THE "A-SPATIALITY" OF CYBERCRIME AND ITS CONNECTION TO THE URBAN ENVIRONMENT

Georgios Germanos[1]

ABSTRACT

This article investigates the concept of *a-spatiality* in relation to cybercrime, examining the ways in which digital criminal activities transcend conventional spatial constraints while simultaneously engaging with the dynamics of urban environments. Addressing a critical gap in existing research, the study explores how urban infrastructure, socio-economic disparities, and public vulnerabilities mediate both the prevalence and consequences of cybercrime. Integrating theoretical perspectives from digital geography and criminology, the paper conceptualizes cybercrime as an inherently urban phenomenon, situated within interwoven digital and physical networks. By examining diverse urban typologies - such as smart cities, global hubs, and informal settlements - it illustrates how these environments shape both exposure and resilience to digital threats. Particular emphasis is placed on the implications for policing, governance, and prevention strategies within increasingly decentralized and technologically mediated contexts. The article concludes by underscoring the urgency of developing adaptive urban policies and fostering cross-sectoral collaboration to address the evolving cyber threat landscape in digitized urban spaces.

Keywords: Cybercrime, A-spatiality, Urban infrastructure, Digital policing, Prevention, Socio-technical systems

[1] Phd Candidate, Department of Informatics and Telecommunications, University of Peloponnese, Tripolis, Greece. Email: germanos@uop.gr ORCID: https://orcid.org/0000-0001-7682-4573

Introduction

Cybercrime is one of the most pressing issues of our time, reshaping how we think about crime, space, and victimization. Unlike traditional crimes that happen in physical, bounded environments, cybercrime occurs in an unbounded, diffuse digital world that isn't limited by geography. This separation, known as "a-spatiality," raises important questions about how we understand crime locations, the relationships between criminals and their victims, and how urban infrastructures can either facilitate or buffer against these harms.

The term "a-spatiality" highlights how geographic space is becoming less significant in digital interactions. This challenges traditional criminological theories that suggest crime depends on physical proximity. Even though the perpetrator and the victim may never be in the same physical location, cybercrime can cause serious and immediate harm. This new understanding of spatiality has significant implications for urban policy, policing techniques, and criminological theory.

Urban settings are particularly relevant to this discussion. Cities, with their abundance of digital infrastructure like data centers, public Wi-Fi, and Internet of Things (IoT) networks, are hubs of connectivity. They also have socioeconomically diverse populations with varying levels of access to cybersecurity resources and expertise. These dynamics create a complex interaction between physical urban environments and a-spatial digital threats, where structural inequality, technological saturation, and a lack of institutional capacity to respond effectively all increase vulnerabilities.

This article aims to explore how the material and social realities of urban life interact with the a-spatial nature of cybercrime. It examines the theoretical foundations of a-spatiality and cybercrime, investigates how urban infrastructure can either encourage or discourage cybercrime, and assesses the socioeconomic factors that influence victimization in urban environments. Finally, it addresses the challenges that a-spatiality poses for law enforcement and suggests ways to adapt policies and build urban resilience.

The article is structured as follows: Section 1 introduces the theoretical background, including definitions of cybercrime and the concept of a-spatiality; Section 2 examines the role of urban infrastructure in facilitating or constraining cybercrime; Section 3 analyzes

socio-economic risk factors influencing cybercrime victimization in urban areas; Section 4 addresses law enforcement and governance challenges posed by a-spatial threats; Section 5 proposes policy measures to enhance urban cyber resilience; and Section 6 concludes with reflections and recommendations for future research and practice.

1. Theoretical background

Definition of cybercrime

Cybercrime is a constantly evolving challenge that covers a wide range of illegal activities made possible by digital technologies. Experts usually divide cybercrime into two main types: cyber-dependent crimes, which rely on digital infrastructure (like hacking and spreading malware), and cyber-enabled crimes, which are traditional crimes enhanced by technology, such as fraud or harassment (Gordon & Ford, 2006; Al-Khater et al., 2020).

The Cambridge Cybercrime Centre offers a practical classification that further explains this distinction. They point out that cyber-dependent crimes are fundamentally technological, while cyber-enabled crimes are traditional crimes that have been transformed through digital means (Ngo et al., 2020). This classification helps us understand the range and methods of online criminal behavior.

Additionally, the ways cybercrime operates are quite different from traditional crimes. Offenders can act across borders, using tools like VPNs and the Dark Web to stay anonymous and hidden (Broadhurst et al., 2013). This makes enforcement challenging, as these crimes often don't have a clear geographic origin or point of contact.

