Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 5, 747-759
2024
Publisher: Learning Gate
DOI: 10.55214/25768484.v8i5.1740
© 2024 by the authors; licensee Learning Gate

Integrating digitization into public administration: Impact on national security and the economy through spatial planning

Orystlava Sydorchuk[1]*, Vitalii Bashtannyk[2], Fedir Terkhanov[3], Oleg Kravtsov[4], Liudmyla Akimova[5], Oleksandr Akimov[6]

[1]Department of Regional and Local Development, Lviv Polytechnic National University, Lviv, Ukraine; Sydorchuk.Orystlava@lpnu.ua (O.S.)

[2,3,4]Department of Public Administration and Local Self-Government, Dnipro University of Technology, Dnipro, Ukraine; AAA321_123@ukr.net (V.B.)

5Department of Labor Resources and Entrepreneurship, National University of Water and Environmental Engineering, Rivne, Ukraine; L_akimova@ukr.net (L.A.)

[6]Department of Public Administration, Interregional Academy of Personnel Management, Kyiv, Ukraine; 1970aaa@ukr.net (O.A.).

Abstract: The evolutionary development of the security sphere, on the one hand, and the rapid involvement of digital technologies (and, as a consequence, changes) on the other, formulate the first level of problematization of this study. The study seeks to provide evidence of how the dynamics of changes in the security sphere are formed by constructing an empirical model of changes and assessing the state security system within the framework of spatial planning under the influence of digital technologies. Particular attention in the study is paid to spatial planning and spatial development in smart cities the main threats to national security are systematized, located in closely intersecting planes of digital technologies, social processes, and economic interests. It is shown that areas covered by spatial planning, and particularly smart cities, pose a serious local threat to national and international security policy at the levels of political, social, technical, and economic governance.

Keywords: *Digitization, Economy, National security, Spatial planning.*

1. Introduction

The practice of defending against and preparing responses to the vast variety of security threats that affect cities and metropolitan regions, from natural catastrophes such as flooding and anthropogenic climate change to crime and terrorism, has been referred to as 'urban resilience' in recent years. In this view, urban resilience encompasses both design changes (structural, architectural, and land-use planning) as well as management and governance initiatives aimed at preventing or mitigating physical and social vulnerability in places, eventually protecting life, property, and economic activity. Furthermore, in recent decades, the threat of armed confrontations and hybrid warfare has grown dramatically, as seen by the examples of Ukraine and Israel, as well as high geopolitical tension in the Middle East. In these circumstances, digital transformation in public administration presents an additional problem to be handled, as an ineffective strategy of integrating digitalization into public administration might become a point of risk.

The idea of digital governance is understood differently across disciplines and theoretical viewpoints. The concept of digital governance has evolved significantly, both in terms of connotation and external extension of its significance, from the earliest forms of government governance to government informationization, e-government, and so on in the information age, and then to digital government, data governance, and so on in the current digital economy. Overall, governance in the

* Correspondence: Sydorchuk.Orystlava@lpnu.ua

digital age has undergone considerable changes: governance challenges are increasingly diversified, complicated, and ambiguous [1]. The advancement of digital technology has provided unparalleled ease to humanity, but it has also introduced new threats and concerns. These dangers and difficulties, in particular, are represented in spatial planning via the lens of national security.

Urban planners and defense planners have collaborated on a same purpose. However, there are inherent difficulties that impede these parties' efforts to apply military solutions to urban problems, particularly economic concerns.

2. Literature Review

Because of its variability and interdisciplinarity, spatial planning study has many crossovers with other disciplines. One important factor influencing how spatial planning works in a given setting is the relationship between spatial planning and the legal framework that enables it to function. Exploring this link is an important research task because it addresses issues connected to the legislation and execution of spatial development plans, land-use planning, regulatory instruments, and any other devices and administrative choices that affect space. Furthermore, spatial planning is a path-dependent activity that evolves and consolidates over time as a result of a variety of factors, including the aforementioned legal system, a country's administrative tradition, and the so-called spatial planning tradition. Finally, earlier solutions continue to impact spatial planning methods. Rather of contributing to convergence, policy mobility events promote overall diversity by borrowing structures that must be adjusted to the new setting in order to work under new conditions [2]. For these reasons, the practice of spatial planning varies greatly over the world. However, the security component in spatial design is becoming increasingly important.

In hazard management literature, urban resilience has typically been defined as primarily focused with natural disaster prevention and recovery.1 However, the phrase has recently taken on a new meaning as governments throughout the world use it to describe counterterrorism and national security measures. The major stated goal of these strategies is to limit terrorists' ability to penetrate targets and to take steps to lessen the consequences of successful strikes [3]. Although such concerns about terrorist threats (as identified by nation states and national governments) are global in scope and not new, they have been pursued more seriously in the United States and the United Kingdom since the attacks on New York and the Pentagon on September 11, 2001, and the suicide bombings on London's underground network on July 7, 2005. This is not to say that attempts to combat urban terrorism did not exist prior to these events, but rather that they acted as a catalyst for increased preventative measures being implemented in the planning, design, and engineering of areas deemed to be at higher risk, with increased emphasis on counter-terrorism as part of a broader and better funded urban resilience agenda.

At the same time, in the literature, spatial development is often defined as the improvement of the settlement system and territorial organization of the economy, in particular, through the implementation of an effective state policy of regional development. The goal of state regulation in this case remains the provision of sustainable and balanced spatial development, including the alignment of the economic and innovative development of regions. Spatial planning is an ongoing process, punctuated by changes in doctrines, frameworks and practices. These changes are often instigated at a national level, and then applied by regions and municipalities.

