming. All of the traditional mass media increases the feeling of dangers of some of the phenomena above (while the role of social networks such as Facebook is positive). Two interpretations are possible. Either people following traditional mass media have a higher felling of danger in general (as the media are likely to provide negative information about the outer world in order to create sensation), or the content of the media directly related to the dangers above creates these feelings of acute dangers. As it was shown in the previous sections, 30% to

34% of the respondents view computer, cyber-attacks, and technological dependence on transnational companies as representing danger or vital danger (the numbers for Internet and electricity outages are 21% to 22% respectfully). In any case, public acceptance of new technologies, such as energy grids, can be highly damaged by the non-adequate feelings of dangers created by the media. Obviously, public policies need to be designed in order to change that perception.

We suggest that public policies should concentrate on creating a positive image of the energy grids and other smart city technologies via global and local information channels in order to overcome the fears that may already have been created in mass media. Namely, we suggest the following steps to be undertaken:

- Creating mass media campaigns that would stress that local energy grids and internet hot spots, especially in small cities, can partly alleviate the danger of energy and Internet outage.
- Locating these campaigns in the non-specialized sections of mass and other media intended for the general public, as often technological innovations are discussed in special sections devoted to new technologies which reduces the audience interested in the new technologies.
- Conveying information on new technologies in the form of how they can solve the existing problems of localities and enhance standard of living in the localities instead of presenting the technological peculiarities of innovations.
- Concentrating on the needs of large and small cities located in different regions, as far as they are likely to differ and unformal media campaign cannot suffice. If possible, it is important to address the most vital problem of the concrete locality. For example, in an anecdotal example mentioned before, where vandals, mostly belonging to the ethnic minority, had a tendency to destroy the smart benches in Usti region in the Czech Republic, it would be necessary to find a way of avoiding that. As far as this ethnic minority is more concentrated in this particular region, other regions do not necessarily need to use the same tactics.
- In order to achieve all of the above, an intense communication between the central and the local governments is necessary for determining the central and local needs and peculiarities that can be addressed by the smart greed technology and the other new technologies belonging to the family of smart city technologies.

7.3. Sociodemographic Indicators

Concerning the sociodemographic indicators, the following results were obtained:

- The higher is the age of the respondents, the lower is perceived danger of Internet outage and computer attack.
- The higher is the subjective standard to living, the less danger the respondents see in energy outage, Internet outage, and technological dependence on corporations.

From the results of the ordinal regression above it follows that two most important worries of respondents from the small villages are energy outages and the Internet outages. Here, it seems reasonable to create smart city projects that are aimed at suppressing these worries such as additional energy or Internet producing units that are independent of the central energy supply. On the other hand, the results of the worry of the dependence on multinational corporation and computer attacks than in some other types of settlements may represent a more general distrust to modern technologies than in the small villages also need to be addressed [65,66]. Our results support the differences in the perception of smart city programs depending on the size of the city in the Czech Republic presented in similar studies (see e.g., [60,61]).

The public mass media and Internet discussion groups do not execute a good job with regard to the above, as far as people frequently following them perceive most of the vulnerabilities above as more vital dangers. However, social networks such as Facebook or Instagram, seem to diminish the perceived danger of the energy and Internet outage. This finding may correspond to a specific

group of people engaging in these social networks which form approximately 50% of our respondents (47% of the respondents never use social networks) and the overall positivity of the information presented there (people mostly use social networks to brag about their achievements and not to discuss serious issues).

The negative relationship of the perceived dangers with age (the higher in the age the lower is the worry of Internet outage and computer attack) may be caused by the less frequent use of the Internet by the older respondents., Therefore, this means less dependence on the Internet and its contents.

The negative relationship of the perceived dangers to urban energy and information networks with the standard of living (better standard of living means less perceived danger) is surprising, as far as people with higher standard of living are more likely to be equipped with computers and to use Internet-based technologies.