While the motivations behind traditional and cybercriminals may overlap, the dynamics of space and evidence are distinct. Traditional crimes are often limited by physical opportunity and presence, whereas cybercrime thrives in connected and accessible environments. This requires new investigative approaches like digital forensics and international cooperation (Wilsem, 2013; Dupont & Holt, 2021).

From a theoretical perspective, Routine Activity Theory has been widely adapted to explain cybercrime victimization. It suggests that the convergence of a motivated offender, a suitable target, and the absence of capable guardianship applies equally in virtual settings (Ahmad & Ramayah, 2022). This framework highlights how online behavior and digital exposure create conditions for crime (Guo et al., 2021).

Moreover, the psychological and emotional impacts of cybercrime can be just as severe as those of physical crimes. Victims often experience distress, loss of control, and damage to their reputation, especially in cases of cyberbullying or identity theft (Lavorgna, 2018; Notté et al., 2021).

In summary, cybercrime represents a reconfiguration of criminal opportunity and behavior, embedded within digital systems and global networks. Understanding its core definitions and features is essential for developing effective legal, theoretical, and enforcement frameworks.

The concept of a-spatiality

The concept of a-spatiality refers to the weakening or erasure of traditional spatial boundaries in digital interactions. Within the context of cybercrime, it describes the disconnection between the physical location of an offender and the space in which the criminal impact is felt. This conceptual shift challenges long-standing assumptions in criminology and geography, where spatial proximity is often viewed as a key determinant of criminal opportunity and enforcement capacity (Castells, 1996).

Digital space is structured not by physical distance, but by connectivity. As Castells (1996) argues in his seminal theory of the "space of flows," the rise of networked societies has produced a new spatial logic — one that prioritizes speed, exchange, and relational networks over territoriality. In this logic, cyberspace becomes a domain where offenders and victims can interact without ever entering the same physical environment.

This a-spatial condition has profound implications for law enforcement and governance. Traditional policing strategies rely on location-based jurisdiction, surveillance, and response. In contrast, cybercrime often spans multiple countries, legal systems, and time zones — complicating everything from evidence collection to prosecution (Real, 2023).

Technologically, the digital infrastructures that enable a-spatiality - such as cloud computing, anonymizing tools, and VPNs - allow offenders to mask their location and operate across sovereign borders. This challenges the applicability of state-bound legal frameworks and calls for new transnational or multilateral approaches (Mone et al., 2024).

From a theoretical standpoint, a-spatiality forces a reevaluation of how crime is embedded in space. Whereas urban criminology traditionally investigates neighborhoods, physical disorder, or proximity-based victimization, cybercrime bypasses such localized conditions.

Instead, the networked environment becomes the relevant "space" — characterized by fluidity, disconnection, and layered visibility (Vakhitova et al., 2015).

Finally, a-spatiality raises critical concerns for data governance and individual privacy. In the absence of clearly bounded spatial protections, personal data becomes globally exposed, increasing the risk of exploitation and loss of informational control. Policymakers must therefore address not only technical vulnerabilities but also the conceptual reorientation of what constitutes a "space of rights" in the digital domain (Meier et al., 2023; Mühlhoff, 2021).

In summary, the a-spatial nature of cybercrime disrupts traditional conceptions of crime geography, enforcement, and urban governance. It requires interdisciplinary engagement to redefine how societies prevent, regulate, and respond to threats in a space that is everywhere — and nowhere.

2. Urban infrastructure and cybercrime

Urban environments are crucial hubs in the digital world, housing physical infrastructures that not only facilitate connectivity but also introduce new vulnerabilities to cybercrime. These infrastructures include public Wi-Fi networks, data centers, telecommunications systems, and increasingly, Internet of Things (IoT) devices embedded in public and semi-public spaces (Sombatruang et al., 2016; Wang et al., 2016).

One of the most common points of cyber vulnerability in cities is public Wi-Fi. While offering convenience and access, these networks often lack strong security protocols, leaving users exposed to attacks such as man-in-the-middle intrusions or rogue access points (Sombatruang et al., 2018; Lambert et al., 2014). Many users underestimate the risks involved, despite growing awareness, and continue to perform sensitive activities over unsecured networks.

Different urban typologies indeed face unique digital risk landscapes shaped by their specific characteristics and infrastructures. Smart cities, characterized by extensive IoT integration and automated systems, encounter heightened vulnerabilities, particularly in areas like sensor networks and critical service sectors (Ahmad et al., 2024; Demertzi et al., 2023; Al-Taleb and Saqib, 2022). This integration increases the attack surface for potential cyber threats, as

malicious entities can exploit weaknesses through diverse digital platforms, which often lack adequate security measures (Neshenko et al. 2020; Wright et al. 2022).

