Municipal Cybersecurity—A Neglected Research Area? A Survey of Current Research

Arnstein Vestad and Bian Yang

Abstract Municipalities are tasked with ensuring the cybersecurity of critical public services and functions in diverse areas such as safe water supply, healthcare, child protective services, and education with vastly different security requirements—all usually served from a common infrastructure with limited technical and organizational cybersecurity capabilities. This literature review identifies recent research on municipal and local government cybersecurity to identify current research areas, state of the art, and research methods used in research so far. We found research in the areas of smart cities, elections, human factors, operational technology, and crisis management. We also give suggestions for further research to develop better models for cybersecurity in cross-disciplinary organizations.

Keywords Cybersecurity · Municipalities · Governance · Literature review

1 Introduction

Municipalities have complex, interwoven ICT infrastructures created to support an equally diverse range of public services. But this complexity is in some way unavoidable; given the diverse set of requirements, municipal cybersecurity must address areas such as the running of schools, child protective services, critical water supply services, and health and social services. From a security point of view, complexity is an enemy, creating dark areas where attackers may infiltrate and establish footholds, posing great risks to the municipality's ability to serve its public.

Incidents like the cyberattack of the Norwegian municipality of Østre Toten [1] illustrate dramatically the great responsibility for protecting highly sensitive information and critical services placed on organizations that may be woefully

A. Vestad (✉) · B. Yang
NTNU, Norwegian University of Science and Technology, Trondheim, Norway
e-mail: arnstein.vestad@ntnu.no

B. Yang
e-mail: bian.yang@ntnu.no

C. Onwubiko et al. (eds.), *Proceedings of the International Conference on Cybersecurity, Situational Awareness and Social Media*, Springer Proceedings in Complexity,
https://doi.org/10.1007/978-981-19-6414-5_9

inadequately furnished to take on this responsibility. Cyberattacks on municipal infrastructures create risks of debilitating operational technology systems in water and sewage services, patient alerting systems in nursing homes, case management systems serving vulnerable populations in child protective services or electronic patient journal systems in primary health care.

New and increasingly stringent legal requirements and regulations, like the EU privacy regulation GDPR, the EU NIS Directive (The directive on security of network and information systems—the first EU-wide cybersecurity regulation), and other sector-specific regulations are also affecting the municipalities—are increasing the burden of regulatory compliance and giving rise to legal risk and large economic penalties for incompliance. At the same time, municipalities face increased needs for public services, such as increased spending on healthcare for the elderly.

Many established cybersecurity knowledge domains are already relevant for municipal activities. A municipal perspective would seem to add little to areas such as malware analysis, firewall configurations, intrusion detection, etc. Nevertheless, the consequences of breaches in security, and evidence from incidents, show both the challenge of establishing a necessary level of cybersecurity controls, the risks of highly interconnected infrastructures in multidisciplinary organizations, as well as the need for suitable methods of analyzing, communicating and understanding risk, and choosing and implementing cost-effective security strategies. This issue will be further developed in the discussion section.

A similar question might be raised when it comes to addressing the municipality as a whole, rather than specific areas of responsibility, for example, health care, water supplies, education, etc., with their differing concerns. The educational domain often has a focus on the rapid adoption of new tools, software, etc., to ensure a good pedagogical environment with less emphasis on confidentiality except for certain types of information (in particular student-related health, social, and child protective services-related information communicated with other relevant authorities). Water supplies have operational technology solutions, often challenged by geographical dispersion and hardware/software solutions that are hard to secure/update, where reliability is a high concern, while confidentiality is less so. The municipal health care sector not only processes large amounts of sensitive personal information from health care journals making confidentiality of prime importance, but is also investing heavily in remote health solutions where reliability will be important to ensure secure patient care. Nevertheless, in municipalities, these systems are usually tightly connected through shared infrastructure and reliance on the shared IT staff supporting the infrastructure and applications. These unique conditions lead to equally unique cybersecurity challenges—and this paper argues for the need for a better understanding of this complexity and how it might best be managed.

A related work [2] performed a review of research and the contributions of professional associations and industry to the cybersecurity of local government organizations—they also focus on cross linkages that go outside or above the municipal level into urban infrastructures in general. The study is from an American perspective—and while most/all countries have a form of local government, the responsibilities and supporting governance structures such as sectorial directorates and authorities

vary from country to country. They conclude that there is a need for more research on what works and why, and suggest action research as a methodology for this. They also recommend more comparative studies between municipalities, as well as more government-industry-university partnerships to support cybersecurity innovation for the sector.

