



Does inter-municipal collaboration strengthen cybersecurity?

David Karlsson, Max Boholm & Johan Berlin

To cite this article: David Karlsson, Max Boholm & Johan Berlin (24 Mar 2026): Does inter-municipal collaboration strengthen cybersecurity?, Journal of Cyber Policy, DOI: [10.1080/23738871.2026.2642608](https://doi.org/10.1080/23738871.2026.2642608)

To link to this article: <https://doi.org/10.1080/23738871.2026.2642608>



© 2026 The Author(s). Published by Informa UK Limited, trading as Taylor & Francis Group



Published online: 24 Mar 2026.



Submit your article to this journal [↗](#)



Article views: 86



View related articles [↗](#)



View Crossmark data [↗](#)

Does inter-municipal collaboration strengthen cybersecurity?

David Karlsson^a, Max Boholm^a and Johan Berlin^{a,b}

^aSchool of Public Administration, University of Gothenburg, Gothenburg, Sweden; ^bDepartment of Social and Behavioural Studies, University West, Trollhättan, Sweden

ABSTRACT

With municipalities increasingly digitising and sharing data, the complexity and risks of cyberthreats are growing, requiring stronger local government cybersecurity measures. Inter-municipal collaboration (IMC) has been identified as a key strategy to enhance cybersecurity, and this study examines its impact on Swedish municipalities. A survey was conducted across all municipalities to assess the extent of IMC, and a Cybersecurity Index (CIX) was developed to measure their cybersecurity efforts. Our analysis evaluates cybersecurity strategies at different collaboration levels. However, the results show that while IMC is widespread, its expected benefits in strengthening cybersecurity are not empirically supported, even for smaller municipalities. The study also highlights risks to public service resilience when municipalities become overly dependent on collaboration. Given the reliance on unproven collaborative solutions, these findings suggest a critical re-evaluation of IMC strategies in municipal cybersecurity management.

ARTICLE HISTORY

Received 3 December 2024
Revised 17 September 2025
Accepted 16 December 2025

KEYWORDS

Cybersecurity; local government; inter-municipal collaboration; public service resilience; policies; Sweden

1. Introduction

Large amounts of sensitive information about both individuals and infrastructure are managed by municipalities throughout the world. Local authorities are digitising rapidly, with IT systems and technologies being developed to automate service operations and establish new channels of communication with citizens (see Gasco Hernandez 2024; Kuhlmann and Heuberger 2023). This development creates a range of new challenges for municipalities.

One such major challenge is that, as municipalities increasingly engage in data sharing to enhance public service delivery, they must balance the benefits of transparency with the risks of cyberthreats (Caldarulo, Olsen, and Feeny 2024). Unfortunately, this also means that, much like any other entity in today's digital world, municipal administrations are vulnerable to information security risks and cyberattacks (Norris et al. 2023; Norris and Mateczun 2022). These threats may come from actors seeking to harm specific municipalities or society at large, or those that want to alter, destroy, block or access sensitive

CONTACT David Karlsson  david.karlsson@spa.gu.se  School of Public Administration, University of Gothenburg, Post Box 712, SE40530 Gothenburg, Sweden

© 2026 The Author(s). Published by Informa UK Limited, trading as Taylor & Francis Group
This is an Open Access article distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/4.0/>), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. The terms on which this article has been published allow the posting of the Accepted Manuscript in a repository by the author(s) or with their consent.

information (Caldarulo, Olsen, and Feeney 2024). Given these heightened security risks associated with vital public services, it is crucial that municipalities are prepared and that they establish concrete and effective policies and protocols to address cybersecurity issues as they arise (Boholm, Berlin, and Karlsson forthcoming; Hatcher, Meares, and Heslen 2020). There has recently been a notably significant growth in cybersecurity practices, although research specifically related to local government cybersecurity is still relatively scarce (as noted by Preis and Susskind 2022; Sandstig, Boholm, and Berlin 2026; Vestad and Yang 2023).

As self-governing entities, municipalities are generally responsible for organising their own operations, including matters concerning preparedness and security. However, given their widely varying capabilities, municipalities are facing formidable challenges. The ability of municipalities to manage these tasks, which – at least in part – are advanced and technical, varies greatly based on a number of factors. The size of the municipality, available financial resources, geographical location, and access to relevant expertise are among the factors that may influence their capabilities. This disparity presents a significant obstacle, especially in the context of multilevel governance, where it is becoming essential to ensure that all responsible units are well-equipped to fulfil their duties.