Conversely, global cities, with their intricate corporate and governmental frameworks, are prime targets for sophisticated cyber threats, including data breaches and ransomware attacks, indicating a strategic vulnerability due to the high density of sensitive data (Mahboob et al. 2023; Jannat et al., 2020). Furthermore, the digital divide is profound in informal settlements, where the absence of cybersecurity infrastructure leaves residents exposed to pervasive threats like identity theft and fraud, primarily through unsecured connectivity options, such as public Wi-Fi (Kravchenko et al., 2024; Egete et al. 2023; Alhalafi and Veeraraghavan 2021). This distinction illustrates how spatial contexts significantly influence the frequency and nature of cyber threats experienced across different urban environments (Neshenko et al. 2020; Ahmad et al. 2024, 254-269; Egete et al. 2023).

Urban data centers also represent attractive targets for cybercriminals, especially those containing government or corporate data. The aggregation of sensitive information in centralized digital repositories can lead to large-scale breaches, often with cascading effects across sectors (McShane et al., 2014). Furthermore, poor segmentation, outdated systems, or insufficient encryption exacerbate these risks.

Expanding on the risks in smart cities mentioned above, the Internet of Things (IoT) introduces particularly complex challenges. Devices such as surveillance cameras, smart lighting systems, and connected transit infrastructure often lack strong security standards, making them attractive for cyber intrusions (MT et al., 2024; Setiadji et al., 2019). These vulnerabilities multiply in systems where functionality is prioritized over security.

The physicality of digital crime often manifests through these nodes. For instance, rogue Wi-Fi access points placed in cafés, libraries, or transit hubs can trick users into connecting, enabling attackers to capture personal data (Банах et al., 2023). Even the spatial concentration of digital infrastructure in certain urban zones can make specific neighborhoods or institutions more vulnerable to targeted attacks.

Real-world examples highlight these dynamics. During the 2016 U.S. Democratic National Convention, attackers exploited public network vulnerabilities to access sensitive communications, demonstrating how urban digital infrastructure can be leveraged for

political cyber operations (Setiadji et al., 2019). Similar tactics have been observed in large international sporting events and public health infrastructures.

Despite these threats, urban planning has traditionally emphasized physical safety and accessibility, often without incorporating cybersecurity as a design principle. As cities become increasingly digitized, integrating cyber resilience into urban development is essential. This requires collaboration between municipal authorities, cybersecurity professionals, and community stakeholders (Spacey et al., 2016).

In conclusion, urban infrastructure plays a dual role: it enables digital access while simultaneously opening up new vectors for exploitation. Cybercrime in the city is not merely a digital phenomenon; it is materially grounded in the physical architecture of connectivity. Protecting these environments requires anticipating risks at both the technological and spatial levels.

3. Socio-economic urban risk factors and victimization

Urban environments are not just filled with digital infrastructure; they also have significant socio-economic inequalities that shape how people access, understand, and are vulnerable to digital threats. Lower-income populations in cities often have limited access to secure technologies, lack awareness of cyber threats, and have inadequate digital skills, which increases their risk of becoming victims of cybercrime (Bernik et al., 2022; Ahmad et al., 2024).

These vulnerabilities are made worse by the “digital divide” — a gap that reflects differences in both access to digital tools and the ability to use them effectively. In cities, this divide often follows existing lines of income, education, age, and migration status, creating zones of digital exclusion within otherwise connected cities (Correa et al., 2023; Lutz, 2019).

For example, elderly people living in low-income neighborhoods may not know how to identify phishing schemes or avoid malware, making them prime targets for online scams and financial fraud (Bernik et al., 2022). Similarly, young people in underserved areas, even though they are often digitally engaged, may lack the protective behaviors or critical thinking skills needed to avoid cyberbullying or online exploitation (Awasthi et al., 2023).

The physical environment also plays a role. In some neighborhoods, public Wi-Fi might be the only accessible form of connectivity, leading residents to depend on insecure networks. In

others, informal housing or overcrowded conditions mean multiple people may share devices, compromising both privacy and data protection (Ganti et al., 2022; Dachaga & Vries, 2021).

Moreover, urban exclusion often results in poor access to services like health care, legal protection, and education, leaving marginalized residents with limited options for redress after victimization. For instance, people in informal settlements or migrant populations may be reluctant to report cybercrimes due to distrust of authorities, legal ambiguity, or lack of resources (Weijer et al., 2020).

Socio-economic stressors also impact digital behavior. People under financial pressure may be more likely to engage in risky online activities, such as using pirated software or clicking on fraudulent job offers — both of which expose them to malware, phishing, or ransomware attacks (Pollock et al., 2022).

