Acta Polytechnica CTU Proceedings **46**:30–39, 2024
https://doi.org/10.14311/APP.2024.46.0030

Published by the Czech Technical University in Prague

"SMART CITIES" AND THEIR VULNERABILITY

Oldřich Krulík[a,*], Jan Kolouch[a], Marek Pačmag[b]

[a] *AMBIS University, Lindnerova 575/1, 180 00 Praha 8 – Libeň, Czech Republic*

[b] *Czech Technical University in Prague, Faculty of Biomedical Engineering, Náměstí Sítná 3105, 272 01 Kladno 1, Czech Republic*

[*] corresponding author: oldrich.krulik@ambis.cz

Abstract. In most discussions, "smart cities" are perceived as a largely positive phenomenon that improves the safety but above all the comfort of its inhabitants. The present paper constructively and critically analyses the approach of de facto unregulated development of "smart cities" with emphasis on the risks associated with this phenomenon. Examples from recent years, not only in the context of developments in Ukraine, show that modern, technological solutions, i.e. e-Government tools, can become a target or even a tool of variously motivated attackers (criminal groups, foreign powers). A "smart" city is often potentially more vulnerable than agglomerations managed more traditionally. This paper aims to demonstrate the possible risks through case studies and determine whether there are more comprehensive theoretical approaches to the subject.

Keywords: Smart cities, threats, adaptability, risk management.

1. Introduction

The presented study aims to interconnect several aspects related to the concepts of "smart cities", including those that are not immediately obvious. The authors operate with the working hypothesis that positive assumptions dominate about the topic, insofar as certain "pessimistic" expectations are already publicly presented. Some examples are related to the significant expansion of information and communication technologies and the potentially rising crime rate in this regard. The authors will therefore try to summarize several lines of concern related to the expansive use of the "smart cities" concept (mentioning, that the agenda needs to be perceived as all inventions in human history – as a "good servant and bad master").

(1.) In the first chapter, the authors try to monitor whether the topic is addressed by international organizations for police cooperation, or whether a certain criminogenic potential has been identified about "smart cities".

(2.) The next part is dedicated to the role of companies that offer technological solutions for "smart cities". Many of these companies come from the People's Republic of China, which may carry certain security connotations. Attention is also paid to relevant experience concerning the coronavirus situation.

(3.) The third part of the article focuses on the technological and cybersecurity side of things. The focus is primarily on the risks and the possibilities of their elimination in the case of building and maintaining "smart cities". The concept of a "smart city" during a military conflict is also being specifically pursued. As a follow-up to the previous chapters, observations related to the concept of "smart cities" within Ukraine will be telegraphically mentioned.

2. Materials and methodology

In this article, the authors present an analysis of the four above-mentioned areas (Figure 1), linking them and presenting partial conclusions related to the building and use of "smart cities". The theme of internal security (crime, crime prevention) is thus linked to challenges in the field of industrial competition (and other challenges related to dependence on non-European suppliers of technological goods and services – a process that has been intensified by the coronavirus situation), the effects of armed conflicts (regarding the agglomerations), with special emphasis on the current experience of Ukraine. Based on an analysis of selected cyber-attacks and risks associated with smart cities, recommendations were made to improve cyber security in this regard.

The study also aims to a certain extent to bridge the absence of complete methodological concepts – when the concepts of "smart city" and security are often limited to information, respectively information and communication technologies, the Internet of Things, and similar aspects, while they usually do not expand much into the area of local public order affairs in the more traditional sense of the word. The authors were also inspired by some existing studies, from which emerge some useful observations.

New possibilities traditionally bring with them new challenges, which may not always be entirely positive. The effects and externalities of the processes and concepts of building smart cities urgently require the interest of the scientific community and responsible agents [1]. Questions can be asked, for example,

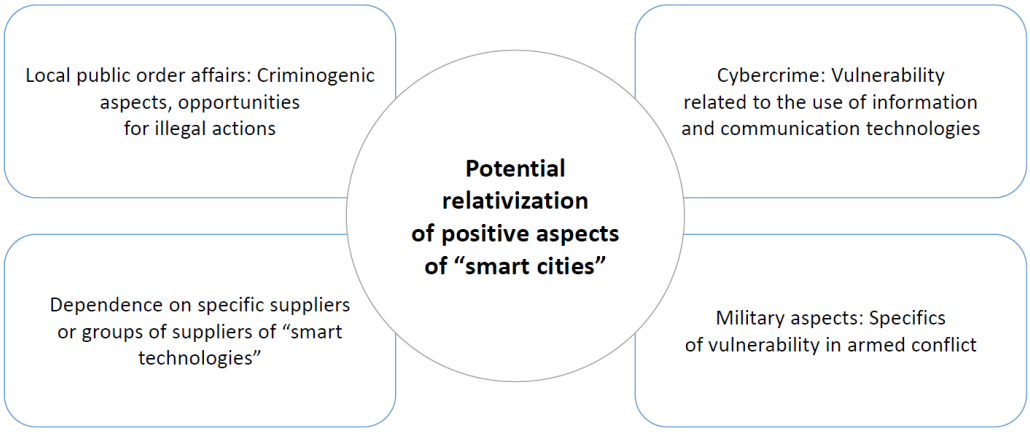

FIGURE 1. Potential internal and external security-related challenges, which can play a role concerning the "smart cities" agenda.

whether general assumptions about the solution uh it's a longof "smart cities" are based on evidence-based conclusions, or whether they are more or less unfounded guesses. A potential security incident could put such overly optimistic expectations into another perspective [2]. It is necessary to directly assume that any processes and models, including the modernization of cities, will bring with them positive and negative impacts, including the building of new barriers (digital divide, etc.) [3]. Cities (and not just "smart" ones) are under increasing pressure to address complex, interrelated challenges (air quality, climate change, carbon footprint reduction, transport, housing affordability, social inequality, biodiversity, and more). At the same time, it can be stated that most developed agglomerations in many countries of the world already contain "smart" elements, such as sensors that monitor air quality, traffic, or street lighting intensity [4]. The promotion of the circular economy (systems in which the waste of one process becomes the fuel of another activity) is not a side of attention [5].