According to Borhani and Esmaeli [4], there are two aspects to spatial planning: developmental and defense-security. Given the significance of the defense-security component for a nation's overall security, large-scale territorial development plans should get particular consideration. A crucial tactic in this aspect of land use planning is to take passive defense factors into account, which help to lessen cities' physical-military vulnerability. These authors integrated multi-criteria decision-making models with geographic information systems (GIS) to conduct a geographical analysis of military-physical vulnerability with the goal of determining Zahedan's security and defense readiness. The maps' geographical analysis results demonstrate, on the one hand, that the city's northern region has the least risk and its core sections the most. However, the western perimeter of the city is less vulnerable than the eastern limit based on the research criteria. This serves as an illustration of current, realistic approaches to national security at the scale of spatial planning.

Back in 2004, J. Light, a professor at Northwestern University's School of Communication and Departments of History and Sociology (USA), asserted that defense planning will likely play a significant role in American cities going forward [5]. The researcher notes that the Cold War civil defense program is frequently cited as evidence that the problems that cities are now confronting are not wholly novel. Stories of how defense sector expansions spurred regional economic growth, how the National Interstate and Defense Highway Act created a national road network, how investments in national security changed the physical landscape of America, and how local leaders profited from increases in defense spending to fund their priorities suggest that, short-term financing issues notwithstanding, city officials will probably find ways to reap the rewards of homeland security investments.

Even a visual description of how urban managers may model their decision-making processes after weapon system manufacturers was provided in one of the Community Analysis Bureau's studies [6]. Figure 1 presents a comparison between the two ideas.

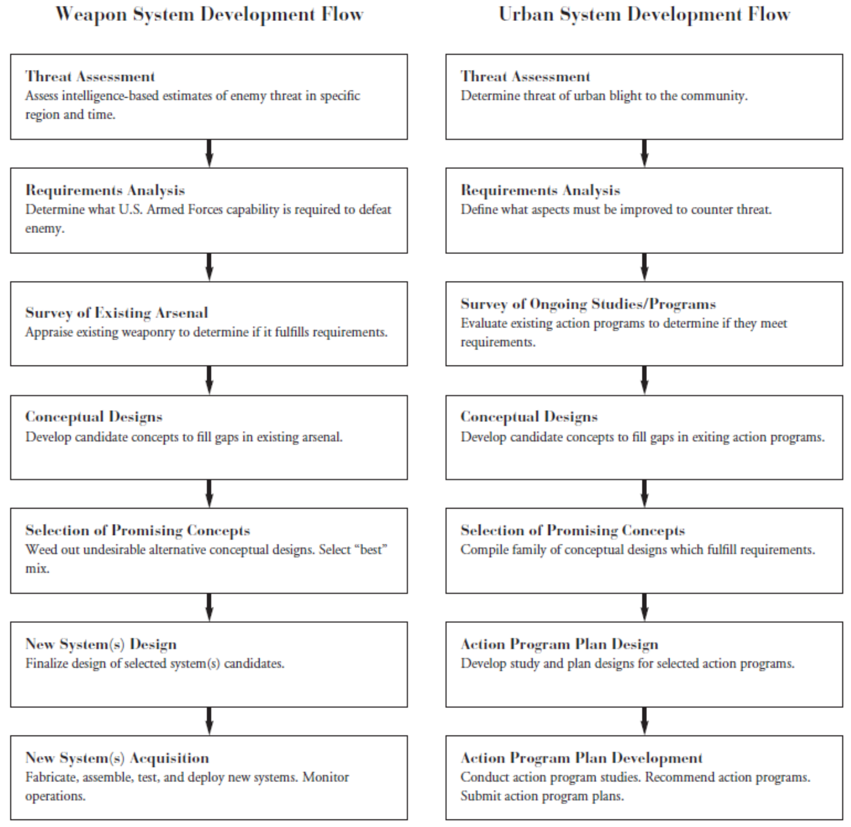
Weapon System Development Flow
Urban System Development Flow
Threat Assessment
Assess intelligence-based estimates of enemy threat in specific region and time.
Threat Assessment
Determine threat of urban blight to the community.
Requirements Analysis
Determine what U.S. Armed Forces capability is required to defeat enemy.
Requirements Analysis
Define what aspects must be improved to counter threat.
Survey of Existing Arsenal
Appraise existing weaponry to determine if it fulfills requirements.
Survey of Ongoing Studies/Programs
Evaluate existing action programs to determine if they meet requirements.
Conceptual Designs
Develop candidate concepts to fill gaps in existing arsenal.
Conceptual Designs
Develop candidate concepts to fill gaps in exiting action programs.
Selection of Promising Concepts
Weed out undesirable alternative conceptual designs. Select "best" mix.
Selection of Promising Concepts
Compile family of conceptual designs which fulfill requirements.
New System(s) Design
Finalize design of selected system(s) candidates.
Action Program Plan Design
Develop study and plan designs for selected action programs.
New System(s) Acquisition
Fabricate, assemble, test, and deploy new systems. Monitor operations.
Action Program Plan Development
Conduct action program studies. Recommend action programs. Submit action program plans.

Figure 1.
Here: Comparison of weapon system and urban system development flows [6].

This alignment is relevant today even more, but now – in the landscape of digital transformation, including digital transformation of both public management and process of spatial planning.

3. Research Methodology

The methodological basis of the study was the provisions of the theory of maintenance and functioning of public administration bodies, formation of the digital economy, information and resource support of state and municipal administration, electronic and digital support of public-private interaction processes and national security. The study used methods of system analysis, methods of generalization, classification, system and structural-functional approaches.

4. Results and Discussion

In the field of political science, security is examined from several angles, encompassing the political system itself (political survival at all levels: players, institutions, regime) as well as society (people, individual social sectors, etc.). Every level of digital technology serves two purposes: first, it creates a digital space where security is also required, leading to the formation of cybersecurity, information security, network security, and digital infrastructure; second, it reinforces and ensures security (e.g., a unified system of video surveillance cameras that allows for real-time recording of threats and taking appropriate actions to eliminate them). Digitalization has already had a major impact on the field of national security, and this impact will only grow as new technologies are developed and introduced.