Finally, while smart city technologies promise improved services, they often reinforce existing inequalities. Surveillance, automated decision systems, and predictive policing algorithms may disproportionately target or neglect marginalized communities if not carefully designed and regulated (Althibyani & Al-Zahrani, 2023). Without inclusive digital policies, the smart city can quickly become a divided city, deepening both physical and digital vulnerability.

In summary, socio-economic inequalities intersect with digital infrastructures in ways that increase cybercrime exposure for urban residents. Addressing these risks requires not only technological interventions but also broader social policies that promote digital equity, cybersecurity education, and accessible victim support systems.

4. Law enforcement and governance challenges

The a-spatial nature of cybercrime challenges traditional law enforcement models rooted in physical jurisdiction and proximity. Digital offenses often span multiple countries, legal systems, and platforms, complicating evidence collection, prosecution, and cooperation across borders (Fahmy, 2024; Ilchyshyn et al., 2023).

A central obstacle is the difficulty of attribution. Cybercriminals routinely exploit obfuscation tools - VPNs, proxy servers, encrypted platforms - to conceal identities and disperse activity across jurisdictions. Even when traced, investigations often stall due to fragmented international legal frameworks, bureaucratic delays in extradition and mutual assistance, or

incompatible laws (Zhang & Gong, 2023; Broadhurst & Chang, 2012). As a result, offenders frequently evade justice by exploiting gaps between national enforcement regimes.

Meanwhile, local police forces are often under-resourced and under-trained in handling digital crimes. Many units lack digital forensics expertise, cyber incident protocols, or the capacity to manage international coordination. This disparity is especially pronounced in smaller or non-metropolitan jurisdictions (Wilson et al., 2022). The resulting gap between citizen expectations and police response can lead to frustration, underreporting, and reduced trust in institutions (Chopin et al., 2024).

To address these challenges, policing must adapt through hybrid models that combine technical capability with local engagement. Investments in specialized training, public-private partnerships, and international cooperation - such as regional CERTs or cross-border task forces - are essential (Gill et al., 2014; Croasdell & Palustre, 2019). Cybercrime cannot be addressed solely through territorial logic; it requires interoperable, transnational, and community-oriented solutions that match the fluid nature of the digital threat landscape.

5. Urban resilience and policy measures

To tackle the risks posed by cybercrime in urban environments, cities need to develop integrated strategies that not only strengthen their digital infrastructure but also support public awareness, response, and recovery. Urban resilience in this context means being prepared technically, but also being adaptable institutionally, responsive legally, and engaged with the community.

A key step in improving resilience is adopting proactive cybersecurity policies at the municipal level. Cities can implement regulatory frameworks that require minimum security standards for public networks, critical infrastructure, and third-party vendors, especially in sectors like healthcare, finance, and transportation (Stadler, 2020). These policies should also prioritize data privacy and accountability to build public trust.

Public-private partnerships are essential for enhancing cyber resilience. By collaborating with technology companies, telecom providers, and cybersecurity experts, municipalities can access up-to-date threat intelligence, training resources, and response protocols. Programs like CERTs (Computer Emergency Response Teams) can be localized to urban regions and tailored to their specific risks (Wilson et al., 2022).

Investing in infrastructure security is equally important. Cities should upgrade their digital systems with adaptive firewalls, intrusion detection systems, and encrypted networks. Smart city technologies need to be evaluated for vulnerabilities before deployment, with security features built in from the start rather than added later (Dash et al., 2022).

On the social side, cybersecurity education and awareness campaigns play a crucial role in reducing victimization. Citizens equipped with basic digital hygiene knowledge — like recognizing phishing attempts, using secure passwords, and reporting suspicious activity — are less likely to fall prey to online threats (Drew, 2020). Educational outreach should be inclusive, multilingual, and tailored to diverse urban demographics, including elderly populations, migrants, and digitally marginalized groups (Althibyani & Al-Zahrani, 2023).

Examples of successful urban interventions include Estonia's national cyber strategy, which integrates public engagement through training, simulations, and open-source tools; Singapore's Smart Nation initiative, which combines secure-by-design architecture with citizen education; and Toronto's municipal cybersecurity framework, which includes neighborhood-based engagement and participatory risk mapping (Gabrian, 2023; Hartati & Muhammad, 2023; Wilson et al., 2022).