1.1 Research Motivation

In similarity with this study, [2] highlights the high level of interconnectedness and overlapping and open-ended systems as a source of risk for municipal infrastructures. The consequences of cybersecurity failures in municipal infrastructures, as evidenced in Norway by the ransomware attack on Østre Toten, show that the societal consequences of a worst-case scenario are real and dramatic. The need to understand both what has been researched and identify new venues of research has led to the following research questions this study aim to answer:

- Q1: What is the state of the art in municipal and local government cybersecurity research?
- Q2: What are the research areas or concerns that current research investigates?
- Q3: What are the research methods used in research on municipal cybersecurity?
- Q4: When considering municipal cybersecurity, what areas require more research?

The rest of this paper will, in Sect. 2, describe the methodology of this literature study, Sect. 3 will give a presentation of the identified studies, while Sect. 4 will give a discussion and propose further research areas.

2 Methodology

This study is guided by the principles and steps for performing a literature review as presented in [3] as well as the guidelines for conducting a systematic mapping survey in [4]. In comparison with a systematic literature review focused on gathering and synthesizing evidence, a systematic mapping study is used to structure a research area. The two approaches are similar when it comes to searching and study selection, but have different goals, and the research questions of a mapping study are more general, as they focus on discovering research trends and research gaps as well as mapping and categorizing research contributions. The steps followed, following the methodology described in [4], consist of the identification of the need for a mapping survey and the appropriate research questions, developing the search, evaluating the search, and inclusion and exclusion criteria and quality criteria, performing the data extraction and classification and conducting and reporting the mapping.

2.1 Selection of Studies

The databases used in this study were ScienceDirect, IEEE digital library, ACM digital library, Springer database, Web of Science, and AIS electronic library. The libraries were chosen to give a broad but technically focused source of material.

The following search term was used: ("municipal" OR "municipality") AND "cybersecurity".

2.2 Inclusion and Exclusion Criteria

We wanted this study to focus on papers that emphasize the municipality itself. Papers focusing primarily on state/national levels are, therefore, excluded, unless the municipal focus is significant. The papers should also have the municipalities as a central actor or theme. We also exclude papers that do not treat cybersecurity as the main topic or concern of the paper (for example, papers mainly about big data, where cybersecurity is one of many concerns). To focus on recent research, the study was limited to 2018–2021, with peer-reviewed papers from academic journals and conference proceedings as quality criteria. The following inclusion and exclusion criteria were used (Table 1).

2.3 Search Results and Reduction Process

The keyword search resulted in Table 2.

244 papers, including 1 retracted paper, were removed after title screening of the original search result that consisted of 627 papers. After title screening, 383 papers were left for record (including abstract) screening. Abstract screening left 34 papers for full-text screening. The relatively significant reduction illustrates that the search terms are quite generic and frequently used in papers on other topics.

In the full-text screening step, the full-text papers were read and further considered for inclusion or exclusion based on the criteria. Through this step, another 13 papers

Table 1 Inclusion and exclusion criteria

Inclusion criteria	Exclusion criteria
Focused on local/municipal government as an important subject AND focused on cybersecurity as the main concern	State/national level as the subject of interest
Published paper from peer-reviewed journal or conference	Cybersecurity as a peripheral concern
From the year 2018 to 2021	Municipal subject merely a background theme

Table 2 Search results

Database	Number of results
Sciencedirect	276
IEEE digital library	28
Web of science	43
ACM Digital library	38
AIS Digital library	28
SpringerLink	214
Total	**627 papers for deduplication and title review**

were considered out of scope, leaving a final count of 21 papers. In addition to these 21 papers, constructive input from peer review pointed out other terms used for similar local government organizations instead of "municipalities"—we performed an additional search of the databases and identified 6 papers to a total of 27.

3 Literature Review

Of the 27 papers in the final review, we identified several topics by a keywording strategy [5] based on identifying keywords from the abstracts of the chosen papers. By far largest was "smart city" with 10 papers, followed by management and governance with 5, human factors with 4, and elections with 4. In the following review, the findings are divided according to these categories.