Technological optimism or pessimism around new ambitious projects generally concentrates on several themes [6]:

(1.) Concerns around fairness or inclusiveness (or more generally the legitimacy of democratic governance at the municipal/city level).

(2.) Concerns about technologies, or specific measures, including the concentration and operationalization of the widest possible spectrum of data, which could expand into the privacy of the widest public. Certain types of data are more sensitive or personal than others, and also raise more concerns about possible misuse or "monetization" (for the needs of targeted advertising, or even more negative purposes).

(3.) Other dimensions of this topic relate to predictive policing or crowd management. However, the data can also represent an essential tool for revealing and correcting some negative trends that may not always be obvious without this data (for example, uneven distribution of services in the territory, which leaves behind various socially excluded locations).

(4.) Concerns about the sustainability of life in the agglomeration, including the position of marginalized communities.

(5.) Concerns about insufficient governance transparency.

3. "Smart cities", local public order affairs, and the international organizations for police cooperation

Examples from recent years show that modern, technological solutions, i.e. e-Government instruments, can become a target or even a tool of variously motivated attackers, typically criminal groups or foreign powers. A "smart" city is potentially more vulnerable mainly due to the lack of implementation of security measures or their imperfect interconnection with other components of the information and communications infrastructure. In terms of protecting "smart cities" from criminal activities, INTERPOL and EUROPOL do agree on the topic – but the whole agenda is still only in the initial phase. Bridging this gap will require a significant effort by several actors, which this study aims to contribute to.

In the case of attacks by a foreign power (sovereign state), this issue must be addressed particularly concerning the purpose of the attack. It may still be criminal activities (see e.g. attacks by state-sponsored criminal groups from the Russian Federation or Democratic People's Republic of Korea) or attacks like an act of war (see Section 6.1).

So if we return to the role of international police structures, then along with unmanned aerial vehicles, border security, 5G networks, environmental crime, and others, the topic of "smart cities" was included in the program of the INTERPOL world conference in Singapore in 2019. The objective of the conference was to create a global innovation agenda that will present

the cooperation of the police and private sector [7]. It is also possible to mention the working document of the INTERPOL Innovation Center, entitled "Scanning for the Future(s) of Policing: First Steps towards a New Global Paradigm" [8], issued in March 2022, where nine basic areas of the global transformation and interconnection were detected (including "smart cities"). It was assumed that in 2050, about 68 percent of the world population will live in cities, which is associated with higher cyber vulnerability in the form of hacking, remote disabling of electricity supplies, etc. Within the document, chapter 2 (New Citizen Relations: Community Policing) deals with the topic in particular:

"In a digital world, it could be increasingly important for police to expand their online community contact and crime reporting platforms. Building a strong relationship with communities, such as through dedicated community teams, has long been a key success factor for effective policing. Now technological advances are creating new opportunities for positive interactions. Multi-channel communication, including app-based crime reporting, can enhance citizen participation and experience while providing real-time awareness to police and enabling them to be more responsive to the needs of their constituents. Digital engagement can also be augmented by automated chatbots and AI solutions to provide faster, more tailored services to communities while lessening the stress on limited resources – both online and offline... Meanwhile, AI-enhanced analytics could further reduce demand on control rooms and contact centers, for example by indicating if the person calling is a serial caller, particularly vulnerable or wanted in connection with another offence elsewhere." [8]

If we study Europol's document entitled Europol Programming Document 2022-2024, special emphasis is placed on several strategic priorities – but "smart cities" are not mentioned in the entire document at all – so it is possible to conclude, that this agenda is not (yet) a priority for Europol [9]. As far as the position of Europol in this regard is concerned as ambiguous, since 2020 there was an increase in funds for Europol by EUR 30 million, for example for the further development of automated biometric identification systems [10].

4. Technologies and "smart cities" – including concerns about the limitation of the standard of human rights protection in the context of the pandemic

The massive proliferation of "smart cities" may provide another area for the proliferation of potentially unreliable technologies or applications that may pose serious risks not only to the protection of personal data but also to the cybersecurity of a given city or state. Another aspect that might need to be considered is cyber and personal data security. Several United States and European agencies marked Chinese technologies and applications as a security challenge. Some Euro-Atlantic countries are now pushing Internet Service Providers to discontinue the use of Chinese hardware (industrial-grade routers, switches, receivers, etc.) in their networks (or at least in the applications involving critical infrastructure).

The COVID-19 crisis in the People's Republic of China has greatly accelerated the testing of some technologies and equipment for "smart cities" (drones, robots, surveillance applications, security cameras with artificial intelligence, etc.). The situation has also caused activism in terms of global support, donation, and export of some "smart" technologies with dual-use (health/surveillance) capabilities, the so-called Digital Silk Road.

Current developments have only revealed more clearly a trend that has been emerging since 2013 (including rhetoric that pits the alleged effectiveness and strength of China's system against the alleged weaknesses of "Western" models). On the other hand, for the Euro-Atlantic players in general, there is a risk that they will leave the development of security technologies, including the security dimension of "smart cities", to authoritarian regimes.