Effective resilience strategies must be contextually tailored to urban typologies. In smart cities, this entails implementing encrypted IoT systems and continuous threat monitoring to safeguard complex infrastructures (Therrien et al., 2019). In contrast, informal settlements benefit more from secure public access points, foundational cybersecurity education, and inclusive reporting mechanisms to build local capacity (Falco et al., 2018). These differentiated approaches reflect the need for adaptable frameworks that address the distinct challenges of varied urban configurations, as spatial factors shape resilience outcomes in diverse ways (Badea and Ranf, 2023).

Importantly, urban resilience must also be approached through a justice lens. Cybersecurity policies should avoid reinforcing existing inequalities or enabling surveillance regimes that disproportionately target marginalized groups. Instead, efforts must ensure that protection, education, and resources are distributed equitably across the urban population (Dupont & Holt, 2021).

In conclusion, building cyber resilience in urban settings requires more than just technical solutions. It demands cross-sectoral coordination, citizen inclusion, legal innovation, and

ongoing investment in secure infrastructure and education. Only through such integrated approaches can cities adapt to the a-spatial dynamics of cybercrime and protect their increasingly digital urban futures.

6. Conclusion

This article delves into the concept of a-spatiality as a key feature of cybercrime and its connection to urban environments. By moving beyond territorial boundaries, cybercrime challenges traditional criminological theories, law enforcement methods, and urban governance structures. The a-spatial nature of digital offenses — happening across jurisdictions without regard for geographic proximity — makes conventional frameworks for prevention, policing, and victim support insufficient.

Urban areas, with their dense digital infrastructure and socio-economic diversity, are particularly affected by these developments. Infrastructures like public Wi-Fi, IoT systems, and data centers create dense nodes of vulnerability, while existing inequalities increase risk exposure among marginalized populations. These dynamics highlight the need to view cybercrime not just as a technological issue but also as a spatial and social one, deeply embedded in the urban fabric.

Theoretically, this article bridges urban criminology with digital geography, emphasizing the importance of spatial theory in understanding crimes that seem to occur "nowhere." Practically, the findings underscore the urgency of adopting integrated policy frameworks that strengthen digital infrastructure, support public education, and facilitate international cooperation.

This analysis also underscores the importance of urban typologies in shaping the nature and severity of cyber threats. From IoT-intensive smart cities to globally networked financial hubs and digitally excluded informal settlements, each urban form presents distinct risks, vulnerabilities, and policy needs. Cybercrime is not experienced uniformly - it is filtered through the spatial, technical, and socio-economic configurations of each city.

Future research should explore the micro-geographies of urban digital risk, evaluate the effectiveness of local cybersecurity initiatives, and investigate how algorithmic governance or surveillance may perpetuate urban exclusions. Policymakers and urban stakeholders must

prioritize equity, resilience, and adaptability in responding to cyber threats — recognizing that urban security today includes protecting the invisible, digital layers of city life.

In an increasingly connected world, where the boundaries between physical and digital space continue to blur, building urban cyber resilience is no longer optional. It is an essential task for cities seeking to safeguard their citizens, institutions, and democratic processes.

Acknowledgments

This manuscript was prepared with the assistance of ChatGPT (OpenAI) and Microsoft Copilot, for purposes of language refinement, grammar correction, and formatting consistency. The author takes full responsibility for the content, interpretations, and conclusions presented herein.

References

Ahmad, I., Anyanwu, A., Onwusinkwue, S., Dawodu, S. O., Akagha, O. V., & Ejairu, E. (2024). Cybersecurity challenges in smart cities: A case review of African metropolises. *Computer Science & IT Research Journal*, 5(2), 254–269. https://doi.org/10.51594/csitrj.v5i2.756

Ahmad, R., & Ramayah, T. (2022). A systematic literature review of routine activity theory's applicability in cybercrimes. *Journal of Cyber Security and Mobility*. https://doi.org/10.13052/jcsm2245-1439.1133

Alhalafi, N., & Veeraraghavan, P. (2021). Cybersecurity policy framework in Saudi Arabia: Literature review. *Frontiers in Computer Science*, 3. https://doi.org/10.3389/fcomp.2021.736874

Al-Khater, W., Al-Máadeed, S., Ahmed, A., Sadiq, A., & Khan, M. (2020*)*. Comprehensive review of cybercrime detection techniques. *IEEE Access*, 8, 137293–137311. https://doi.org/10.1109/access.2020.3011259

Al-Taleb, N., & Saqib, N. A. (2022). Towards a hybrid machine learning model for intelligent cyber threat identification in smart city environments. *Applied Sciences*, 12(4), 1863. https://doi.org/10.3390/app12041863

Althibyani, H., & Al-Zahrani, A. (2023). Investigating the effect of students' knowledge, beliefs, and digital citizenship skills on the prevention of cybercrime. *Sustainability*, 15(15), 11512. https://doi.org/10.3390/su151511512