3.1 Smart Cities

The most frequently explored theme by far is smart cities. Smart city is a nebulous term, used on diverse themes concerning social, environmental, and economic development in an urban setting, often designed around information technology and Internet of things-enabled sensor technologies, supporting mobility, efficient city management, interconnected health services, etc. [6]. Since smart cities are by nature also a municipality, this link is a natural one. Pelton and Singh [7] gives a general overview of security issues that smart city planners should consider, especially those connected to network security and vulnerabilities.

In [6], the authors present a literature review of security, privacy, and risk of smart cities, identifying several clusters of research themes, such as privacy and security of mobile devices and services, smart city infrastructure, smart power systems, smart healthcare, frameworks, algorithms and protocols, operational threats, use and adoption by citizens as well as the use of blockchain. From this, they also develop a "smart city interaction framework" where security, privacy, and risk are discussed

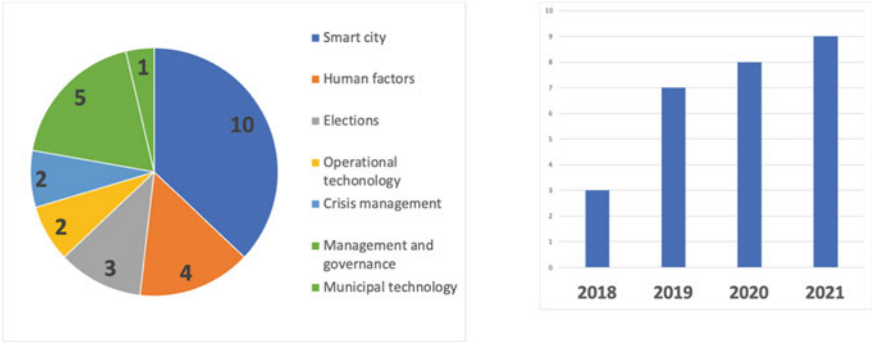

Fig. 1 Distribution by year and by thematic content

in a more holistic manner as it relates to key challenges for smart cities such as trust, operational and transitional issues, and technological and sustainability issues (Fig. 1).

Also, from a more policy-oriented perspective, [8] investigates the underdeveloped focus on management and policy when it comes to securing smart cities and the need for a dual focus on both the technological and the policy level. The paper also provides a review of privacy and security vulnerabilities imparted by the generic architecture of the smart city, such as physical level vulnerabilities connected to device level protection and mobile crowd sensing, communication level vulnerabilities, data processing, and storage level vulnerabilities. This is followed by an overview of domain-specific security challenges such as smart health, smart transportation, smart grid, smart home, and public safety and emergency management. They discuss the privacy and security of smart cities from the perspective of policymaking and regulation and technical aspects, pointing out the need for a holistic approach incorporating legal and organizational issues and technology.

Smart cities are made up of a multitude of organizations, stakeholders, technological standards, protocols, and solutions as well as vendors that produce them. Third-party risk management and well-defined security requirements, as well as who is responsible for meeting the requirements, are necessary. Vitunskaite et al. [9] reviewed 93 different standards relevant to the smart city, of which 13 consider security, and performed a comparative case study of three large smart city projects to investigate their governance models, security measures, technical standards, and third-party management. They suggest that government should mandate standards and minimum security requirements and requirements for third party and supply chain management.

The inherent complexity and high level of integration on technical, organizational, and societal level of smart cities, and their inherent risk suggest the need for a holistic risk management process. Ullah et al. [10] reviewed 796 papers to propose a multilayered technology-organization-environment (TOE-based) risk management framework for sustainable smart city governance. They identify 56 key risks grouped

into three categories: technological, organizational, and external environment, to help both researchers and practitioners focus on the top risks of smart city governance.

Cybersecurity needs to be "built-in" and not "bolted on" as an afterthought. The authors of [11] conducted a case study of four smart city projects to identify a common set of principles for security and privacy to serve as best practices and guidelines that communities could use. The guidelines identified the areas of specific technology usage, implementation of a cybersecurity management process and framework, and cybersecurity expertise and public–private partnerships.