The People's Republic of China has made the "smart city" concept a part of its national development strategy. This concept is explicitly mentioned in the 13th Five-Year Plan (for 2016 to 2020), adopted in March 2016 [11–13]. Since then, the government in Beijing has massively supported the development of "smart cities" across the country. In January 2019, it was reported that a total of 500 "smart city" pilot projects were being developed. The government has also encouraged domestic technology companies to become global leaders and to engage in overseas "smart city" projects [14].

The definition of a smart city through the lens of the People's Republic of China was initially understood as a synonym for a "safe city" and the development of monitoring tools for state security agencies. After all, this (although not only) functionality is offered by several Chinese companies on a commercial basis (advanced camera systems, including facial recognition technology; collection and analysis of big data; tracking applications, etc.) [13].

The coronavirus has also indirectly helped local governments in the People's Republic of China to further test and tune up the existing applications and solutions. The year 2020 was in this regard planned as the starting point of the full launch of the "National Reputation System"[1], which sooner or later will probably form a part of the "smart city" model in

[1]This concept, also known as the Social Credit System, was developed since 2008/2009 for monitoring natural and legal persons in the People's Republic of China, with an emphasis on various aspects of their economic and social behavior (social credibility) [15].

this country. In early March 2020, the government in Beijing announced stimulus measures to help the economy recover from the coronavirus-related crisis (support for the rapid development of 5G base stations, large data centers, artificial intelligence, the Internet of Things, etc.) [16].

An approach that combines big data analysis and "social management", in other words, expects the specific use of data by government bodies for various purposes, including anticipating and preventing protest movements. The registration of an individual's real name is already mandatory to buy medicine or to use public transport. Cloud systems, used by police, are increasingly analyzing individuals' data, including social media accounts, to identify potentially dangerous trends. The term "predictive police" thus takes on a completely new dimension.

This also applies to the counter-terrorism agenda. In particular, Xinjiang province is becoming an incubator for high-tech surveillance tools[2].

Companies from the People's Republic of China are increasingly able to provide a "comprehensive smart city package" that connects the various components through partnerships between the nation's technology companies. Data collection efforts are facilitated by the fact that the country is home to Internet and e-government industry champions (Baidu, Alibaba, Xiaomi) that have ambitions to expand globally [17]. These companies also quite often offer their services abroad collectively and are increasingly approaching European cities and other public institutions, offering to "improve" their infrastructure (cities, ports, airports, railway stations, etc.). At the same time, the "security" side of the agenda is usually promoted as well [18]. Already in December 2019, after all, Beijing explicitly mentioned "smart cities" as an area of future cooperation between the People's Republic of China and the European Union. Many European regional authorities or municipalities may choose such solutions because they do not analyze the geostrategic aspects of such purchases or investments [19].

Specific examples of cooperation and transfer of knowledge and technology in Europe include:

- **Spain:** Municipalities such as Mazarrón (province of Murcía) received temperature-measuring drones in 2020 [20].
- **Italy:** Torino received drones for public space monitoring, also in 2020 [21].
- **Serbia:** In April 2019, Huawei launched a "smart city pilot project" in the city of Niš. This is probably the most significant relevant project of the People's Republic of China on European soil. The concept is trying to include smart lighting and mobility services. This follows the project in Belgrade, where the city signed a Memorandum of Understanding with Huawei. The Serbian capital is already equipped with Huawei's facial recognition surveillance cameras [22].

Beijing promotes its concept of "smart cities" through bilateral and regional frameworks, such as the People's Republic of China – Association of Southeast Asian Nations (ASEAN) summit, or the Forum for Cooperation with the post-Soviet Central Asian Republic, especially under the banner of the "Belt and Road Initiative". In addition to donations, Beijing promotes its influence through a series of training programs provided to officials and technicians from abroad, especially from developing countries (they are trained in, among other things, how the context can be used for specific social, political, or security purposes) [23].

5. Cybersecurity of "smart cities"

All components of "smart cities" can be exposed to new vulnerabilities that can be exploited by cybercriminals or state-sponsored actors. High complexity, high interdependency, and intensive communication lead to unbounded attack surface and cryptography-related issues [24]. The potential consequences of cyber attacks on smart cities are significant, ranging from economic losses and infrastructure damage to threats against public safety and privacy. Therefore, it is crucial to implement robust cybersecurity measures.

As far as the basic approach is concerned when building "smart cities", it is imperative that the SD3 (security by design, default, and deployment) rule is respected. This rule assumes that security is an integral part of all processes. At the same time, other regulatory connotations (international and national) should be taken into account. Typically, this will include the need to respect the protection of personal data as set out in Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) or the rules set out in Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS 2 Directive) to ensure cybersecurity.

Disruption on a relatively large scale can be thus achieved remotely, without the physical presence of foreign actors on the territory of another state. Such a remote attack is then much easier to mask, deny, or deflect as an act of terrorism – instead of foreign power aggression.

To enhance the cybersecurity of "smart cities", several measures should be adopted to mitigate potential risks and protect the digital infrastructure. The authors have to mention several crucial cybersecurity measures that can be implemented:

[2]Xinjiang (Uyghur) Autonomous Region is the territory where the surveillance system is reinforced with the dense camera system, including facial recognition. It is also associated with a smartphone app that police forces are using to get quick and comprehensive data about individuals.