Understanding how the collaboration between spatial planning/development experts and military experts developed and then broke down in Los Angeles in particular demonstrates how a shared understanding of the rapidly growing urban crisis as a national security crisis helped to turn urban planning concerns into strategic challenges that needed to be addressed by deploying techniques and technologies of command, control, computers, communications, intelligence, surveillance, and reconnaissance. However, in the end, this shared understanding was unable to eliminate the underlying tensions that separate military from urban operations [7]. Calvin Hamilton's 1964 appointment as head of planning for Los Angeles served as a spark for the first technology transfer partnerships. Hamilton was originally from Pittsburgh, where he had assisted the city in becoming the first in the country to implement military information management advances for the management of its Community Renewal Program. One of Hamilton's top goals when the Pittsburgh department took on the task of renewal planning was to create "a concept of an information system [that went] well beyond that which we have normally thought of" [7]. The answer was clear to Hamilton: the department jumped into simulation right away, using the models and techniques developed by the RAND Corporation for the Strategic Air Force Command and other social science simulations. Hamilton wanted his team to take more technical and scientific approaches to municipal operations, carrying over from his work in Pittsburgh into Los Angeles. To this purpose, the Los Angeles Planning Department launched a number of programs. One program that was started in 1965 was the Mathematical Model Development Program, which aimed to develop a collection of cybernetic urban models that could be utilized by the city's computers. Combining cybernetics, data processing, and computer simulations led to the development of decision aids for war games, command-and-control computer systems like the Air Force's Semi-Automatic Ground Environment (SAGE), an early air defense system, and efforts to enhance military operations. Subsequent reports from the city planners explicitly stated that urban issues were now security risks, which made the need to spend more in information management techniques drawn from military planning clear [7].

In Los Angeles, which is home to many of the top aerospace industries and think tanks in the country, there have been particularly strong efforts to leverage the knowledge and technologies from the defense community to enhance renewal planning. However, the experience in Los Angeles was not unique. City authorities in the United States in the late 1960s and early 1970s used the national attention-grabbing incidents of urban violence to their advantage, arguing that it was critical to adopt a more technologically advanced strategy to enhance living conditions in the country's cities. Urban security concerns and the general consensus that military and urban planning are fundamentally similar led to a number of meetings, joint ventures, and technology transfer projects that eventually resulted in the creation of urban information systems in several cities.

But since today's technology differ from those of the past, domestic social welfare planning is not now included in the definition of "homeland security planning". Nonetheless, while choosing which of these technologies, if any, to implement, local officials need to exercise caution. Technical systems' essential elements are people, organizations, and funding. History shows that comparable inventions have varied outcomes according on the context in which they are used.

In the paper "Evolving security motifs, Olympic spectacle and urban planning legacy: from militarization to security-by-design", Jon Coaffee [8] notes that as militarized security regimes have grown more commonplace during the Olympics, urban planning has played a more important role in these security operations by incorporating security features that are built to lessen the impact of any potential terrorist attack. By creating a variety of more socially engaging public areas that are guarded by more covert and ecologically friendly security equipment, these protective elements also give the host city a permanent physical legacy of safety, security, and crime prevention. The majority of Olympic organizers now have to make preparations that involve trying to "design-out" terrorism by using highly militaristic strategies and costly, comprehensive contingency planning, as well as equating spectacle with safety. By adopting the principles of security-by-design, the Games-time security infrastructure becomes a less noticeable but enduring physical legacy that can support local initiatives for crime prevention, climate resilience, and regeneration. This marks a high point in the practice of spatial planning. In her last thoughts, Coaffee considers how future Olympiads will strike a balance between planned security and spectacle as a result of the security infrastructure's ongoing growth. By analogy, it can be said that in overall, spatial planning today implies balancing and alignment between security, convenience / social benefits, and economic rationality. Digitalization, integrated into public administration, can both bring benefits and create challenges.

Bella Permata [9] examines the connection between national security and geographical data. She states that the information that characterizes objects, events, or other features that are located on or near the earth's surface is referred to as spatial data, according to IBM. In general, it has to do with location data. It is vital to the security of the country. from recognizing, evaluating, reacting, and organizing actions. Its significance in providing accurate and fast data gathering and analysis can assist the government in spotting potential terrorist threats in public spaces or tracking the possible movement of enemy troops. Spatial data is therefore required to maintain national security. To put it succinctly, given the current pace of advancements in geospatial technology, spatial data has untapped potential for decision-making. Incorporating geographical data into government data collection, management, and distribution processes is essential for making full use of it when it comes to national security and related intergovernmental procedures. Wide-ranging access to spatial development is made possible by digital technology, and this creates a kind of landscape of risks.

According to Permata [9], too many sources are available for a project that is only a layer or map. Each ministry or organization has a different source for obtaining the same field file. It complicates and prolongs the process of gathering, integrating, synchronizing, and distributing geographical data. As a result, there is a chance that many places in this terrain have digital vulnerabilities. This is only one of many problems that spatial planning faces as a result of public administration's integration of digitalization.

Since the preparation and application of strategic plans founded on audacious ideas by urban and metropolitan regions worldwide in the 1990s, strategic spatial planning has experienced broad adoption. In addition to addressing issues related to spatial organization, their objective was to direct these areas' future growth in a way that would improve their standing in the global urban network and draw tertiary economic activity, particularly in the highest-value industries [10]. The content and methods of the new strategic spatial planning are different from those of the previous kind, and these distinctions are based on the planning's guiding principles. Experts point out that this kind of planning entails analyzing structural difficulties and obstacles critically as well as coming up with innovative ideas for potential fixes and strategies for implementing them.

Chigbu and Kalashyan [11] suggest the schematic depiction of relationship between land-use planning and public administration (see Fig. 2).