In [12], the authors identify cyber situational awareness as a critical issue in securing smart cities. They investigate through a literature survey the availability and sufficiency of data-driven techniques to support cyber situational awareness in the context of smart cities. The techniques are classified as "system abstraction", "risk and vulnerability assessment", and "attack detection methods", looking into the theoretical background (such as graph theory, neural networks, simulations, etc.), data input, accuracy, and scope of the techniques as well as their support for visual representation.

Smart cities are arguably distributed, and the use of blockchain as a distributed mechanism to address security requirements for smart cities was addressed by several authors including [6, 8], and [10]. Paul et al. [13] proposes a smart access control framework in a public and a private blockchain for smart city applications, taking into account the need for low resource consumption for IoT devices in the smart city. The authors of [14] conducted a bibliometric review of literature on blockchain in the context of smart cities, identifying key research and influential studies. They identified research in key areas such as the use of IoT for security in sensor data collection, privacy for machine learning, smart contracts for transparent and reliable data sharing, and blockchain use for empowering smart communities and fostering sustainability in smart cities.

Privacy is also an essential issue in smart city development and is also heavily regulated. The EU General Data Protection Regulation (GDPR) imposes strict rules that affect how smart city technology can be utilized when it processes personal data and high fines for lack of compliance. One of the primary measures the GDPR imposes is the need to perform Data protection impact assessments (DPIA) when processing entails high risks to individuals' rights and freedoms. Developing the DPIA can be a complex and costly undertaking, [15] suggests a smart city topology that aids in clustering services based on data protection to make the DPIA process more efficient.

3.2 Operational Technology

Operational technology (OT) is heavily utilized in the municipalities' responsibility for water supply and wastewater treatments. Lindstrom et al. [16] points out that the cybersecurity of OT systems is an important issue, OT systems are often required to be dependable and have high up-time, is often rarely patched and have other typical

security vulnerabilities. While many organizations have an IT security policy, few have an OT policy, and the researchers, through an in-depth qualitative study and action research develop an OT policy for a Swedish municipality.

Gouglidis et al. [17] also discussed OT technologies and provides a game theoretical approach to the problem of choosing an optimal defense strategy based on a threat model for a water utility system. The framework was demonstrated using data from an industrial control system (ICS) test-bed in.

3.3 Elections

Municipalities are a part of the democratic structure of the nation and are managed through political and democratic processes, of which elections are a key issue. While the cybersecurity requirements and other aspects of election integrity are not governed directly by the municipalities, municipalities are often responsible for the implementation/running of the elections.

Three papers addressed the theme of election cybersecurity. The authors of [18] describe the potential value of electronic voting, and the cybersecurity responsibilities, including preparedness plans for incidents that municipalities would need to have, mainly from a legal perspective. Also, from a legal perspective, the authors of [19] present findings from a review of online voting in Ontario, showing issues with weak voter authentication, poor transparency of election results, and a general lack of disaster-preparedness. The authors of [20] describe the development of cybersecurity awareness training specific to election integrity for poll workers in the municipality, and how specific and relevant training increases the effectiveness of cybersecurity awareness.

3.4 Human Issues and Cybersecurity Awareness

Accounting for the human element in cybersecurity is critical, and no less so for municipalities. While [20] discussed cybersecurity awareness in connection with elections, [21] looked into how the Swedish public sector, including municipalities, responded to the changing threat landscape connected with the Covid-19 pandemic, and used communication to enhancing employee cyber security awareness. Among the findings were data showing that 74% of municipalities have outsourced or have less than one dedicated staff for cybersecurity, and 74% of municipalities report as not yet having implemented cybersecurity work.

The skills shortage in cybersecurity has been a frequent theme in news media, the author of [22] of describes the application of competency-based education (CBE) and the use of the NIST NICE (National initiative for cybersecurity education) framework in a project to enhance cybersecurity capabilities in a metropolitan region in the U.S. By using a formal training framework, the local government will be able to

assess and direct training activities and to assess what competencies are most needed. CBE allows this training to be outcomes based and organized around the relevant knowledge, skills, abilities, and tasks defined by the NICE framework. The research also describes creating clear learning pathways and using digital badging and e-portfolios to give motivation, clarity, and a good fit between cybersecurity needs of the organization and training outcomes.

Also, connected to human issues, [23] investigated the relationship between municipalities affected by a ransomware attack and the effect of the security behaviors of the population in or near the municipality, suggesting an effect of cybersecurity incidents extending outside the municipality. People who live close to an attacked community are more likely to take preventive actions to reduce their susceptibility to ransomware.