(1.) **Risk assessment and planning.** To identify potential vulnerabilities and threats in "smart city" systems, a thorough risk assessment is essential. Risk assessment helps in developing comprehensive cyber security plans and strategies for effective risk mitigation.

(2.) **Securing Internet of Things (IoT) devices.** "Smart cities" heavily rely on Internet of Things devices, such as sensors, cameras, and connected infrastructure. Securing these devices is essential to prevent unauthorized access, data breaches, and potential exploitation.

(3.) **Network security.** Strong network security measures, including firewalls, intrusion detection and prevention systems, and encryption protocols to safeguard "smart city" networks from unauthorized access and data breaches should be implemented.

(4.) **Secured communication channels.** It is essential to secure communication channels between devices, sensors, and systems within the "smart city" infrastructure. This can be achieved through encryption and authentication mechanisms to prevent interception and tampering of data.

(5.) **Regular security updates.** All systems but also applications used should be updated daily. Updates should include security patches, firmware updates, and software upgrades. Known vulnerabilities should also be addressed immediately and patches applied to mitigate potential risks.

(6.) **Access control and authentication.** Strict access controls and multi-factor authentication mechanisms need to be put in place to ensure that only authorized personnel have access to critical systems and sensitive data. These measures can help prevent unauthorized access by cyber attackers.

(7.) **Data encryption.** Encryption of data both at rest and in transit must be provided to protect it from unauthorized access. This includes encryption of data stored in databases, transmitted over networks, or processed by various "smart city" applications.

(8.) **Incident response and recovery plans.** Comprehensive incident response and recovery plans must be in place to deal with cyber-attacks immediately. These plans should include procedures for identifying, mitigating, as well as recovering from security incidents and temporary fallback plans to handle the critical city services without the respective network backgrounds.

(9.) **Vendor security assessments.** A key component of building "smart cities" is conducting a thorough security assessment of vendors that provide smart city technologies or services. In particular, it is necessary to identify whether suppliers are adhering to security practices and standards, what their previous reputation is, etc. The supplier and its technology or services may be the target of supply chain attacks, but at the same time, it may be an entity that will carry out one of the previously mentioned attacks.

(10.) **Data protection.** Strict measures to protect personal data, as well as the accompanying metadata, must be put in place to comply with the relevant regulations and to protect both personal and operational data collected by "smart city" systems. In this respect, it is essential to put in place measures to allow for anonymization or pseudonymization of data.

(11.) **Regular security audits.** It is imperative to ensure that regular security audits and penetration tests are carried out to identify vulnerabilities and weaknesses in the infrastructure. These audits and tests can help to identify potential security weaknesses and enable their timely remediation.

It's important to note that the specific cybersecurity measures implemented in a smart city may vary depending on the technologies and systems deployed. Cybersecurity in "smart cities" requires a multi-layered approach that includes technology, policies, and active collaboration between stakeholders (system administrators, vendors, etc.). By prioritizing cybersecurity measures, "smart cities" can reap the benefits of advanced technologies while effectively mitigating potential risks and ensuring the safety and privacy of their citizens. A comprehensive cybersecurity strategy should be developed, considering the unique characteristics and requirements of each "smart city" project.

6. Military aspects: "Smart city" as a battlefield

Another topic that cannot be ignored here, is the eventuality that the city with "smart infrastructure" would become the scene of military conflict. Examples of smart agglomeration are in Table 1 [25]. An urbanized world, heavily dependent on modern technologies, contributes to the ever-increasing complexity of future military operations. What is positive in times of peace can be a serious challenge in times of war. Let's imagine the situation: An enemy has compromised the 5G network in a certain big city. Traffic lights are not operating and the traffic situation is unmanageable. Garbage is not taken out and attracts rodents. Disruption of delivery of drinking water or electricity supplies can also occur.

If we think of "smart cities" as a battlefield, we need to focus on the infrastructure components that can be attacked in the first row:

(1.) **Physical objects.** Remotely controlled machines supporting critical services, such as water treatment, can be physically destroyed to affect the comfort of city residents. Similarly, electricity supply may be disrupted.

Attacker's position	• It is important that the occupied agglomeration does not collapse or disintegrate. • We have to prevent a humanitarian disaster.	• It is different if the occupied agglomeration collapses, or decomposes.
Defender's position	• It is important that the occupied agglomeration does not collapse or fall apart. • In the event of retreat or evacuation of the city, it is expected no intentional damage to its infrastructure.	• It is irrelevant, if the agglomeration, occupied by the enemy collapses. • Possible problems that arise can be used for international politics or propaganda purposes.

TABLE 1. Four basic model situations regarding access to "smart agglomeration" in the context of military operations.

(2.) **Information and communication technologies infrastructure.** In particular, 5^{th} and next-generation Internet of Things (IoT) enabled networks – which can also be the target of some forms of attacks.

(3.) **Sensors.** These may be tracking or reconnaissance sensors that are accessed illegitimately, or they may be misused to transmit false data.

(4.) **Computing capacities.** Data of all kinds can be altered and lead to confusing results.

(5.) **Transportation.** Physical destruction cannot be ruled out, nor various forms of "remote" communication blocking.

(6.) **Access to cloud services** may be temporarily interrupted; data may be manipulated and altered.

(7.) Unauthorized **access to analytical platforms** or manipulation of data will make it possible to change decision-making algorithms.

(8.) **Access to mobile or other applications** may be denied (including online banking or other functions).