In navigating these capacity challenges – in cybersecurity as well as in many vital operational areas in local government – many municipalities have engaged in various forms of *inter-municipal collaboration* (IMC)¹ (Teles and Swianiewicz 2018). Among other potential benefits, advocates expect IMC to bring about economies of scale. Collaboration provides opportunities to share key experts and for the joint development of policy tools (Bel and Warner 2015) that might be useful in tackling cybersecurity threats. Collaborative relationships also provide the possibility to learn from each other's past experiences of cyber incidents (Fusi, Jung, and Welch 2023). Zhen Li and Qi Liao (2018) have specifically highlighted the establishment of collaboration mechanisms to pool government cybersecurity resources and avoid unnecessary competition among agencies as a topic in need of further research. Similarly, Donald F. Norris and Laura K. Mateczun (2022) emphasise the critical role of partnerships in alleviating resource constraints in local government cybersecurity. They recommend collaboration not only with other municipalities but also with universities and regional organisations to enhance capacity and share expertise.

As we will see, the literature suggests that, while IMC is becoming increasingly common across various operational areas, its success is by no means always guaranteed. The anticipated gains in terms of efficiency and quality might remain unrealised in certain scenarios. Moreover, the effectiveness of IMC seems to vary depending on the operational area. For example, areas linked to administrative systems and operational support, which do not have the intricate political complexities of core municipal activities such as education and social care, may stand a better chance of benefiting from coordination as IMC may offer the possibility of sharing infrastructure, as well as relief from administrative and managerial burdens, through the utilisation of professional management (Struk and Bakoš 2021). If this is the case, managing cybersecurity would be an area that is particularly suited for IMC, and especially for smaller municipalities that might not possess the resources to manage security operations efficiently on their own (Hatcher, Meares, and Heslen 2020).

Taking into consideration the assumptions made in previous IMC studies, the aim of this article is to examine more closely the dynamics of collaborative cybersecurity efforts. Our primary aim is to investigate *whether inter-municipal collaboration (IMC)*

contributes to strengthening cybersecurity in local government. To achieve this, the study focuses on two empirical research questions: Firstly, *to what extent do municipalities collaborate on cybersecurity efforts?* Secondly, *does the extent and nature of such collaborations contribute to enhancing the level of ambition in relation to cybersecurity in the municipalities?* In addressing the research questions, our study will focus on Swedish local government, adopting a policy-focused perspective to highlight the municipalities' strategic commitment and readiness to face both current and future cybersecurity challenges.

The question of the prevalence of IMC in cybersecurity is a critical initial step in examining the effects of such collaboration. To our knowledge, as of yet no comprehensive study has explored the extent of IMC in the cybersecurity field within a national context. Charting the actual landscape of IMC in cybersecurity across Sweden consequently represents a significant empirical contribution in its own right. More importantly, however, without systematic knowledge of the prevalence of IMC, research has lacked the empirical foundation necessary to assess its potential impact. This article seeks to enhance our understanding and investigate whether this type of prevalent strategy actually contributes to fortifying cybersecurity in municipalities, moving towards a critical perspective on methodologies and a pathway to evidence-based strategies that are effective.

The importance of *security policies* is frequently emphasised in the literature concerning cybersecurity management (Azmi, Tibben, and Win 2018; Cram, Proudfoot, and D'Arcy 2017; Hatcher, Meares, and Heslen 2020). Norris et al. (2023) and Norris and Mateczun (2025) emphasise that policy adoption and implementation are essential for local governments to be able to provide high levels of cybersecurity (Boholm, Berlin, and Karlsson forthcoming). Moreover, the emphasis on taking concrete action to strengthen cybersecurity and monitoring the effectiveness of previous action plans is supported by various frameworks (Atoum, Ootom, and Ali 2014; Azmi, Tibben, and Win 2018; Eloff and Eloff 2005).

To assess the level of ambition of Swedish municipalities in relation to cybersecurity from a policy perspective, we will focus on their policies, action plans and risk assessments. To facilitate this investigation and examine variations in approaches among municipalities, we have developed a *Cybersecurity Index* (CIX). This index is a novel contribution made by this study, and it will serve as an indicator of the ambition and priority levels of municipal cybersecurity. Additionally, we will employ data from a comprehensive survey targeting *Chief Information Security Officers* (CISOs), or their equivalents, in examining each municipality's collaborative efforts in relation to cybersecurity. This approach not only aids in understanding the scope of collaboration but, in conjunction with the CIX, it also helps to explore the potential benefits of IMC for cybersecurity. By controlling for relevant factors, we aim to determine whether the theoretical expectations surrounding IMC and cybersecurity enhancement hold true in practice.