Awasthi, L., et al. (2023). Cyber crime prevention model using artificial intelligence. *JCHR*. https://doi.org/10.53555/jchr.v13.i4s.1660

Badea, D., & Ranf, D. E. (2023). Challenges of post-pandemic urban resilience management. *Studies in Business and Economics*, 18(1), 37–53. https://doi.org/10.2478/sbe-2023-0002

Bernik, I., Prislan, K., & Mihelič, A. (2022). Country life in the digital era: Comparison of technology use and cybercrime victimization between residents of rural and urban environments in Slovenia. *Sustainability*, 14(21), 14487. https://doi.org/10.3390/su142114487

Broadhurst, R., & Chang, L. (2012). Cybercrime in Asia: Trends and challenges. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2118322

Broadhurst, R., Grabosky, P., Alazab, M., Bouhours, B., & Chon, S. (2013). Organizations and cybercrime: An analysis of the nature of groups engaged in cybercrime. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2345525

Castells, M. (1996). The Rise of the Network Society. Oxford: Blackwell.

Chopin, U., Faubert, É., Décary-Hétu, U., Dupont, B., Ratcliffe, T., & Malm, C. (2024). Are cyber-investigators resilient in the face of adversity? An inductive qualitative analysis exploring investigators' perceptions regarding the challenges and successes in online crime police investigations. *CrimRxiv*. https://doi.org/10.21428/cb6ab371.9aae757e

Correa, J., Ulloa-León, F., Vergara-Perucich, F., Aguirre, C., & Truffello, R. (2023). Infrastructural inequality: Exploring the emergence of digital classes in the metropolitan area of Santiago, Chile. Bulletin of Geography. *Socio-Economic Series*, 62, 107–122. https://doi.org/10.12775/bgss-2023-0037

Croasdell, D., & Palustre, A. (2019). Transnational cooperation in cybersecurity. https://doi.org/10.24251/hicss.2019.674

Dachaga, W., & Vries, W. (2021). Land tenure security and health nexus: A conceptual framework for navigating the connections between land tenure security and health. *Land*, 10(3), 257. https://doi.org/10.3390/land10030257

Dash, B., Ansari, M., Sharma, P., & Ali, A. (2022). Threats and opportunities with AI-based cyber security intrusion detection: A review. *International Journal of Software Engineering & Applications*, 13(5), 13–21. https://doi.org/10.5121/ijsea.2022.13502

Demertzi, V., Demertzis, S., & Demertzis, K. (2023). An overview of cyber threats, attacks and countermeasures on the primary domains of smart cities. *Applied Sciences*, 13(2), 790. https://doi.org/10.3390/app13020790

Drew, J. (2020). A study of cybercrime victimisation and prevention: Exploring the use of online crime prevention behaviours and strategies. *Journal of Criminological Research Policy and Practice*, 6(1), 17–33. https://doi.org/10.1108/jcrpp-12-2019-0070

Dupont, B., & Holt, T. (2021). The human factor of cybercrime. *Social Science Computer Review*, 40(4), 860–864. https://doi.org/10.1177/08944393211011584

Egete, D. O., Ele, B., & Eko, C. E. (2023). Synopsis of cybersecurity and risks associated with cybercrime to susceptible and blameless global citizenries. *European Journal of Theoretical and Applied Sciences*, 1(5), 475–487. https://doi.org/10.59324/ejtas.2023.1(5).37

Fahmy, W. (2024). The Cybercrime Acts and the Electronic Transaction in International Law. *Economics Law and Policy*, 7(1), 18. https://doi.org/10.22158/elp.v7n1p18

De Falco, S., Angelidou, M., & Addie, J.-P. D. (2018). From the "smart city" to the "smart metropolis"? Building resilience in the urban periphery. *European Urban and Regional Studies*, 26(2), 205–223. https://doi.org/10.1177/0969776418783813

Gabrian, C. (2023). How the Russia-Ukraine war may change the cybercrime ecosystem. *Bulletin of Carol I National Defence University*, 11(4), 43–49. https://doi.org/10.53477/2284-9378-22-92

Ganti, M., Yusuf, H., Wismayanti, Y., Setiawan, H., Susantyo, B., Konita, I., … Sulubere, M. (2022). The issues and socio-economic potentials of urban marginal groups in Indonesia. In *Proceedings of the International Conference on Social Sciences*, 246–259. https://doi.org/10.2991/978-2-494069-65-7_23