Without necessarily being "smart cities", the considerable experience can be drawn from the situation in the Middle East, where large cities such as Mosul or Aleppo have become examples of the collapse that has affected hundreds of thousands of inhabitants [26]. Directly in the context of the war against Ukraine, it is possible to mention the case of the "remote" takeover of the airport in Kyiv in 2016 – which, moreover, was reacted to in the Kremlin's propaganda environment by saying that if the country is unable to defend its infrastructure, it deserves an attack of this kind (the attacker's guilt, traditionally, was not mentioned at all) [13].

These or other challenges of the security discourse lead to the following statements:

- In a city, remotely controlled by the enemy, the quality of life may be reduced considerably.
- The progress and habituation of the public to a certain standard are so complex that "returning to offline (non-smart) mode" is no longer an alternative for most cities.
- The Achilles heel is represented by data centers controlling processes, owned and operated by third parties, which present another set of opportunities for attackers.
- The scenario does not even need to be a conflict between states, but also an incident caused by terrorists or violent extremists.

6.1. "Smart Cities" and war against Ukraine

The "Smart cities" agenda has been monitored within Ukraine at least since 2016. The Committee for Housing and Land Management received a request from the Ministry of Regional Development, Construction and Housing and Communal Services of Ukraine to preparea profile of a "smart sustainable city". Voznesensk was chosen as a pilot city (approximately 30 000 inhabitants, Mykolayivsk region, in March 2022 the city was heavily damaged). The creation of the related study started in December 2017 and was completed in January 2019. Based on the analysis, a list of challenges Ukraine faces on the way to "smartization" was created [27]. It was evident, that many cities, despite having some development potential, are trying to use some individual innovations rather than coherent strategies. The problem was also the insufficient integration of activities that were carried out selectively. A positive fact has been the increasing involvement of ICT in the city management process. The added value was the systematic improvement of the quality of public services and the increase of social participation in the public decision-making process, which makes it possible to integrate local society and build trust in public institutions [28].

Before the outbreak of the current phase of the conflict in Ukraine, there was a consensus that, due to the high population density, cities show significant potential for creativity and innovation, energy savings, and environmental friendliness, creating a positive dynamic interaction of these elements for develop-

ment [29]. The Cities in Motion Index was chosen for the calculations of relevant indices for Ukrainian cities, which takes into account the maximum number of indicators and assesses such socio-economic aspects of the possible development of cities as, for example, human capital, social cohesion, governance, mobility and transport, urban planning and technology [30]. Examples of best practices in other countries, especially Poland (Warsaw, Lublin) were also mapped. At the same time, it was found that both in Poland and Ukraine the concept is only in the initial phase of implementation [31]. In the context of Ukraine's ambitions for accession to the European Union, a sustainability project, Smart City Kharkiv, was launched, initially phased until 2030 [27].

The year 2022, characterized by the escalation of the conflict, continues to be marked by the "smartization" and decentralization of infrastructural processes – in light of the massive destruction and deterioration of living conditions in several large cities of Ukraine. Several instruments are specifically targeted at rural areas, such as the use of "smart fertilizers", leading to a less negative impact on the environment, and maintaining biodiversity and food security during war [32]. The key priorities of smart management in the cities of Kyiv, Poltava, Kharkiv, Odesa, Lviv, and Dnipro were determined (multimodal transport systems, cooperation between public and private sector actors, self-managing energy networks, etc.). However, the complex problems that arise from the ongoing war logically complicate the implementation of the concept. At the same time, it is already heard, in the environment of Ukraine representatives, that when the fighting ends, the efforts of the authorities will not be to restore the cities to their original state but to "upgrade" them to become pioneers of innovative solutions of all kinds.

After about half a year, the war moved into the attrition phase, where the military, human, and economic reserves of the warring countries play a key role [30]. The Kremlin perceives the massive destruction of Ukraine's civil infrastructure (electric power grids, heating), ideally across the entire territory, up to the very west, as compensation for unsatisfactory developments on the battlefield. At the turn of 2022 and 2023, there were practically 3 to 4 million people without electricity, running water, and heating, especially in larger agglomerations. It should be noted that Kyiv is now, after absorbing the number of internally displaced persons, more populous than Berlin, the most populous city in the territory of the European Union Member States (around 3.6 million people). The most fundamental challenge during the winter of 2022/2023 in Kyiv was the water supply – when the electricity goes out, the water in the pipes freezes, and their repair will be extremely expensive. The situation is similar in other cities, especially in Odesa.

The liberation of Kherson can also be seen from this point of view (before the invasion, around 300 000 inhabitants lived here; now it is "roughly 50 000 people" and practically no public infrastructure works there). The same applies to the surroundings of this city, but also to several other regions of Ukraine near the front. To this must be added the mining of several localities, which complicates the possible revitalization plans.

At the same time, the official speakers of the Russian Federation did not hide the efforts to encourage emigration from Ukraine and strengthen anti-Ukrainian sentiments in Europe. There are also malicious references to the fact that "power cuts" in Ukraine allegedly led to many cases of looting and an outburst of the wide spectrum of crime. The statement of the National Police of Ukraine on the development of registered crime for November and December 2022, on the contrary, speaks of a decrease in registered crime by 13 to 16 % [33, 34]. Police forces, aided by curfews and other restrictive measures, declare an uncompromising stance on looting cases. According to police statistics, this approach is bearing fruit [13, 35].