8. Conclusions and Implications

Overall, public perceptions of new technologies represent an important aspect that may be crucial for the successful implementations of new technologies including urban energy networks. The lack of public acceptance may cause lack of use, lack of maintenance of new equipment (in the best case) or active destruction of the technologies (in the worst case). Public perceptions differ across the country, which, among other factors, questions the applicability of the universal technology for all the locations. The size of agglomeration seems to be the one of the most important factors that defines the perceptions of electricity technologies including the urban energy networks in the Czech Republic. The populations of the small towns and especially villages, some of which are located in mountains far from the energy centers may differ in their perceptions of energy networks from the big populated central cities. Less populated locations are usually less endowed with the resources necessary to build and maintain the infrastructural projects including the energy networks. Moreover, they usually have poorer existing infrastructure of both the energy and the Internet connection. They are the last to have the access to the internet as for the commercial providers, they require large investments to bring the internet (and electricity for the electricity providers) to the locality. They have longer electricity distribution lines that are vulnerable to the break downs because of the weather conditions. They are also the last to receive help and support in the case of a more extensive blackout simply because there are fewer people living there. All these factors, plus the influence of the mass media and other Internet resources, shift their perceptions of dangers of the new energy technologies to the negative side. This shift, if large enough, can eventually disable the success of these technologies in these localities. Our results showed the differences in perceived dangers of energy networks depending on the size of the agglomeration.

All in all, our results demonstrate that more worries about the threats and dangers for urban energy networks, information networks, and energy grids are manifested by the inhabitants of rural settlements and small towns rather than by the people residing in large cities and city agglomerations.

While the reasons of perceived threats for people living in small villages are obvious (these settlements are usually situated in the locations that are more difficult to reach and due to the lower number of inhabitants typically have worse access to the infrastructure), the reasons behind the fears of people originating from the medium-size cities are less clear. However, it has to be noted that except for the phenomenon of the middle-sized city, the total trend seems to reveal the existence of more fears of the potential threats to the urban energy and communication networks in smaller cities. It becomes clear that the smart city projects targeted at the small cities (e.g., important university towns with a focus on biotechnologies and start-ups) should concentrate on the creation of the new energy grids which, ideally, would be independent on centrally supplied electricity and on the provision of the new stable and reliable Internet grid possibly offered via the Wi-Fi hotspots or other available technologies. This is an important outcome since some smaller cities often become important hubs for the development of technological and research advancements (for example, university towns of Cambridge, Oxford, or Berkeley).

Furthermore, mass media (both traditional outlets and those operating on the Internet) do not seem to relieve the worries of threats and dangers to urban energy and information networks, as far as people frequently following them tend to perceive the dangers and threats to be more vital. In addition, the use of social media, such as Facebook or Instagram, relieves these worries which may be related to the self-selection of people using them and the overall positive mood of showing off in these media.

The negative role of mass media that increases citizens' worries about the smart city and other related technologies may originate from the two sources. The first one is the overall level of negativity of the media which comes from the attempt to create sensation of any kind that may increase the worries of the audience in general. Secondly, the content directly related to the new smart-city related technologies, Internet, and energy provision may create specific threats, some of which are discussed in this paper. One could not avoid that in the democratic environment. However, local and state authorities can work on the positive image of new technologies to overcome these negative worries. The policy recommendations we might suggest include the placement of positive messages to the sections devoted to the general public (as opposed to the sections of mass media devoted to new technologies), discussion of new media from the point of view of how it can increase the quality of life and solve the troublesome issues existing in localities and for the people living there (as opposed to discussing the technological peculiarities of the technologies), adaptation of the message to the locations as different locations have different needs and issues that can be solved, and distinguishing the central and local level of information which require the communication of the central and local governments (some benefits of the technologies in questions hold for the whole country, while others are localized).

Today, the resilience of urban energy supply becomes a crucial component of the long-term resilience of the energy system to climate change and other threats. Understanding the new emerging interactions and threats in the smart cities is going to be of enormous importance when considering the future structure of urban energy grids. In this context, alternative coordination strategies are being explored aimed at improving the resilience of the urban energy systems. Modern resilience of utilities becomes the basis for developing a more resilient urban energy system and a better understanding of the impacts of climate change. Researchers should start developing new tools, methods, and analyses in order to optimize the use of decentralized energy in urban energy systems and to enhance their management. Given the complexity of the global energy system and the potential for climate change, flexible and adaptable solutions are needed for the threats to be promptly identified and prevented.