3.5 Crisis Management

Despite all protective measures, cybersecurity incidents occur, and preparedness is key to managing the following crisis. The authors in [24] aimed to support the development of educational simulations and related experiential learning exercises that help prepare city and public infrastructure personnel to effectively respond to cybersecurity attacks. They conducted 8 expert interviews including 12 cybersecurity experts from federal, state, and city organizations, as well as academics with relevant expertise. They organized their findings into crucial learning outcomes, scenarios, roles, and issues that simulation designers should consider.

The authors in [25] analyzed municipalities responsibilities when handling crisis in general and cyber-incidents in particular. A crisis management model and a tentative design to be tested when executing cyber training and exercises in a training environment, such as the Norwegian Cyber Range is suggested.

3.6 Management and Governance

Managerial aspects, such as governance, investments and sourcing have also been studied. The authors of [26] conducted a nationwide survey of the cybersecurity practices of local governments in the United States. They found inadequate investments, low use of tools, recommended practices and appropriate policies, low awareness of standards, and limited ability to address cyber events. The paper calls not only for more management awareness and investments, but also for researchers to investigate cybersecurity at the grassroots level. The call for investments is also supported by [27] that utilized data from a cyber incident database with 865 incidents by U.S. local governments and departments between 2006 and 2017 finding a significant reduction in incidents correlated with IT investments in cybersecurity, and found that this effect was increasing over time (making investments more effective).

The authors of [28] investigated the decisions of local governments to outsource cybersecurity services and how cybersecurity outsourcing differs from other IT outsourcing activities because of complexity and information asymmetry—they found a clear trend toward outsourcing despite arguments against this. One specific type of outsourcing is cloud services—the authors of [29] describe a case study of Australian local government authorities and the factors used to assess cloud requirements proposing a conceptual cloud computing security requirements model with four components—data security, risk assessment, legal and compliance requirements, and business and technical requirements.

The authors of [30] used the NIST CSF to target three levels, executive, management, and technical to ascertain an organization-wide understanding of cybersecurity risks. The paper also describes other related cybersecurity standards. The research describes a process to evaluate cybersecurity maturity in local government organizations and presents measurable metrics and improvement steps.

3.7 Municipal Technology

The authors of [31] investigated the use of the security protocol HTTPS by Portuguese municipalities by performing scanning of the municipalities' web pages and grading their use of certificates and protocols. The study was a follow-up of a previous study to identify drivers or correlations for municipal cybersecurity performance, where a weak correlation between population and tax level was found. No similar correlation could be found in the follow-up, suggesting other factors such as awareness to have a higher effect.

3.8 Research Methods

A variety of research methods were used in the identified studies as listed in Table 3:

Qualitative methods such as descriptive case studies, interviews, and document studies seem to be the most common approach. While there is a need for quantitative

Table 3 Research methods

Research method	Counts	References
Technical information gathering	1	[31]
Literature studies	7	[2, 6, 8–10, 12, 14]
Case studies	9	[9, 11, 15, 17, 19, 20, 22, 29, 30]
Quantitative studies (surveys)	4	[21, 23, 26, 27]
Other qualitative methods (expert interviews, document studies, action research)	6	[11, 15, 16, p., 18, 24, 28]

data to compare and contrast what works and what does not, many of the specific issues of municipal cybersecurity, such as organization, culture, capabilities, and policies, is likely more suited to qualitative methods.

4 Discussion

Leavitt [23] in his study of organizational change developed the model later known as Leavitt's diamond. The model is frequently used in socio-technical analysis, as it incorporates both social (structures, people, tasks) as well as technical elements, and how they interact. Since municipal cybersecurity is, to a great extent, an organizational issue, concerned with an organization tasked with ensuring the security of their operation, the diamond model serves as an interesting analysis framework to understand how the papers contribute to the different parts of the model:

- **Structure**: Papers with a focus on organizational structure, communication, policies, responsibilities, also risks on organizational level, standards (non-technical)
- **Tasks**: Papers focusing on (security-related) tasks, activities that the organization is performing to fulfill (or support) their mission.
- **People**: Papers with a focus on the human aspects of cybersecurity, awareness, culture, as well as attitudes, and skills
- **Technology**: computer systems, software, devices, but in addition methods, frameworks, etc., used as tools to support cybersecurity work in the organization

4.1 Thematic Contributions

Of the 27 papers, 20 papers were considered to contribute primarily to structure (in relation to the areas of structure, task, people, and technology). They present a high-level overview of risks in their area (smart cities, elections, etc.), discussed policy issues, presented regulations, and management frameworks, gave a legal perspective or organizational topics such as roles and responsibilities and outsourcing strategies.