In summary, it can be stated that Ukraine's ambitions to build "smart cities" have been replaced by ambitions to decentralize energy and other critical infrastructure. The main reason for this approach is to better protect against the cyber attacks that took place at the beginning of the war. In particular, the Wiper malware attacks targeted information and communication technologies controlling electricity distribution in Ukraine (Hermetic Wiper, 23 February 2022; Isaac Wiper, 24 February 2022; Caddy Wiper, 14 March 2022; Industroyer 2 and Caddy Wiper, 8 April 2022, etc.). In this context, the following preventive or reactive tools that alleviate this situation can be mentioned:

- Massive investments in digitization, with an emphasis on tools (applications), intended for people who are constantly migrating (nationally and internationally displaced persons), so that these persons also have a channel for communication with public institutions and can prove their electronic identity for various purposes [13].
- Building so-called "points of un-breakability". There are now (February 2023) more than 4 000 such points, and this network is still growing. These are shelters with free heat, electricity, medical supplies, internet, etc. located in schools, medical facilities, private companies, and elsewhere. It can also be a heated tent. This can be seen as a great inspiration for countries whose shelter network is currently very sparse and usually without the mentioned functionalities [13].
- The European Commission explicitly mentions Ukraine as a pioneer of decentralized energetics (generators, smaller substations, small steam-gas power plants, innovative photovoltaic solutions), as the burden on the environment that this model entails is also important. More than 300 000 power generators can be mentioned, in almost every major

company in the field of production and services, including banks or gas stations [36].

- The e-Enemy application, intended for reporting alleged saboteurs, is perceived rather questionably [37–39].
- Cyberspace is becoming an important strategic, tactical, and operational part of the battlefield's operations. An example might be some Ukrainian army operations being canceled due to them being disconnected from Starlink [37].
- In addition, it is possible to mention information about the development in Transcarpathian Ukraine, which is now perceived as a center (cluster) of the development of information and communication technologies. During the first 7 months of the war, around 100 companies and 28 000 experts related to the state-of-art technologies, moved to this region from the rest of the country [1].

7. Results

In the current phase, the authors perceive the text as a springboard for other researchers who would focus on topics that can be characterized as security-related meta-aspects of the concept of "smart cities". Given the existing challenges and pressures, it seems possible that the key aspect of the related efforts is not the "city" (or even "big city"), which objectively represents a vulnerable environment, prone to the concentration of a whole range of negatives and weaknesses – but the "smartness", that can be implemented to any territory (small village, countryside), but also concerning dynamically moving individuals (or groups of individuals, firms, etc.). The issue as a whole also represents a task for progressive public administration, police officers (where the authors are also professionally connected) – but also society as a whole.

8. Discussion

In the paper, the authors addressed some potentially negative aspects of the concept of "smart cities". They believe that the sooner these possibilities become the subject of more detailed research, the more likely their possible impacts will not devalue the whole "smart cities" idea. Overall, it can be stated that relevant scientific articles, as well as documents, prepared by the international police organizations, perceive the topic only in fragments so far, or about the advantages and opportunities it can bring to law enforcement authorities. Large agglomerations are however generally perceived as places where crime tends to be concentrated, as this aspect cannot be perceived (and the countryside cannot be idealized at all). Possible investments in surveillance technologies are then an effort to solve the consequences, not the causes of certain negatives.

From the point of view of the technological equipment of "smart cities", the question is to what extent the priorities of free trade are compatible with a certain vigilance towards technologies from outside the European Union Member States (especially regarding the production of the firms from the People's Republic of China, where the export of technologies can also be seen as part of geostrategic ambitions, the end of which is not easy to see). In this regard, the coronavirus situation represented a multidimensional impulse – many individuals and companies accepted the remote-work model, in which it is irrelevant whether a certain person resides in a specific city, near the workplace, or anywhere else.

Europe has already run out of its "peace dividend", and for this reason, it seems to be necessary to invest significant financial resources in securing "smart cities" against the robust intervention of a foreign power. This is an additional cost, which was not always expected, but which seems necessary in the current situation. In the event of an armed conflict, large cities become traps that concentrate on several negatives and only a limited spectrum of positives. This statement is directly connected to the experience of the Ukraine. This country has involuntarily become a pioneer of solutions, which apparently cannot be perceived as "smart cities", but as "smart decentralization" or "smart mobility". Any large concentration of people poses a challenge to a functioning infrastructure, which is extremely demanding during the war. Priorities of environmental protection or economies of scale have therefore given way in favor of the aforementioned decentralization and mobility.

9. Conclusion

The concept of "smart cities", even if we are aware of its positive aspects, poses a significant challenge to modern societies. The concentration of population in cities is not positive in itself. At this point it is necessary to summarise the possible negatives associated with the process of creating "smart cities":

- Not all "smart cities" (or their managers respectively) see economic, environmental, and social well-being for their current and future residents as their primary objective.
- Some "smart city" proposals sometimes seem to be motivated by "technology for technology's sake" (because it is currently "in vogue", without real need).
- Large-scale implementation of technologies, without meaningful participation of the interested community, or at least a significant part of it, is also perceived as a step in the wrong direction.
- A city can be very "smart" but not necessarily inclusive. It can also be environmentally sustainable, but at the same time, it can be exclusively expensive.
- Without strict oversight, technology may exacerbate, rather than correct, weaknesses in urban governance.

The paper presented primarily the risks associated with the use of "smart cities". Through mapping the various vulnerabilities and comparing potential risks, the presented paper may provide a suitable starting point for further research regarding local public order affairs.

The whole concept of "smart cities" is also an economic and industrial challenge for Europe and the European Union, in particular, because many technology companies from the People's Republic of China have already achieved a significant market share in the global market for "smart" technologies and solutions (beating some European or North American competitors). It cannot be ruled out that if Euro-Atlantic companies remain passive, European cities will have to rely on foreign technologies or become uncompetitive compared to cities in other regions that have already incorporated advanced technologies into their daily lives.