When it comes to the pathways for further research, it might be interesting to obtain similar (or comparable) data on how people perceive the dangers and threats for urban energy and information networks in other countries and regions and to run a cross-country comparison. We assume that various differences might emerge based on the size of the specific urban centers, the level of infrastructure development, as well as on the familiarity with the novel technologies and approaches. Overall, our results might be of a special interest for urban planners, stakeholders and policymakers, as well as for the law enforcement agencies and the academic research communities specializing in urban energy networks and energy economics and policy.

Author Contributions: Conceptualization, I.Č., W.S., F.-D.W., and R.K.; methodology, I.Č. and W.S.; validation F.-D.W., and R.K.; formal analysis, I.Č., W.S., F.-D.W., and R.K.; investigation, I.Č. and F.-D.W.; resources, F.-D.W., W.S., and R.K.; data curation, I.Č.; writing—original draft preparation, I.Č., W.S., F.-D.W., and R.K.; supervision, I.Č., W.S., F.-D.W., and R.K.; project administration, I.Č. and W.S. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

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

References

1. Becker, S.; Angel, J.; Naumann, M. Energy democracy as the right to the city: Urban energy struggles in Berlin and London. *Environ. Plan. A Econ. Space* **2020**, *52*, 1093–1111. [CrossRef]
2. Liu, W.; Song, Z. Review of studies on the resilience of urban critical infrastructure networks. *Reliab. Eng. Syst. Saf.* **2020**, *193*, 106617. [CrossRef]
3. Strielkowski, W.; Veinbender, T.; Tvaronavičienė, M.; Lace, N. Economic efficiency and energy security of smart cities. *Econ. Res. Ekon. Istraživanja* **2020**, *33*, 788–803. [CrossRef]
4. Yan, J.; Liu, J.; Tseng, F.M. An evaluation system based on the self-organizing system framework of smart cities: A case study of smart transportation systems in China. *Technol. Forecast. Soc. Chang.* **2020**, *153*, 119371. [CrossRef]
5. Shrestha, A.; Bishwokarma, R.; Chapagain, A.; Banjara, S.; Aryal, S.; Mali, B.; Korba, P. Peer-to-peer energy trading in micro/mini-grids for local energy communities: A review and case study of Nepal. *IEEE Access* **2019**, *7*, 131911–131928. [CrossRef]
6. Strielkowski, W. *Social Impacts of Smart Grids: The Future of the Smart Grids and Energy Market Design*, 1st ed.; Elsevier: London, UK, 2019; 342p.
7. Delponte, I.; Schenone, C. RES Implementation in Urban Areas: An Updated Overview. *Sustainability* **2020**, *12*, 382. [CrossRef]
8. Reihani, E.; Siano, P.; Genova, M. A New Method for Peer-to-Peer Energy Exchange in Distribution Grids. *Energies* **2020**, *13*, 799. [CrossRef]
9. Wang, F.; Zheng, X.Z.; Li, N.; Shen, X. Systemic vulnerability assessment of urban water distribution networks considering failure scenario uncertainty. *Int. J. Crit. Infrastruct. Prot.* **2019**, *26*, 100299. [CrossRef]