Four papers were more focused on the human aspect, such as awareness training and communication about cybersecurity to municipal employees and the effect of awareness among citizens after municipal cybersecurity incidents. Eight papers contributed to the technology aspect, as defined above—of these four could be considered technology in a narrower sense, such as analysis of technical issues, technical methods for security analysis, game theoretic approaches as well as strategies for the use of blockchain. Four other papers contributed under a more open definition of technology, with a management framework or a more analytical framework for cybersecurity and frameworks for risk analysis and data protection analysis.

4.2 Identified Gaps and Need for Research

While the identified literature is highly relevant to municipal cybersecurity and approaches the issue from differing perspectives, several areas have received less attention. A major focus has been placed on "smart cities" and related privacy and security challenges—while several authors point to the risks of interconnecting legacy technologies not built for a new threat landscape. This illustrates a focus on the "new and shiny" while both incidents and surveys demonstrate that many municipalities are not yet able to cope with today's challenges.

Cybersecurity in the municipal sector is of vital importance to the delivery of critical services in a democratic society and research need to address the fundamental nature of the municipal organization with its high interconnectedness of infrastructure, governance, and personnel performing tasks in areas with widely differing security requirements, cultures, and maturity.

Lack of focus on cross-organizational interactions

In the reviewed literature, limited attention is given to the structural issue that most significantly describes municipalities—the wide span in tasks, and how this affects cybersecurity. On the organizational level, we need a better understanding of how organizations with a wide span of tasks, with associated variety in technical solutions, cybersecurity threat landscapes, and applicable cybersecurity solutions (both technical, human and organizational), need to organize their security management and operational capabilities. The municipalities' need to provide services, from schools to health and water supplies, with hugely different cybersecurity requirements, as economically efficient as possible, is a complex socio-technical issue. And if they are not able to ensure the security of existing services, building smart cities on top of a weak foundation might not turn out to be very smart.

Lack of focus on tasks and capabilities

None of the papers contribute significantly to the tasks component of Leavitt's diamond discussing activities and tasks relevant to cybersecurity such as vulnerability management, access control management, security monitoring and security event analysis, especially in cross-functional organizations. Research could be improved by addressing these task in a socio-technical perspective as a set of cybersecurity *capabilities* including both human and technological aspects in a municipal enterprise cybersecurity architecture. There is a need for a better understanding of how to manage the broad scope of systems and responsibilities in a municipality that poses an extra challenge both in relation to technical integration and cross-functional cooperation (for example, between IT-departments and OT-departments).

The high complexity of cybersecurity in municipal organizations also raises the need for better tools to understand and manage this complexity, including tools that enable a better understanding of cross-organizational risks and risks connected to the high interdependence of municipalities on complex supply chains and ecosystems.

Simulation technology can be a possible avenue of research in this area by allowing the study of cybersecurity as emergent phenomenon in a complex environment.

5 Conclusion

This mapping study was conducted to provide an overview of the state of research on municipal cybersecurity. The municipalities are tasked with managing cybersecurity in complex interconnected infrastructures both within their own sphere of control, but also in connection with others, such as governmental IT-services, third-party vendors of cloud services, and, in providing remote health services, even into private homes. The survey showed that while cybersecurity issues relevant to municipalities are discussed, most significantly in the context of the emerging area of smart cities, important areas such as management of cybersecurity in cross-functional organizations, and research that takes into account needed cybersecurity capabilities and the complexity and risk of such systems in cross-functional organizations is still lacking.

Acknowledgements This work has received funding from the Research Council of Norway through the SFI Norwegian Centre for Cybersecurity in Critical Sectors (NORCICS) project no. 310105.