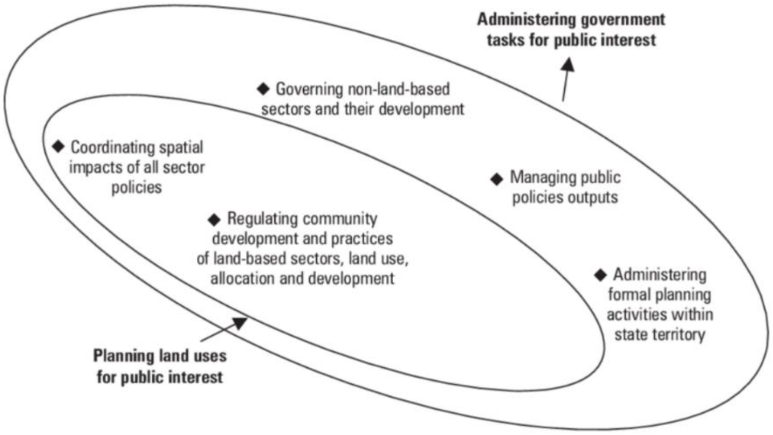
Administering government tasks for public interest
◆ Governing non-land-based sectors and their development
◆ Coordinating spatial impacts of all sector policies
◆ Managing public policies outputs
◆ Regulating community development and practices of land-based sectors, land use, allocation and development
◆ Administering formal planning activities within state territory
Planning land uses for public interest

Figure 2.
Here: Relationship between land-use planning and public administration [11].

However, the resilience concept should be applied to these interactions. Specifically, urban resilience offers a fresh perspective on and method for handling vulnerability and unpredictability. An alternate paradigm for planning techniques is provided by urban resilience [12].

Urban buildings can be influenced by spatial design in a way that reduces cities' susceptibility to several hazards. But the issue remains: What constitutes the urban structure? Three definitions of urban structure are found in contemporary literature:

1. Physical/environmental structure. This implies the buildings, infrastructure, and communication network that make up the settlement structure, as well as the network of green spaces that include parks, rivers, and other areas.

2. Socioeconomic structure: How social groupings are distributed, how money is distributed, how cohesive the economy and society are, etc.

3. Institutional structure; it includes things like the institutions' hierarchy, the public's legitimacy of their judgments, the number and caliber of their staff, their level of responsibility, and their level of collaboration and coordination.

Some scholars include in this list digital structure [13]. However, in our opinion, digital structure is a framework uniting all these three elements, since in modern cities and other territories' structures, as well as in their public management, digital systems is a foundation for functioning.

The way governments run cities is being revolutionized by the Internet of Things (IoT). These days, it is possible to link and remotely monitor every facet of city life, including trash management, housing, community development, energy and water management, health care, security, and mobility. Often referred to as "smart cities", these local governments use technology to better serve their citizens' needs and operate more efficiently.

The infrastructure of smart cities is made up of three levels, according to the Institute of Defense and Business (IDB). A critical mass of sensors, networks, and cellphones linked by a fast communication network constitutes the first. Data on energy use, traffic volume and trends, pollution levels, and other topics are gathered using that technological base. Applications for continuously analyzing raw data streams are used in the second layer to forecast use and trends and provide warnings, insights, or suggested actions. Thirdly, public support and involvement are essential to increase data availability and establish a genuine open-access system that enables individuals and organizations to use information for their own objectives [14]. Many smart technologies have already been implemented in cities like Singapore, Dubai, and New York City, but since there are so many linked devices, these networks are a perfect target for bad actors and hackers who want to disrupt the system or exploit it for

DOI: 10.55214/25768484.v8i5.1740

financial benefit. The following are the main cybersecurity threats that smart cities must proactively guard against.

However, there is also the fourth element, which is somehow overlooked in – it is critical infrastructure and defense issues.

As Dandan Jin [1] correctly points out, public governance has many potentials as well as obstacles in the current digital era. Significant obstacles include cybersecurity concerns, the digital divide, and regulatory difficulties; nevertheless, potential include improved service delivery, transparency, and data-driven decision-making. Through the appropriate management of these obstacles and the strategic utilization of digital technology, governments may enhance the efficacy, responsiveness, and public involvement of governance. However, defense-related concerns now take up a far larger space in proper public administration and geographical planning. However, economic concerns may run counter to defense-related goals. Smart city initiatives are frequently portrayed as brand-new utopias that are constructed from the ground up with a strong emphasis on optics and aesthetics: how the city appears from above or from a distance, with towering, shiny skyscrapers covered in or surrounded by greenery (for "sustainability purposes") and populated with stylized, carefree people. Naturally, there is no insecurity in these beautiful depictions. The interest and business relationships of a territory with hostile governments and organizations provide another possible source of economic vulnerability. These linkages are typically subtle and difficult to identify. Urban security is a subject where smart tools are actually put to the test in existing cities.

In the era of hybrid warfare, sustainable public administration within spatial planning becomes even more complicated, in particular due to infrastructure issues.

Specialists believe that infrastructures may be conceptually classified into three main categories: common infrastructures, special infrastructures, and essential infrastructures [15]. The fact that these three categories are related to one another and can alternate between them based on the security and safety of the processes or systems whose components they are is a crucial characteristic. As a result, the infrastructure becomes crucial because of the significance of its destination and the adverse consequences it causes - whether it is destroyed or utilized in hybrid warfare tactics and strategies.

President Bill Clinton of the United States of America issued "The Executive Order 13010 for the Critical Infrastructures Protection" on July 15, 1996, which marked the beginning of the institutionalization of concerns about the definition and protection of critical infrastructures. For the purposes of this statement, critical infrastructures were those vitally important national facilities whose loss or incapacity may have major repercussions, especially for the defense or economic security of the United States. The following are listed in the Executive Order as essential infrastructure: banking and finance; emergency services (fire, police, and ambulance); telecommunications; power systems; fuel depots and transportation networks; and the stability of the government. Executive Order 13231, "Critical Infrastructure Protection in the Information Age", was subsequently issued during the Bush administration in the wake of the September 11, 2001 events. This executive order was more comprehensive than the previous one, defining critical infrastructure as any physical or virtual system or goods /means that are so important to the United States that their incapacity or destruction may affect public health and safety, military and/or economic security, or any combination of the aforementioned [16].