10. Che, Y.; Jia, J.; Zhao, Y.; He, D.; Cao, T. Vulnerability assessment of urban power grid based on combination evaluation. *Saf. Sci.* **2019**, *113*, 144–153. [CrossRef]
11. Ceglia, F.; Esposito, P.; Marrasso, E.; Sasso, M. From smart energy community to smart energy municipalities: Literature review, agendas and pathways. *J. Clean. Prod.* **2020**, *254*, 120118. [CrossRef]
12. Agbali, M.; Trillo, C.; Ibrahim, I.A.; Arayici, Y.; Fernando, T. Are smart innovation ecosystems really seeking to meet citizens' needs? Insights from the stakeholders' vision on smart city strategy implementation. *Smart Cities* **2019**, *2*, 19. [CrossRef]
13. Bibri, S.E.; Krogstie, J. The emerging data–driven Smart City and its innovative applied solutions for sustainability: The cases of London and Barcelona. *Energy Inform.* **2020**, *3*, 1–42. [CrossRef]
14. Fadly, D. Low-carbon transition: Private sector investment in renewable energy projects in developing countries. *World Dev.* **2019**, *122*, 552–569. [CrossRef]
15. Bahrami, A.; Teimourian, A.; Okoye, C.O.; Shiri, H. Technical and economic analysis of wind energy potential in Uzbekistan. *J. Clean. Prod.* **2019**, *223*, 801–814. [CrossRef]
16. Hui, H.; Ding, Y.; Shi, Q.; Li, F.; Song, Y.; Yan, J. 5G network-based Internet of Things for demand response in smart grid: A survey on application potential. *Appl. Energy* **2020**, *257*, 113972. [CrossRef]
17. Al Ridhawi, I.; Otoum, S.; Aloqaily, M.; Jararweh, Y.; Baker, T. Providing secure and reliable communication for next generation networks in smart cities. *Sustain. Cities Soc.* **2020**, *56*, 102080. [CrossRef]
18. Alaqeel, T.A.; Suryanarayanan, S. A comprehensive cost-benefit analysis of the penetration of Smart Grid technologies in the Saudi Arabian electricity infrastructure. *Util. Policy* **2019**, *60*, 100933. [CrossRef]
19. Lind, L.; Cossent, R.; Chaves-Ávila, J.P.; Gómez San Román, T. Transmission and distribution coordination in power systems with high shares of distributed energy resources providing balancing and congestion management services. *Wiley Interdiscip. Rev. Energy Environ.* **2019**, *8*, e357. [CrossRef]
20. Ali, S.S.; Choi, B.J. State-of-the-Art Artificial Intelligence Techniques for Distributed Smart Grids: A Review. *Electronics* **2020**, *9*, 1030. [CrossRef]
21. Čábelková, I.; Strielkowski, W.; Firsova, I.; Korovushkina, M. Public Acceptance of Renewable Energy Sources: A case study from the Czech Republic. *Energies* **2020**, *13*, 1742. [CrossRef]
22. Rajapaksa, D.; Islam, M.; Managi, S. Pro-environmental behavior: The role of public perception in infrastructure and the social factors for sustainable development. *Sustainability* **2018**, *10*, 937. [CrossRef]
23. Van Zoonen, L. Privacy concerns in smart cities. *Gov. Inf. Q.* **2016**, *33*, 472–480. [CrossRef]
24. Van Dijk, T.A. *Discourse and Communication: New Approaches to the Analysis of Mass Media Discourse and Communication*; Walter de Gruyter Publishing: Berlin, Germany, 2011; Volume 10, p. 375.