References

1. KPMG: IKT-sikkerhet i Østre Toten kommune forut for dataangrepet 9. januar 2021. IKT-sikkerhet i Østre Toten kommune forut for dataangrepet 9. januar 2021, Aug. 26, 2021. https://www.ototen.no/_f/p1/i5689ceb7-72b4-44d0-970c-a5c4828047e5/endelig-rapport-26082021-kpmg_sladdet.pdf. Accessed 2 Sept 2021
2. Preis, B., Susskind, L.: Municipal cybersecurity: more work needs to be done. Urban Aff. Rev. (2020). https://doi.org/10.1177/1078087420973760
3. Fink, A.: Conducting Research Literature Reviews: From the Internet to Paper, 5th edn. Sage, Los Angeles (2020)
4. Petersen, K., Vakkalanka, S., Kuzniarz, L.: Guidelines for conducting systematic mapping studies in software engineering: an update. Inf. Softw. Technol. **64**, 1–18 (2015). https://doi.org/10.1016/j.infsof.2015.03.007
5. Petersen, K., Feldt, R., Mujtaba, S., Mattsson, M.: Systematic mapping studies in software engineering (2008). https://doi.org/10.14236/ewic/EASE2008.8
6. Ismagilova, E., Hughes, L., Rana, N.P., Dwivedi, Y.K.: Security, privacy and risks within smart cities: literature review and development of a smart city interaction framework. Inf. Syst. Front. (2020). https://doi.org/10.1007/s10796-020-10044-1
7. Pelton, J.N., Singh, I.B.: Cyber defense in the age of the smart city. In: Smart Cities of Today and Tomorrow, pp. 67–83. Springer International Publishing, Cham (2019). https://doi.org/10.1007/978-3-319-95822-4_4
8. Habibzadeh, H., Nussbaum, B.H., Anjomshoa, F., Kantarci, B., Soyata, T.: A survey on cybersecurity, data privacy, and policy issues in cyber-physical system deployments in smart cities. Sustain. Cities Soc. **50**, 101660 (2019). https://doi.org/10.1016/j.scs.2019.101660
9. Vitunskaite, M., He, Y., Brandstetter, T., Janicke, H.: Smart cities and cyber security: are we there yet? A comparative study on the role of standards, third party risk management and