Thus, the communications system architecture, the infrastructure ensuring mobility in the three spaces of manifestation, the spaces/means of securing resources, the spaces ensuring the operation of institutions with authority over state governance, and the spaces guaranteeing safety and national security are the most crucial components of critical infrastructures. Today, computerization is given considerable attention, particularly because of its worldwide nature, which has led to the identification of the twenty-first century as the age of cyberspace.

In June 2016, during the NATO Defense Ministers' meeting in Brussels, Belgium, Secretary-General Jens Stoltenberg emphasized the significance of cyberspace, saying that "most crises and conflicts of today have a cyber dimension" and that "treating the cyber world as an operational domain, would allow us to better protect our operations and missions". Cyberspace is recognized by NATO as an operational field of war, alongside the land, air, and sea spaces.

There is no question in the minds of many concerned with security today that hybrid warfare is a tactic used in the Cold War and that cyberattacks are one of its weapons. The execution of countermeasures must accelerate in light of these two facts.

In the case of a hybrid-type crisis, the space for force engagement at the NATO level is assessed based on the PMESII (political, military, economic, social, infrastructure, and information) pillars. The space of some regions of the world, including those far apart, where political, economic, spiritual, and other interests are maintained or promoted (by force of arms as well), strategic interest space (an area or a land or sea region in the vicinity of national territory), and the national territory are among the development spectrum of warfare asymmetric actions, such as the hybrid war, according to some military specialists [17].

The usage of cutting-edge technology like cloud computing, big data analytics, IoT, and AI has surged dramatically as smart cities become more commonplace. Urban surroundings might become more sustainable and efficient with the help of these technologies, but they also present new security issues that need to be resolved. The possible security risks connected to the most popular developing technologies utilized in smart city initiatives were determined by a Telo [18] research. The survey discovered that DDoS assaults, device vulnerabilities, and data breaches were the most risks to IoT devices. The most common hazards associated with cloud computing were malware attacks, insider threats, and data breaches. The biggest challenges to big data analytics were adversarial assaults, unforeseen effects, and data breaches. Lastly, it was determined that the biggest security issues facing AI were adversarial attacks, model flaws, and privacy concerns. Policymakers, city planners, and technology suppliers may create complete security policies for smart cities by using the insights this study offers to detect possible security risks and suggest appropriate responses.

Rather than using conventional military tactics, hybrid tactics take use of social, political, and economic weaknesses in addition to military ones in order to destabilize targets. European policymakers are growing more concerned about Moscow's use of hybrid assaults and the threat they represent to vital infrastructure following Russia's invasion of Ukraine in February 2022. Concerns about the risks presented by Russia's hybrid strikes have grown in response to suspicious events including the interruption of trains in Germany, the damage of communication cables in France, and GPS anomalies in Finland [19]. To increase the resilience of their vital infrastructure, European nations have taken action. While France, Italy, and the UK have made investments to safeguard undersea infrastructure, Norway, Denmark, and the Netherlands have increased security around critical energy infrastructure, and Czechia has released a national policy aimed at fending against hybrid threats.

Pestana and Sofou [20] investigate how business process management and data governance might be integrated to counter the dangers posed by hybrid attacks that target critical infrastructure weaknesses. In order to safeguard sensitive data and digital assets and to guarantee stakeholder collaboration in situations involving cross-border decision-making, the research highlights the significance of information security. The importance of data governance in thwarting hybrid assaults on critical infrastructures (CI) is examined. The suggested paradigm for understanding hybrid threats as multifaceted, time-sensitive issues is shown with an example from an airport, with an emphasis on possible assaults against CI. The following are the primary conclusions made in the paper:

- Hybrid threats, which primarily target critical infrastructure (CI), take use of flaws in digital infrastructure to erode public confidence in democratic processes and security.
- Establishing ownership, accountability, and verifiability frameworks for digital information distribution during emergencies can be aided by data governance in the fight against hybrid assaults.
- By strengthening response awareness, proactive security escalation, and thorough logging for non-repudiation, data governance and business process management together improve response efforts and lessen the impact of cascading assaults.

- Digital assets are safeguarded by the combination of proactive tactics and the information security lifecycle, which includes knowledge management, detection, prevention, and reaction for incident mitigation.

- In order to effectively respond to emergencies in vital infrastructures such as airports, it is important to implement strong data governance frameworks that increase resilience against hybrid threats, encourage trustworthy information flow, and facilitate stakeholder engagement.

The following are the consequences of the paper's primary findings [20]:

- Enhanced Resilience: By creating responsibility, guaranteeing data integrity, and promoting quick reaction awareness, data governance frameworks strengthen cybersecurity infrastructure (CI) against hybrid attacks.

- Better Response Coordination: By combining data governance and business process management, cascade impacts of CI assaults may be mitigated by thorough logging for non-repudiation, proactive security escalation, and efficient response coordination.

- Stakeholder Collaboration: In order to guarantee the validity and integrity of information shared during emergencies, airport authorities, airlines, security agencies, and other stakeholders must work together.

- Proactive Security Measures: To protect data integrity and stop illegal alterations, the study highlights the importance of proactive security measures including encryption, access restrictions, and lineage tracking. This strengthens defenses against hybrid assaults.

- Ensuring data safety, correctness, and integrity through data governance frameworks enables decision-makers to make well-informed choices, preserve data dependability, and mitigate the risks associated with erroneous information or improper data handling. This improves the security posture of CI as a whole.