Gill, C., Weisburd, D., Telep, C. W., Vitter, Z., & Bennett, T. (2014). Community-oriented policing to reduce crime, disorder and fear and increase satisfaction and legitimacy among citizens: A systematic review. *Journal of Experimental Criminology*, 10(4), 399–428. https://doi.org/10.1007/s11292-014-9210-y

Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. *Journal in Computer Virology*, 2(1), 13–20. https://doi.org/10.1007/s11416-006-0015-z

Guo, Z., et al. (2021). Online social deception and its countermeasures: A survey. *IEEE Access*, 9, 1770–1806. https://doi.org/10.1109/access.2020.3047337

Hartati, C., & Muhammad, A. (2023). Combating cybercrime and cyberterrorism in Indonesia. *Jurnal Hubungan Internasional*, 11(2), 45–56. https://doi.org/10.18196/jhi.v11i2.15647

Ilchyshyn, N., et al. (2023). International legal cooperation in the field of criminal justice: New challenges and ways to overcome them. *Journal of Law and Sustainable Development*, 11(4), e767. https://doi.org/10.55908/sdgs.v11i4.767

Jannat, A., Ilyas, A., Saeed, T., Iftikhar, A., Zahra, A., & Jafri, A. R. (2020). Exploration of solutions for smart cities: Challenges in privacy and security. In *2020 IEEE 23rd International Multitopic Conference (INMIC)*, 1–5. https://doi.org/10.1109/inmic50486.2020.9318070

Kravchenko, O., Veklych, V., Krykhivskyi, M., & Madryha, T. (2024). Cybersecurity in the face of information warfare and cyberattacks. *Multidisciplinary Science Journal*, 6, 2024ss0219. https://doi.org/10.31893/multiscience.2024ss0219

Lambert, A., McQuire, S., & Papastergiadis, N. (2014). Free public Wi-Fi and e-planning. *International Journal of E-Planning Research*, 3(2), 70–85. https://doi.org/10.4018/ijepr.2014040105

Lavorgna, A. (2018). Cyber-organised crime: A case of moral panic? *Trends in Organized Crime*, 22(4), 357–374. https://doi.org/10.1007/s12117-018-9342-y

Lutz, C. (2019). Digital inequalities in the age of artificial intelligence and big data. *Human Behavior and Emerging Technologies*, 1(2), 141–148. https://doi.org/10.1002/hbe2.140

Mahboob, S. M., Abbas, S. S., & Shaheen, I. A. (2023). Adapting to cybersecurity challenges: Assessing the effectiveness of international law against cyber terrorism. *Journal of Social Research Development*, 4(4), 669–685. https://doi.org/10.53664/jsrd/04-04-2023-02-669-685

McShane, I., Meredyth, D., & Wilson, C. (2014). Broadband as civic infrastructure – the Australian case. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2401477

Meier, Y., & Krämer, N. C. (2023). A longitudinal examination of internet users' privacy protection behaviors in relation to their perceived collective value of privacy and individual privacy concerns. *New Media & Society*, 26(10), 5942–5961. https://doi.org/10.1177/14614448221142799

Mone, V., Abdulajonovich, S. M., Younas, A., & Petikam, S. (2024). Data warfare and creating a global legal and regulatory landscape: Challenges and solutions. *International Journal of Legal Information*, 52(2), 124–134. https://doi.org/10.1017/jli.2024.22

MT, S., Aminanto, A., & Aminanto, M. (2024). Empowering digital resilience: Machine learning-based policing models for cyber-attack detection in Wi-Fi networks. *Electronics*, 13(13), 2583. https://doi.org/10.3390/electronics13132583

Mühlhoff, R. (2021). Predictive privacy: Towards an applied ethics of data analytics. *Ethics and Information Technology*, 23(4), 675–690. https://doi.org/10.1007/s10676-021-09606-x

Neshenko, N., Nader, C., Bou-Harb, E., & Furht, B. (2020). A survey of methods supporting cyber situational awareness in the context of smart cities. *Journal of Big Data*, 7(1). https://doi.org/10.1186/s40537-020-00363-0

Ngo, F., et al. (2020). Victimization in cyberspace: Is it how long we spend online, what we do online, or what we post online? *Criminal Justice Review*, 45(4), 430–451. https://doi.org/10.1177/0734016820934175

Notté, R., Leukfeldt, R., & Malsch, M. (2021). Double, triple or quadruple hits? Exploring the impact of cybercrime on victims in the Netherlands. *International Review of Victimology*, 27(3), 272–294. https://doi.org/10.1177/02697580211010692

Pollock, T., Levy, Y., Li, W., & Kumar, A. (2022). Pilot testing of experimental procedures to measure user's judgment errors in simulated social engineering attacks. *Online Journal of*