2. Cybersecurity collaboration and IMC

A main theme in public management literature is that inter-organisational collaboration in the public sector is desirable, even a self-evident virtue of advanced societies (Hudson et al. 1999). Public authorities are also more and more dependent on collaboration within

inter-organisational networks to deliver integrated digital public services (Wouters et al. 2023). The importance of collaboration has been particularly emphasised in the context of cybersecurity (Azmi, Tibben, and Win 2018; Li and Liao 2018).

Cybersecurity is a domain where collaboration is often indispensable: the security of individual organisations can impact others, specialised expertise is scarce, threats evolve rapidly, and protective measures require continuous adaptation. Moreover, collaboration in cybersecurity is particularly dependent on the willingness of actors to share sensitive information, which is both essential for, and often a barrier to, effective joint action (Dunn-Cavelty and Suter 2009; Solansky and Beck 2021).

While municipalities are formally responsible for their own cybersecurity, research shows that few organisations – particularly those with limited resources and capacity – are able to sustain high levels of security on their own. As a result, many municipalities depend on both other public authorities and private-sector actors for support. Public-private partnerships (PPPs) have therefore become a mechanism for pooling knowledge, sharing threat intelligence and coordinating protective measures (Dunn-Cavelty and Suter 2009). Yet research also shows that such partnerships are not always functional arrangements but often problematic (Carr 2016; Newlove-Eriksson, Giacomello, and Eriksson 2018). PPPs for cybersecurity are shaped by tensions between divergent interests (Dunn-Cavelty and Suter 2009), with loyalty and professional networks playing an important role in sustaining cooperation (Christensen and Petersen 2017). Analyses of national cybersecurity strategies indicate that while PPPs are widely invoked, most states still emphasise state-centric and domestically focused measures (Craig, Johnson, and Gallop 2022). Evidence from Ukraine further illustrates how PPPs can be crucial in practice, enabling rapid and large-scale private-sector contributions to national cyber defence, but also highlights challenges related to coordination, sustainability and diverging incentives (Axon et al. 2024). More broadly, research on PPPs highlights that collaboration in the field of cybersecurity presents a distinct set of challenges. These arise from the combination of high technical complexity, the sensitivity and rapidly evolving nature of threat intelligence, strong interdependencies across organisational boundaries, fragmented roles and responsibilities, and the need for continuous political negotiation (Dunn Cavelty 2025).

Within the broader collaboration literature, one of the most prominent and widely studied forms of public inter-organisational cooperation is inter-municipal collaboration (IMC). Here, local authorities cooperate with each other in various ways as a strategy to streamline and improve public services. Such collaboration may involve networking, information-sharing, joint activities across technical and welfare sectors, and the pooling of administrative and technical support. Notably, such collaborations also encompass initiatives in the wider realm of e-governance (Helin 2020).

IMC emerges for several reasons (Erlingsson, Isaksson, and Persson 2021), with financial motivations paramount as municipalities seek economies of scale to cut overheads and administrative costs (Silvestre, Marques, and Gomes 2018; Tavares and Feiock 2018). A related incentive is the rationalisation and heightened efficiency that derives from large-scale operations, allowing municipalities to broaden their services and deliver more at the same cost as previously. IMC is also a potential approach to tackling recruitment challenges and, as with larger organisations, establishing a workforce with all the essential specialist competence required (see Mattisson 2017; Meltzer 2024).

However, studies examining the effects of IMC, especially in relation to these objectives, have yielded mixed results. Some research has shown limited or no significant effects in terms of quality, cost and efficiency (e.g. Dahlberg and Helin 2017; Elston, Bel, and Wang 2023; Luca and Modrego 2021). That said, where cost savings from collaboration are limited, IMC may still have benefits in terms of better service quality or access to services (Aldag, Warner, and Bel 2019). Furthermore, the number of partners in a collaborative effort or the form of the collaboration can affect the benefits (Blåka 2017; Blåka, Jacobsen, and Morken 2023). If, for example, the collaboration occurs in a project form, the advantages of cooperation risk being confined to the project and not integrated into the regular activities of the participating organisations (Löfström 2010).

Another challenge that may arise relates to asymmetries in collaboration, where smaller partner municipalities may benefit from improved service quality but at the cost of reduced decision-making autonomy, whereas larger host municipalities may experience an adverse impact on service quality without changes in decision-making autonomy (Arntsen, Torjesen, and Karlsen 2021).