25. DeVreese, C.H.; Boomgaarden, H.G. Media message flows and interpersonal communication: The conditional nature of efects on public opinion. *Commun. Res.* **2006**, *33*, 19–37. [CrossRef]
26. Murphy, J.; Link, M.W.; Childs, J.H.; Tesfaye, C.L.; Dean, E.; Stern, M.; Pasek, J.; Cohen, J.; Callegaro, J.; Harwood, P. Social media in public opinion research: Executive summary of the aapor task force on emerging technologies in public opinion research. *Public Opin. Q.* **2014**, *78*, 788–794. [CrossRef]
27. Söderström, O.; Paasche, T.; Klauser, F. Smart cities as corporate storytelling. *City* **2014**, *18*, 307–320. [CrossRef]
28. White, J.M. Anticipatory logics of the smart city's global imaginary. *Urban Geogr.* **2016**, *37*, 572–589. [CrossRef]
29. Datta, A. New urban utopias of postcolonial India: 'Entrepreneurial urbanization' in Dholera smart city, Gujarat. *Dialogues Hum. Geogr.* **2015**, *5*, 3–22. [CrossRef]
30. Greenfield, A. *Against the Smart City: A Pamphlet. This Is Part I of "The City is Here to Use"*; Do Projects Publishing: New York, NY, USA, 2013; 147p.
31. Singh, I.B.; Pelton, J.N. Securing the cyber city of the future. *Future* **2013**, *47*, 22.
32. Townsend, A.M. *Smart Cities: Big Data, Civic Hackers, and the Quest for a New Utopia*; WW Norton & Company: New York, NY, USA, 2013; 400p.
33. Kitchin, R.; Dodge, M. The (in) security of smart cities: Vulnerabilities, risks, mitigation, and prevention. *J. Urban Technol.* **2019**, *26*, 47–65. [CrossRef]
34. Little, R.G. Managing the risk of cascading failure in complex urban infrastructures. In *Disrupted Cities*; Routledge: London, UK, 2010; pp. 39–52. 19p.
35. Kitchin, R.; Dodge, M. *Code/Space: Software and Everyday Life*; MIT Press: Cambridge, MA, USA, 2011; 290p.
36. Cerrudo, C. An emerging US (and world) threat: Cities wide open to cyber attacks. *Secur. Smart Cities* **2015**, *17*, 137–151.
37. Yigitcanlar, T.; Kamruzzaman, M.; Foth, M.; Sabatini-Marques, J.; da Costa, E.; Ioppolo, G. Can cities become smart without being sustainable? A systematic review of the literature. *Sustain. Cities Soc.* **2019**, *45*, 348–365. [CrossRef]
38. Marx, M.A.; Rodriguez, C.V.; Greenko, J.; Das, D.; Heffernan, R.; Karpati, A.M.; Weiss, D. Diarrheal illness detected through syndromic surveillance after a massive power outage: New York City, August 2003. *Am. J. Public Health* **2006**, *96*, 547–553. [CrossRef] [PubMed]
39. Anderson, G.B.; Bell, M.L. Lights out: Impact of the August 2003 power outage on mortality in New York, NY. *Epidemiology* **2012**, *23*, 189–193. [CrossRef] [PubMed]
40. Li, L.; Ma, Z.; Cao, T. Leveraging social media data to study the community resilience of New York City to 2019 power outage. *Int. J. Disaster Risk Reduct.* **2020**, 101776. [CrossRef]
41. Akter, S. Understanding the power outage cost of residential consumers in the city of Dhaka. *South Asian J. Manag.* **2008**, *15*, 64.
42. Sun, T.; Wang, X.; Ma, X. Relationship between the economic cost and the reliability of the electric power supply system in city: A case in Shanghai of China. *Appl. Energy* **2009**, *86*, 2262–2267. [CrossRef]
43. Ruiz-Romero, S.; Colmenar-Santos, A.; Mur-Pérez, F.; López-Rey, Á. Integration of distributed generation in the power distribution network: The need for smart grid control systems, communication and equipment for a smart city-use cases. *Renew. Sustain. Energy Rev.* **2014**, *38*, 223–234. [CrossRef]
44. Jiang, D. The construction of smart city information system based on the internet of Things and cloud computing. *Comput. Commun.* **2020**, *150*, 158–166. [CrossRef]
45. Jin, J.; Gubbi, J.; Marusic, S.; Palaniswami, M. An information framework for creating a smart city through internet of things. *IEEE Internet Things J.* **2014**, *1*, 112–121. [CrossRef]
46. Jalali, R.; El-Khatib, K.; McGregor, C. Smart city architecture for community level services through the internet of things. In Proceedings of the IEEE 2015 18th International Conference on Intelligence in Next Generation Networks, Paris, France, 17–19 February 2015; pp. 108–113.
47. Losavio, M.M.; Chow, K.P.; Koltay, A.; James, J. The Internet of Things and the Smart City: Legal challenges with digital forensics, privacy, and security. *Secur. Priv.* **2018**, *1*, e23. [CrossRef]
48. Sanchez, L.; Muñoz, L.; Galache, J.A.; Sotres, P.; Santana, J.R.; Gutierrez, V.; Pfisterer, D. SmartSantander: IoT experimentation over a smart city testbed. *Comput. Netw.* **2014**, *61*, 217–238. [CrossRef]
49. Gunduz, M.Z.; Das, R. Cyber-security on smart grid: Threats and potential solutions. *Comput. Netw.* **2020**, *169*, 107094. [CrossRef]
50. Garcia-Font, V.; Garrigues, C.; Rifà-Pous, H. Attack classification schema for smart city WSNs. *Sensors* **2017**, *17*, 771. [CrossRef] [PubMed]