Applied Knowledge Management, 10(2), 23–40. https://doi.org/10.36965/ojakm.2022.10(2)23-40

Real, C. T. (2023). El peso de la historia: Desafíos de la policía en la gobernanza del cibercrimen en España. *Revista de Estudios en Seguridad Internacional*, 9(2), 77–99. https://doi.org/10.18847/1.18.5

Setiadji, M., Ibrahim, R., & Amiruddin, A. (2019). Lightweight method for detecting fake authentication attack on Wi-Fi. *Proceedings of the Electrical Engineering Computer Science and Informatics*, 6(1). https://doi.org/10.11591/eecsi.v6.2003

Sombatruang, N., Kadobayashi, Y., Sasse, M. A., Baddeley, M., & Miyamoto, D. (2018). The continued risks of unsecured public Wi-Fi and why users keep using it: Evidence from Japan. In *IEEE 16th Annual Conference on Privacy, Security and Trust (PST)* (pp. 1–11). https://doi.org/10.1109/pst.2018.8514208

Sombatruang, N., Sasse, M. A., & Baddeley, M. (2016). Why do people use unsecure public Wi-Fi? An investigation of behaviour and factors driving decisions. In *Proceedings of the 6th Workshop on Socio-Technical Aspects in Security and Trust* (pp. 61–72). https://doi.org/10.1145/3046055.3046058

Spacey, R., Muir, A., Cooke, L., Creaser, C., & Spezi, V. (2016). Filtering wireless (Wi-Fi) Internet access in public places. *Journal of Librarianship and Information Science*, 49(1), 15–25. https://doi.org/10.1177/0961000615590693

Stadler, L. (2020). Risks of privacy-enhancing technologies: Complexity and implications of differential privacy in the context of cybercrime. *International Journal of Law and Information Technology*, 28(3), 211–230. https://doi.org/10.5772/intechopen.92752

Therrien, M.-C., Usher, S., & Matyas, D. (2019). Enabling strategies and impeding factors to urban resilience implementation: A scoping review. *Journal of Contingencies and Crisis Management*, 28(1), 83–102. https://doi.org/10.1111/1468-5973.12283

Vakhitova, Z., Reynald, D. M., & Townsley, M. (2015). Toward the adaptation of routine activity and lifestyle exposure theories to account for cyber abuse victimization. *Journal of Contemporary Criminal Justice*, 32(2), 169–188. https://doi.org/10.1177/1043986215621379

van de Weijer, S., Leukfeldt, R., & van der Zee, S. (2020). Reporting cybercrime victimization: Determinants, motives, and previous experiences. *Policing: An International Journal*, 43(1), 17–34. https://doi.org/10.1108/pijpsm-07-2019-0122

Whitehead, J., et al. (2019). How can the spatial equity of health services be defined and measured? A systematic review of spatial equity definitions and methods. *Journal of Health Services Research & Policy*, 24(4), 270–278. https://doi.org/10.1177/1355819619837292

Wilsem, J. (2013). Hacking and harassment – Do they have something in common? Comparing risk factors for online victimization. *Journal of Contemporary Criminal Justice*, 29(4), 437–453. https://doi.org/10.1177/1043986213507402

Wilson, M., Cross, C., Holt, T., & Powell, A. (2022). Police preparedness to respond to cybercrime in Australia: An analysis of individual and organizational capabilities. *Journal of Criminology*, 55(4), 468–494. https://doi.org/10.1177/26338076221123080

Wright, M., Chizari, H., & Viana, T. (2022). A systematic review of smart city infrastructure threat modelling methodologies: A Bayesian focused review. *Sustainability*, 14(16), 10368. https://doi.org/10.3390/su141610368

Yang, W., Chookhampaeng, C., & Chano, J. (2023). Spatial visualization ability assessment for analyzing differences and exploring influencing factors: Literature review with bibliometrics and experiment. *Indonesian Journal of Science and Technology*, 9(1), 191–224. https://doi.org/10.17509/ijost.v9i1.66774

Zhang, H., & Gong, X. (2023). The research on an electronic evidence forensic system for cross-border cybercrime. *The International Journal of Evidence & Proof*, 28(1), 21–44. https://doi.org/10.1177/13657127231187059

Банах, Р., Piskozub, А., & Opirskyy, І. (2023). Devising a method for detecting “evil twin” attacks on IEEE 802.11 networks (Wi-Fi) with KNN classification model. *Eastern-European Journal of Enterprise Technologies*, 3(9(123)), 20–32. https://doi.org/10.15587/1729-4061.2023.282131