Data governance in the context of CIs and emergency response scenarios entails comprehending the patterns of content circulation that underpin this environment in order to trace the evolution of digital information dissemination during emergencies [21]. This makes it possible to create a chain of proof at each point in the data's journey by establishing a responsible and verifiable ownership structure. It includes a thorough structure that specifies data security, correctness, integrity, and administration. This data governance framework includes developing policies, methods, and standards covering many concerns including quality, security, privacy, and compliance with applicable regulations in order to guarantee data protection and suitability for purpose [22]. By developing a methodical and consistent approach to data management, data governance assists decision makers in making well-informed decisions, protecting accuracy and integrity, and managing risks associated with incomplete or badly handled data.

Collaboration, unambiguous communication, and well-defined responsibilities for responsibility are essential for effective data governance. This framework consists of procedures for maintaining data correctness through quality controls, integrity checks, and audits as well as procedures for managing, safeguarding, and monitoring data, enforcing policies, and preventing unwanted access. Access restrictions, lineage tracking, and encryption are some of the methods used to protect data integrity and stop illegal changes. Integrity controls ensure that datasets are reliable by detecting changes or discrepancies through the use of hash functions or checksum techniques [23].

While the national security system is a common target of cyberwarfare, considerably less research has been done on the equally dangerous weaknesses in municipal administration. In this work, we investigate the possible effects of cyberwarfare aimed at smart cities as well as the connection between cyberattacks and urban social disturbance. In order to uncover operational, procedural, governance, and skill deficiencies in responding to and constructing resilience against fictitious but plausible occurrences, Soare and Burton [24] provide a foresight scenario. In a future scenario, a network of hackers connected to an authoritarian, revisionist regime launches a persistent cyberattack on Megalopolinn, the capital of a significant NATO partner in Europe. The writers outline the many avenues for cyberattack in a smart city grid and show how, when paired with other hybrid warfare strategies, they might seriously undermine the social, political, and technological systems and procedures of the city. The scenario posits that Megalopolinn's 5G servers and transmission masts are rendered inoperable by widespread Distributed Denial of Service (DDoS) assaults that leverage the city's millions of IoT gadgets. A self-replicating and self-learning worm has entered the smart city's master network and is quickly spreading throughout the smart critical infrastructure grid. In a matter of hours, the virus spreads throughout the grid's various sectors, taking down City Hall systems and interrupting law enforcement's and emergency services' GPS functions. This situation is obviously quite likely to occur in real life.

Such forward-looking situations show that smart cities are architecturally fragile. From the perspectives of technology, society, and government, they have several points of failure that have cascading, systemic repercussions. The goal of Soare and Burton's foresight scenario is to increase awareness of less obvious hazards and vulnerabilities - in this example, the interdependencies between local government, social order, and smart city grids - rather than to paint a picture of the future. The scenario also illustrates how security vulnerabilities associated with smart cities may impact national security as a whole and with allies.

Cyber dangers specific to smart grids and other smart city services are constantly evolving. As an illustration, the outcomes of the GridEx III "cyberwar games" conducted by the North American Electric Reliability Corporation (NERC) exposed serious issues with grid operators' cyber threat intelligence procedures (see Fig. 3) [25]. According to 98 percent of participants in a Dimensional Research study, cyberattacks are a possibility for smart cities. Smart grids, transit, security cameras, wastewater treatment, and other municipal services are all managed by smart cities using IT technology.

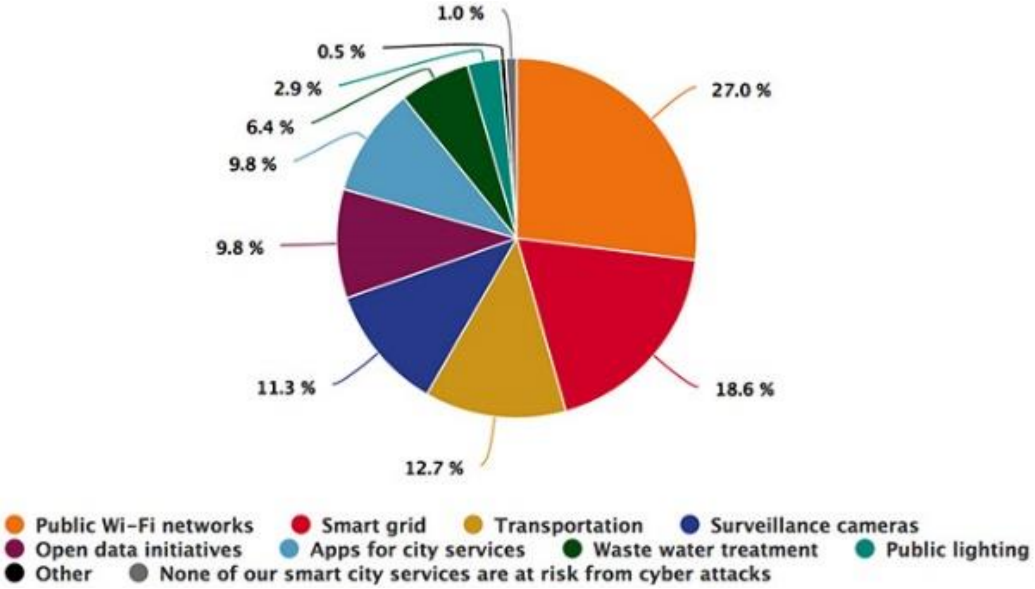

Figure 3.
Here: Risks of cyber-attacks on smart cities grid [25].

Scholars began to incorporate cities in IR studies due to two growing themes. The first was the trend of globalization, which made cities more significant from a political, economic, and military standpoint as well as in their capacity as command posts and planning hubs [26]. The globe became "flat" due to the consequences of globalization and the quick spread of information and communication technology. Changes made globally had an impact locally and vice versa. The second trend has to do with urbanization, which has been fueled by factors such as globalization, the expansion of industry and foreign markets, the increase of service-driven economies and employment prospects, and the collapse of rural economies and ways of life. More than half of the world's population has lived in cities since 2016; by 2050, this number is expected to increase to two thirds, or 7 billion people [27].