51. Nautiyal, L.; Malik, P.; Agarwal, A. Cybersecurity System: An Essential Pillar of Smart Cities. In *Smart Cities*; Springer: Cham, Switzerland, 2018; pp. 25–50.
52. Healey, J.; Mosser, P.; Rosen, K.; Tache, A.; The Future of Financial Stability and Cyber Risk. The Brookings Institution Cybersecurity Project. 2018. Available online: https://www.brookings.edu/wp-content/uploads/2018/10/Healey-et-al_Financial-Stability-and-Cyber-Risk.pdf (accessed on 20 August 2020).
53. Svoboda, J.; Lukáš, L. Common Attributes of Security Breach Types. In Proceedings of the Third International Conference on Information Security and Digital Forensics, (ISDF2017), Thessaloniki, Greece, 8–10 December 2017; p. 21.
54. Azarov, V.N.; Kabanov, A.S.; Kopylov, O.A.; Morgunov, M.Y. Methods for the modelling of transport security. In Proceedings of the 2016 IEEE Conference on Quality Management, Transport and Information Security, Information Technologies (IT&MQ&IS), Nalchik, Russia, 4–11 October 2016; pp. 16–21.
55. Lysne, O.; Elmokashfi, A.; Schia, N.N.; Gjesvik, L.; Friis, K. Critical Communication Infrastructures and Huawei. Lynse et al. Critical Communication Infrastructures and Huawei in TPRC. 2019. Available online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3426222 (accessed on 24 August 2020).
56. Creech, B. Fake news and the discursive construction of technology companies' social power. *Media Cult. Soc.* **2020**. [CrossRef]
57. Ries, T. The Global Security Environment 2030. 2010. Available online: https://www.diva-portal.org/smash/get/diva2:563590/FULLTEXT01.pdf (accessed on 24 August 2020).
58. Moran, T.H. Multinational corporations and dependency: A dialogue for dependentistas and non-dependentistas. *Int. Organ.* **1978**, 79–100. [CrossRef]
59. Tarzi, S.M. Third world governments and multinational corporations: Dynamics of host's bargaining power. *Int. Relat.* **1991**, *10*, 237–249. [CrossRef]
60. Maryska, M.; Doucek, P.; Nedomová, L. Smart City Concept-Czech Republic Case. In *International Conference on Management and Industrial Engineering*; Niculescu Publishing House: Bucharest, Romania, 2017; pp. 676–684.
61. Vácha, T.; Přibyl, O.; Lom, M.; Bacúrová, M. Involving citizens in smart city projects: Systems engineering meets participation. In Proceedings of the IEEE 2016 Smart Cities Symposium Prague (SCSP), Prague, Czech Republic, 26–27 May 2016; pp. 1–6.
62. IDNES. Ústí čelí kritice kvůli parku. Lavička stála 60 tisíc, skluzavka půl milionu. 2010. Available online: https://www.idnes.cz/zpravy/domaci/usti-celi-kritice-kvuli-parku-lavicka-stala-60-tisic-skluzavka-pul-milionu.A101126_1489322_usti-zpravy_alh (accessed on 24 August 2020).
63. Šafhauser, R. Chytrá lavička se zahradou v Praze 6 uschla, nemá se o ni kdo starat. 2019. Available online: https://www.impuls.cz/regiony/praha/chytra-lavicka-magistrat-zahrada-uschla-vyrobce-zaleval-na-vlastni-naklady.A190826_163803_imp-praha_kov (accessed on 24 August 2020).
64. Sociologickýústav. Akademie věd ČR (Academy of Sciences of the Czech Republic). Centrum pro výzkum veřejného mínění. Naše společnost 2019—červen (dataset), version 1.0. Prague Český sociálněvědní datový archive. 2019. Available online: https://cvvmapp.soc.cas.cz (accessed on 21 August 2020). [CrossRef]
65. Klain, S.C.; Satterfield, T.; MacDonald, S.; Battista, N.; Chan, K.M. Will communities "open-up" to offshore wind? Lessons learned from New England islands in the United States. *Energy Res. Soc. Sci.* **2017**, *34*, 13–26. [CrossRef]
66. Simon, J.; Omar, A. Cybersecurity investments in the supply chain: Coordination and a strategic attacker. *Eur. J. Oper. Res.* **2020**, *282*, 161–171. [CrossRef]