security ownership. Comput. Secur. **83**, 313–331 (2019). https://doi.org/10.1016/j.cose.2019.02.009
10. Ullah, F., Qayyum, S., Thaheem, M.J., Al-Turjman, F., Sepasgozar, S.M.E.: Risk management in sustainable smart cities governance: a TOE framework. Technol. Forecast. Soc. Chang. **167**, 120743 (2021). https://doi.org/10.1016/j.techfore.2021.120743
11. Dickens, C., Boynton, P., Rhee, S.: Principles for designed-in security and privacy for smart cities. In: Proceedings of the Fourth Workshop on International Science of Smart City Operations and Platforms Engineering, pp. 25–29, New York, NY, USA (2019). https://doi.org/10.1145/3313237.3313300
12. Neshenko, N., Nader, C., Bou-Harb, E., Furht, B.: A survey of methods supporting cyber situational awareness in the context of smart cities. J. Big Data **7**(1), 92 (2020). https://doi.org/10.1186/s40537-020-00363-0
13. Paul, R., Ghosh, N., Sau, S., Chakrabarti, A., Mohapatra, P.: Blockchain based secure smart city architecture using low resource IoTs. Comput. Netw. **196**, 108234 (2021). https://doi.org/10.1016/j.comnet.2021.108234
14. Rejeb, A., Rejeb, K., Simske, S.J., Keogh, J.G.: Blockchain technology in the smart city: a bibliometric review. Qual Quant (2021). https://doi.org/10.1007/s11135-021-01251-2
15. Vandercruysse, L., Buts, C., Dooms, M.: A typology of Smart City services: the case of data protection impact assessment. Cities **104**, 102731 (2020). https://doi.org/10.1016/j.cities.2020.102731
16. Lindstrom, J., Viklund, P., Tideman, F., Hallgren, B., Elvelin, J.: Oh, no—not another policy! Oh, yes—an OT-policy!, vol. 81, pp. 582–587 (2019). https://doi.org/10.1016/j.procir.2019.03.159
17. Gouglidis, A., König, S., Green, B., Rossegger, K., Hutchison, D.: Protecting water utility networks from advanced persistent threats: a case study. In: Rass, S., Schauer, S. (eds.) Game Theory for Security and Risk Management, pp. 313–333. Springer International Publishing, Cham (2018). https://doi.org/10.1007/978-3-319-75268-6_13
18. Ivanova, K.: Online voting as an element of cybersecurity of megacities. Pravoprimenenie-Law Enforcement Rev. **3**(2), 31–37 (2019). https://doi.org/10.24147/2542-1514.2019.3(2).31-37
19. Cardillo, A., Akinyokun, N., Essex, A.: Online voting in Ontario municipal elections: a conflict of legal principles and technology? vol. 11759, pp. 67–82 (2019). https://doi.org/10.1007/978-3-030-30625-0_5
20. Schürmann, C., Jensen, L.H., Sigbjörnsdóttir, R.M.: Effective cybersecurity awareness training for election officials. In: Krimmer, R., Volkamer, M., Beckert, B., Küsters, R., Kulyk, O., Duenas-Cid, D., Solvak, M. (eds.) Electronic Voting, vol. 12455, pp. 196–212. Springer International Publishing, Cham (2020). https://doi.org/10.1007/978-3-030-60347-2_13
21. Andreasson, A., Artman, H., Brynielsson, J., Franke, U.: A census of Swedish public sector employee communication on cybersecurity during the COVID-19 Pandemic. In: 2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), Jun. 2021, pp. 1–8. https://doi.org/10.1109/CyberSA52016.2021.9478241
22. Pike, R.: Enhancing cybersecurity capability in local governments through competency-based education. In: Hawaii International Conference on System Sciences 2021 (HICSS-54), Jan. 2021 [Online]. https://aisel.aisnet.org/hicss-54/dg/cybersecurity_and_government/3
23. Marett, K., Nabors, M.: Local learning from municipal ransomware attacks. In: AMCIS 2020 Proceedings, Aug. 2020 [Online]. https://aisel.aisnet.org/amcis2020/data_science_analytics_for_decision_support/data_science_analytics_for_decision_support/6
24. Gedris, K., et al.: Simulating municipal cybersecurity incidents: recommendations from expert interviews. In: Hawaii International Conference on System Sciences 2021 (HICSS-54), Jan. 2021 [Online]. https://aisel.aisnet.org/hicss-54/dg/cybersecurity_and_government/5
25. Østby, G., Katt, B.: Cyber crisis management roles—a municipality responsibility case study. In: Murayama, Y., Velev, D., Zlateva, P. (eds.) Information Technology in Disaster Risk Reduction, vol. 575, pp. 168–181. Springer International Publishing, Cham, 2020. https://doi.org/10.1007/978-3-030-48939-7_15

26. Norris, D.F., Mateczun, L., Joshi, A., Finin, T.: Managing cybersecurity at the grassroots: Evidence from the first nationwide survey of local government cybersecurity. J. Urban Aff. **43**(8), 1173–1195 (2021). https://doi.org/10.1080/07352166.2020.1727295
27. Kesan, J.P., Zhang, L.: An empirical investigation of the relationship between local government budgets, IT expenditures, and cyber losses. IEEE Trans. Emerg. Top. Comput. **9**(2), 582–596 (2021). https://doi.org/10.1109/TETC.2019.2915098
28. Nussbaum, B., Park, S.: A tough decision made easy? Local government decision-making about contracting for cybersecurity. New York, NY, USA (2018). https://doi.org/10.1145/3209281.3209368
29. Ali, O., Shrestha, A., Chatfield, A., Murray, P.: Assessing information security risks in the cloud: a case study of Australian local government authorities. Gov. Inf. Q. **37**(1), 101419 (2020). https://doi.org/10.1016/j.giq.2019.101419
30. Ibrahim, A., Valli, C., McAteer, I., Chaudhry, J.: A security review of local government using NIST CSF: a case study. J. Supercomput. **74**(10), 5171–5186 (2018). https://doi.org/10.1007/s11227-018-2479-2
31. Gomes, H., Zúquete, A., Dias, G.P., Marques, F., Silva, C.: Evolution of HTTPS usage by portuguese municipalities. In: Rocha, Á., Adeli, H., Reis, L.P., Costanzo, S., Orovic, I., Moreira, F. (eds.) Trends and Innovations in Information Systems and Technologies, vol. 1160, pp. 339–348. Springer International Publishing, Cham. https://doi.org/10.1007/978-3-030-45691-7_31