Recent studies have shown how heavily dependent vital smart city infrastructure is on services that are typically organized at the federal level, such as 5G mobile networks, GPS, and satellite-based services. Local government officials are rarely, if ever, involved in policy-making processes, despite the fact that their everyday operations rely heavily on these technology [28].

The dense smart city infrastructure reframes the city for its residents as a "platform for services" [29]. Applications that GPS-track and predict the arrival time of public transit (buses, subway, trains), online tax submission, healthcare applications, and other services are made available by local governments. Safety, sustainability, equality, and resilience need to be given more consideration in the design and management of smart cities, according to recent study from Carnegie Mellon University. The UN issues a warning, noting that while smart urbanization and technology advancement can be vital avenues for promoting social inclusion, they can also exacerbate social inequality. The influence on smart city infrastructure is shaped in part by the pre-existing social structure of a city. Due to its brittleness and susceptibility to social biases, private tech companies refuse to offer face recognition technology for use in smart policing applications utilized by local law enforcement agencies around the United States [30]. The skilled labor and investments in cutting-edge, secure technologies required to implement smart city initiatives safely are beyond the means of less wealthy communities, which also exacerbates rather than lessens social exclusion and unequal access to improved local government, public services, and higher living standards. A poorly considered strategy for incorporating digitization into public administration within the context of spatial planning and development is likely to cause a digital gap and increase the risk of rioting. With the aid of social networks, this is also a favorable environment for social engineering. For instance, the 2018 NATO Capstone Concept on Urban Warfare takes into account how a city's socioeconomic structure affects military operations' security and effectiveness. Even the literature on data privacy emphasizes the technological rather than the social factors. Contrary to popular belief, the literature on smart city infrastructure virtually never addresses the social structure of the city as a component of its critical infrastructure, including psychological and behavioral aspects of the city, problems with social cohesiveness and group identity, and concerns with social justice and equality. This is a significant disparity in light of the fact that 84% of cyberattacks and misinformation rely on social engineering [31].

Despite the transatlantic region's adoption of cyber security standards, protections, and authentication methods, new technologies and components introduced to smart city networks, such sensors and IoT devices, remain susceptible. An increased density of overcrowded networks has resulted from the focus on lowering network latency and boosting broadband access, which is especially important during times of crisis when networks see sudden surges in data usage [32]. These networks are fragile and prone to failure since they cannot support all users and Internet of Things devices. Supervisory control and data acquisition (SCADA), an automated control system that has been shown to be a substantial and multifaceted single point of failure in smart city grids, is used by the majority of water and energy contractors, who also follow diverse cyber security standards [29]. Security of a networked system like a smart city depends on its weakest link. The high degree of interconnectedness between the data and the systems that rely on it in smart cities means that any corruption or disruption in one area of the puzzle may have significant ripple effects throughout the entire grid. Critical services including the police, fire, emergency medical services, power grids, and financial markets can all be affected by jamming and spoofing GPS signals [28]. Small, commercially accessible drones may be used to quickly generate these effects.

Paradoxically, security-by-design methods to the technology and services purchased are still not receiving enough attention in public procurement. Despite their high costs, local procurement of new services and technologies may be given priority over maintaining older systems that are already installed in the critical infrastructure grid in order to increase public exposure. For instance, a 2018 UK

DOI: 10.55214/25768484.v8i5.1740

government assessment indicated that upgrading national and local broadband networks would cost £33.4 billion over a ten-year period. However, if authorities rebuilt the infrastructure gradually over a longer period of time, the estimate might be as low as 30%. In the transatlantic region, protracted periods of fiscal austerity have increased the likelihood of long-term local underinvestment in vital infrastructure.

The noteworthy (but also profit-seeking) effort to overcome the technological and cyber security concerns brought by developing smart city infrastructure has been spearheaded by the private sector. Prioritizing data security and integrity (particularly in the context of 5G networks), implementing failsafe and overriding mechanisms (particularly for large-scale command systems), controlling access, encrypting data, updating security protocols on a regular basis, patching software, deploying network intrusion mechanisms, and providing staff training are just a few of the technical solutions available [33]. Despite the availability of technology solutions, state and non-state actors can engage in cyber or hybrid disruption below the line of force, using both military and civilian socio-technological instruments to reward the disruptor. It is comparatively inexpensive (for example, dark web ransomware can be purchased for less than $50), it gives the attackers income from ransomware premiums, and it is widely known due to the disruption that the attacks cause to local government and public services over several days or months [34]. Local governments bear significant financial and public trust costs as a result of cyberattacks on smart city grids. While not the exclusive means, technological weaknesses play a significant role in the instigation of cyber warfare.

Resilience in these circumstances can only be attained by careful study, best practices, and striking a balance between the public and private sectors' competing economic interests. Urban planners may need to adopt hybrid management solutions in order to manage smart city initiatives that involve complex factors like new technologies, despite the traditional division between public and private entities. This is especially the case when multidisciplinary and complex skills are needed.

5. Conclusion

The technical, social, economic, and political governance levels of national and international security policy face a very significant local threat in the twenty-first century from areas covered by spatial planning, and particularly from smart cities. In these conditions, integrating digitization into public administration in frames of spatial planning and spatial development should obligatory consider impact on national security and the economy, being a mandatory part of spatial planning projects, based on matrix approach covering all the above described elements of national security variable in spatial planning.

This is by no means a call for territorial and city planners to completely cut ties with the defense community, as this piece makes clear. In the event that safeguarding metropolitan regions continues to be a top priority for the country, it will be prudent to seek guidance on some issues from the defense specialists of that country. However, when these partnerships take shape, region/city administrators will need to discuss precisely what homeland security planning should include and establish precise boundaries for the scope of subsequent partnerships.

Copyright:

References

[1] D. Jin, "The Challenges and Opportunities of Public Governance in the Digital Era," International Journal of Social Sciences and Public Administration, 2(3), pp. 472-478. 2024.