Cybersecurity in "smart cities" requires a multi-layered approach that includes technology, policies, and active collaboration between stakeholders (system administrators, vendors, cyber security specialists, etc.). By prioritizing cybersecurity measures, "smart cities" can reap the benefits of advanced technologies while effectively mitigating potential risks and ensuring the safety and privacy of their citizens.

A comprehensive cybersecurity strategy should be developed, considering the unique characteristics and requirements of each "smart city" project.

"Smart cities" will certainly become the environment for future combat operations. As the current conflict in Ukraine shows, cyberspace is becoming an important part of modern conflicts and even the battlefields (an example might be some Ukrainian army's operations being canceled due to them being disconnected from Starlink). Even in the real world, a weak adversary can get a much stronger country into widespread complications. One side may succeed in a fight in the true sense of the word, but its success will be negated by the "winner" losing control of many of "its" agglomerations. Examples from recent years, not only in the context of developments in Ukraine, represent that modern, technological solutions, i.e. tools of e-Government, can become a target or even a tool of variously motivated attackers (criminal groups, foreign powers). At the same time, it can be anticipated that in certain respects the "smart" cities are often potentially more vulnerable than agglomerations managed more traditionally.

Respective sub-themes and perspectives still exist to a certain extent rather "side by side" and are not interconnected – which the authors to some extent try to bridge in this study. At the same time, the literature related to the mentioned agenda is still relatively limited, not to mention peer-reviewed academic outputs. Although these aspects are already on the agenda of international police cooperation organizations, the topic as a whole is still being addressed only in fragments. As a result, it is currently also an assignment for progressive state administration and security forces, which the authors also, to a certain extent, try to represent.

Acknowledgements

The authors would like to thank AMBIS College, Prague, Czech Republic, for its support.

References

[1] Y. Popova, S. Popovs. Effects and externalities of smart governance. *Smart Cities* **6**(2):1109–1131, 2023. https://doi.org/10.3390/smartcities6020053

[2] D. Mills, S. Pudney, P. Pevcin, J. Dvorak. Evidence-based public policy decision-making in smart cities: Does extant theory support achievement of city sustainability objectives? *Sustainability* **14**(1):3, 2021. https://doi.org/10.3390/su14010003

[3] K. Vitálišová, A. Vaňová, A. Ivan, et al. Impacts of smart governance on urban development. In O. Gervasi, B. Murgante, A. M. A. C. Rocha, et al. (eds.), *Computational Science and Its Applications – ICCSA 2023 Workshops*, pp. 547–564. Springer Nature Switzerland, Cham, 2023. https://doi.org/10.1007/978-3-031-37120-2_35

[4] Eco-Business. Tencent's 'smart city' seen as model for post-coronavirus China, 2020. [2023-05-14]. https://www.eco-business.com/news/tencents-smart-city-seen-as-model-for-post-coronavirus-china/

[5] Mapping Smart Cities in the Euroepan Union. Brussels: European Parliament: Directorate General for Internal Policies; Committee on Industry, Research and Energy, 2014 IP/A/ITRE/ST/2013-02, 2018. [2021-11-23]. http://www.itu.int/en/ITU-T/climatechange/resources/Documents/MappingSmartCitiesinEU-2014.pdf

[6] E. Shahini, E. Skuraj, F. Sallaku, S. Shahini. Smart fertilizers as a solution for the biodiversity and food security during the war in Ukraine. *Scientific Horizons* **25**(6):129–137, 2022. https://doi.org/10.48077/scihor.25(6).2022.129-137

[7] INTERPOL. Interpol World: Finding joint solutions to future security challenges, 2019. [2023-05-14]. https://www.interpol.int/news-and-events/news/2019/interpol-world-finding-joint-solutions-to-future-security-challenges

[8] INTERPOL Innovation Centre. Scanning for the future(s) of policing: First steps towards a new global paradigm, 2022. [2023-05-14]. https://1url.cz/LuL43

[9] Europol. Europol programming document 2022–2024, 2021. [2023-05-14]. https://1url.cz/rutdG

[10] Article 19. European Union: Civil society challenges European Union plans to expand biometric mass surveillance, 2020. [2023-05-19]. https://1url.cz/autdp

[11] A. Ekman, C. d. E. Picardo. Towards urban decoupling? China's smart city ambitions at the time of COVID-19, 2020. [2023-05-14]. https://1url.cz/tutdq

[12] United Nations Interregional Crime and Justice Research Institute. The conflict in Ukraine and its impact on organized crime and security – November 2022, 2022. [2023-05-19]. https://1url.cz/cutIi

[13] Ukrinform. Punkty nezlamnosti: zymu perezhyvemo — svitlo, zv'yazok, teplo i voda budut', 2022. [2023-05-19]. https://www.ukrinform.ua/rubric-ato/3621302-punkti-nezlamnosti-zimu-perezivemo-svitlo-zvazok-teplo-i-voda-budut.html

[14] United Nations Economic Commission for Europe, Genéve. Smart sustainable cities profile: Voznesensk, Ukraine, 2019. [2023-05-19]. https://unece.org/dam/hlm/documents/publications/ssc_profile_voznesensk.eng.pdf

[15] A. Boquen. An introduction to China's social corporate credit system, 2020. New Horizons Global Partners. [2023-05-14]. https://nhglobalpartners.com/chinas-social-credit-system-explained/

[16] Xinhua Net. China vies for smart city building, 2019. [2023-05-14]. http://www.xinhuanet.com/english/2019-01/02/c_137714396.htm

[17] Xinhua Net. Alibaba offers AI diagnostic tool of COVID-19 to more countries, 2020. [2023-05-14]. http://www.xinhuanet.com/english/2020-03/19/c_138895495.htm

[18] L. Lucas, R. Waters. China and United States compete to dominate big data, 2018. Financial Times. [2023-05-14]. https://www.ft.com/content/e33a6994-447e-11e8-93cf-67ac3a6482fd

[19] A. Ekman. China's smart cities: The new geopolitical battleground, 2020. Ifri. [2023-05-14]. https://www.ifri.org/en/publications/etudes-de-lifri/chinas-smart-cities-new-geopolitical-battleground

[20] A. Atkinson. Drones used to calibrate temperatures in Mazarron, 2020. The Leader. [2023-05-14]. https://www.theleader.info/2020/03/30/drones-used-to-calibrate-temperatures-in-mazarron/

[21] Dà-Jiāng Innovations. In Europe's fight against COVID-19, drones rise to the challenge, 2020. [2023-05-14]. https://content.dji.com/in-europes-fight-against-covid-19-drones-rise-to-the-challenge/

[22] China Daily Global. Huawei opens innovation hub in Serbia, 2019. [2023-05-14]. https://global.chinadaily.com.cn/a/202009/16/WS5f617b77a31024ad0ba79db7.html

[23] Association of South East Asian Nations. Asean-china leaders' statement on smart city cooperation initiative, 2019. [2023-05-14]. https://asean.org/asean-china-leaders-statement-smart-city-cooperation-initiative/

[24] A. AlDairi, L. Tawalbeh. Cyber security attacks on smart cities and associated mobile technologies. *Procedia Computer Science* **109**:1086–1091, 2017. https://doi.org/10.1016/j.procs.2017.05.391

[25] M. Kovalsky, R. J. Ross, G. Lindsay. Contesting key terrain. *The Cyber Defense Review* **5**(3):133–150, 2020. [2023-05-14]. https://www.jstor.org/stable/10.2307/26954877

[26] Times of Israel. Cyber attacks again hit israel's water system, shutting agricultural pumps, 2020. [2023-05-17]. https://www.timesofisrael.com/cyber-attacks-again-hit-israels-water-system-shutting-agricultural-pumps/

[27] I. Yu. Matyushenko, V. V. Reznikov, A. Pozdniakova, O. V. Tofaniuk. Implementation of a smart sustainable city concept in Ukraine at an example of Kharkiv city. In *2021 2nd International Conference on Internet and E-Business*, ICIEB'21, pp. 29–34. ACM, 2021. https://doi.org/10.1145/3471988.3471993

[28] M. Czupich, S. Kucherenko, V. Riznyk. Contemporary challenges to the development of cities – the experience of Poland and Ukraine. *Studia Miejskie* **38**:23–38, 2020. https://doi.org/10.25167/sm.2176

[29] V. Babenko, O. Matsenko, Y. Chorna, V. Troynikova. Breakthrough innovations in implementing the «smart cities» concept: EU experience and Ukraine's opportunities. *Herald of Khmelnytskyi National University* **302**(1):269–277, 2022. https://doi.org/10.31891/2307-5740-2022-302-1-45

[30] V. Dykan, M. Ieromyna, U. Storozhylova, L. Bilous. Implementation of smart city concept in Ukraine. *SHS Web of Conferences* **67**:06015, 2019. https://doi.org/10.1051/shsconf/20196706015

[31] R. Lozynskyy, V. Pantyley, A. Sawicka. The smart city concept in Poland and Ukraine: in search of cooperation opportunities. *Bulletin of Geography Socio-economic Series* **52**(52):95–109, 2021. https://doi.org/10.2478/bog-2021-0016

[32] Shanghai Cooperation Organization Secretariat. Shanghai Cooperation Organization Secretary-General meets with Alibaba vice president, 2020. [2023-05-14]. http://eng.sectsco.org/news/20200523/649480.html

[33] Global Initiative against Transnational Organized Crime. New front lines: Organized criminal economies in Ukraine in 2022, 2023. [2023-05-19]. https://1url.cz/wutIW

[34] EuroNews. Ukraine says cyber attack on Kyiv airport was launched from Russia, 2016. [2023-05-27]. https://www.euronews.com/2016/01/18/ukraine-says-cyber-attack-on-kyiv-airport-was-launched-from-russia

[35] Ukrinform. Crime rate down 13 % in Ukraine: Police chief, 2023. [2023-05-19]. https://www.ukrinform.net/rubric-crime/3633228-crime-rate-down-13-in-ukraine-police-chief.html

[36] Ukrinform. Almost 290,000 power generators imported into Ukraine, 2022. [2023-05-19]. https://www.ukrinform.net/rubric-economy/3642827-almost-290000-power-generators-imported-into-ukraine-since-nov.html

[37] Ukrinform. Enemy-spotting chatbot in Ukraine boasts over 344,000 reports, 2022. [2023-05-19]. https://www.ukrinform.net/rubric-ato/3544619-enemyspotting-chatbot-in-ukraine-boasts-over-344000-reports.html

[38] e-Vorog. [2023-05-19]. https://t.me/evorog_bot

[39] Ministerstvo tsyfrovoyi transformatsiyi Ukrayiny. e-Vorog, 2021. [2023-05-19]. https://www.youtube.com/watch?v=VTAxA3Omfmw