[2] R. Thakur et al., Urban and Regional Planning and Development: 20th Century Forms and 21st Century Transformations. New York, Springer, 2020.

[3] J. Coaffee and P. O'Hare, "Urban resilience and national security: the role for planning," Urban Design and Planning, 161(4), pp. 173-182, 2006.

[4] K. Borhani and Sh. Esmaeli, “Defense-security planning of cities using spatial analysis of physical and military vulnerability (Case study: Zahedan),” Journal of National Security, 11(39), pp. 405-430, 2021.

[5] J. Light, “Urban Planning and Defense Planning, Past and Future,” Journal of the American Planning Association, 70(4), pp. 399-410, 2004.

[6] T. Quiggin, Seeing The Invisible: National Security Intelligence In An Uncertain Age. Hackensack, World Scientific Publishing, 2007.

[7] V. Eick and K. Briken, Urban (In)Security: Policing the Neoliberal Crisis. Ottawa, Red Quill Books, 2013.

[8] J. Coaffee, “Evolving security motifs, Olympic spectacle and urban planning legacy: from militarization to security-by-design,” Planning Perspectives, 39(3), pp. 637-657, 2024.

[9] B. Permata, “Spatial Data Relation to National Security,” Medium, September 26, 2023. https://medium.com/@bellaaprmt/spatial-data-relation-to-national-security-9f23f0cce834

[10] E. Thoidou, “Strategic spatial planning in the era of crisis: Current trends and evidence from the metropolitan area of Thessaloniki,” Spatium, 30, pp. 12-17, 2013.

[11] U. Chigbu and V. Kalashyan, “Land-Use Planning and Public Administration in Bavaria, Germany: Towards A Public Administration Approach To Land-Use Planning,” Geomatics Landmanagement and Landscape, 4(1), pp. 7-17, 2015.

[12] P. Lu and D. Stead, “Understanding the notion of resilience in spatial planning: A case study of Rotterdam, The Netherlands,” Cities, 35, pp. 200-212, 2013.

[13] H. Hosoya et al., Eds., The Industrious City: Urban Industry in the Digital Age. Zürich, Lars Müller Publishers, 2021.

[14] L. Suzuki and A. Finkelstein, Data as Infrastructure for Smart Cities (Computing and Networks). London, The Institution of Engineering and Technology, 2019.

[15] W. Gao, Digital Analysis of Urban Structure and Its Environment Implication (Advances in 21st Century Human Settlements). London, Springer, 2023.

[16] D. Ionita, “Space – An Essential Feature of the Hybrid War,” Land Forces Academy Review, XXII(1), pp. 5-9. 2017.

[17] O. Fridman et al., Hybrid Conflicts and Information Warfare: New Labels, Old Politics. Boulder, Lynne Rienner Publishers, 2018.

[18] J. Telo, “Smart City Security Threats and Countermeasures in the Context of Emerging Technologies,” International Journal of Intelligent Automation and Computing, 6(1), pp. 31-45. 2023.

[19] H. Pillay, Protecting Europe’s Critical Infrastructure from Russian Hybrid Threats. London.2023 Centre for European Reform. 2023, 11 p.

[20] G. Pestana and S. Sofou, “Data Governance to Counter Hybrid Threats against Critical Infrastructures,” Smart Cities, 7(4), pp. 1857-1877, 2024

[21] R. Abraham, J. Schneider, J. Vom Brocke, “Data governance: A conceptual framework, structured review, and research agenda,” International Journal of Information Management, 49, pp. 424-438. 2019.

[22] J. Rascao, “Data Governance in the Digital Age. In Handbook of Research on Digital Transformation and Challenges to Data Security and Privacy (pp. 34-62). IGI Global. 2021.

[23] M. Micheli, M. Ponti, M. Craglia, A. Berti Suman, “Emerging models of data governance in the age of data fixation,” Big Data & Society, 7(2), 2053951720948087. 2020.

[24] S. Soare and J. Burton. Smart Cities, Cyber Warfare and Social Disorder. Tallinn, CCDCOE. 2020.

[25] R. Andrade et al., Cybersecurity Risk of IoT on Smart Cities. London, Springer, 2021.

[26] S. Gongadze, “The Emergent Role of Cities as Actors in International Relations,” E-International Relations, August 6, 2019. https://www.e-ir.info/2019/08/06/the-emergent-role-of-cities-as-actors-in-international-relations/

[27] H. Ritchie and M. Roser, Urbanisation. Our World in Data, 2018. ourworldindata.org/urbanization

[28] S. Polunsky, “The City-Sized Hole in U.S. GPS Planning,” Belfer Center, Harvard University Kennedy School, Homeland Security Policy Paper #3. 2019.

[29] R. Kitchin and M. Dodge, M., “The (In)Security of Smart Cities: Vulnerabilities, Risks, Mitigation, and Prevention,” Journal of Urban Technology, 26 (2), pp. 47-65. 2017.

[30] J. Greene, “Microsoft won’t sell police its facial-recognition technology, following similar moves by Amazon and IBM,” Washington Post, June 11. 2020. https://www.washingtonpost.com/technology/2020/06/11/ microsoft-facial-recognition/

[31] European Union Agency for Cybersecurity. ENISA Threat Landscape 2020. https://www.enisa.europa.eu/publications/enisa-threatlandscape-2020-main-incidents

[32] A. Afflerbach, “Broadband Performance is About More than Speed,” CTC Technology, 2019. https://www.ctcnet.us/blog/broadband-performanceis-about-more-than-speed/

[33] Deloitte Center for Government Insights, “Making smart cities cybersecure,” 2019. https://www2.deloitte.com/content/dam/Deloitte/de/Documents/risk/Report_making_smart_cities_cyber_secure.pdf

[34] M. Fernandez, et al., “Ransomware Attack Hits 22 Texas Towns, Authorities Say,” New York Times, 20 August, 2019. https://www.nytimes. com/2019/08/20/us/texas-ransomware.html