Previous studies provide evidence that IMC facilitates the coordination of interdependent subjects and rationalises existing resources in e-government (Ferro and Sorrentino 2010). In the context of public service resilience, and specifically in the domain of cybersecurity, previous research has also suggested that IMC can improve the ability of local authorities to address critical challenges (Elston and Bel 2023). However, it is likely that the benefits of collaboration are dependent on the nature of the policy area or operations (Baba and Asami 2020). Policymaking in more politicised areas may be less frequently delegated to other actors as local decision-makers often prefer close supervision and control over such policies (Strebel and Bundi 2023).

This article adopts a policy-based approach to cybersecurity, and there are indeed compelling reasons to anticipate that the development of policies by municipalities is predicated on cooperation and learning from other municipalities. The phenomenon of public organisations developing their policies and strategies influenced by the work of other, similar organisations is prevalent. This is known as *horizontal policy diffusion* in the academic literature (Wasserfallen 2018), where the term ‘horizontal’ refers to the exchange of ideas and practices between organisations at the same level (e.g. municipalities or states), as opposed to ‘vertical diffusion’, which describes the influence of higher levels of governance on lower ones. Examples of horizontal diffusion in municipal strategic planning include local climate initiatives (e.g. Schoenefeld et al. 2023), and the eService sector (e.g. Cepparulo and Zanfei 2021).

However, while collaboration is often cited as a crucial aspect of cybersecurity in local government that warrants further attention in the research (Li and Liao 2018), no empirical studies have yet examined the impact of IMC on cybersecurity initiatives. Based on general findings in the IMC literature, collaboration likely provides access to expertise and resources that enhance cybersecurity preparedness. It is also expected to facilitate the development of policies and strategies through shared learning. Building on these insights, we posit the following expectations:

H1: Municipalities engaged in IMC are more likely to have developed and implemented cybersecurity measures.

H2: The effects of IMC are expected to be stronger in smaller municipalities than in larger ones, given their more limited internal resources.

These hypotheses guide the subsequent analysis of whether, and under what conditions, IMC strengthens local governments' cybersecurity policies and practices.

3. Methodology and the case of Sweden

In decentralised welfare states, as in the Scandinavian countries, the primary responsibility for implementing essential societal functions lies with sub-national authorities. Alongside Denmark, Sweden possesses the most expansive public sector within the OECD, and the country has one of the most decentralised public administrative systems in the world, with local and regional authorities shouldering a significant overall proportion of public services (Erlingsson et al. 2025; Loughlin, Hendriks, and Lidström 2010; Montin 2015). Approximately one third of Swedes' personal income is channelled directly to local and regional governance through taxes. Municipalities are responsible for healthcare and social welfare, care of the elderly, childcare, primary and secondary education, and integration of immigrants. They also manage emergency services and firefighting, as well as the continuous operation of critical infrastructure, such as electricity, water and sewage, and public transport. The responsibility for these essential services is permanent, in both normal times and during crises, highlighting the vital importance of municipalities from a security and resilience perspective. Most, if not all, of these crucial public services and systems are today facing cybersecurity threats.

A simple media search reveals hundreds of reported incidents of varying scale, yet it is well known that many cases are never publicly reported, and that no national compilation of municipal cyber incidents currently exists. The most widely publicised incident was the Kalix ransomware attack in 2021, which paralysed numerous municipal systems – home care, payroll, email, and internal networks – and forced staff to revert to analogue routines. This case has since been the subject of research (Holmström and Große 2025), and the lessons learned are now widely used in training and knowledge development across the local government sector. In 2024, in Bjurholm, Sweden's smallest municipality, a severe attack shut down almost all internal systems for several weeks. In 2022, the city of Norrköping was forced into crisis mode after detecting a serious intrusion: systems were reset, all staff were required to change passwords, and analogue work routines were prepared. Most incidents, however, are smaller in scale and receive less attention. A typical example is the phishing incident in 2023 in Gislaved, where compromised credentials were used to send fraudulent emails, but a swift response limited the damage.

A more recent case with particularly wide-ranging impact – and with important implications from a collaboration perspective – was the Miljödata attack in 2025. A breach against this occupational health system provider simultaneously affected around 200 municipalities and regions, and highly sensitive personnel data were exposed. The incident starkly demonstrated how reliance on shared digital systems can create cascading vulnerabilities, underscoring the policy dilemma between efficiency gains through joint platforms and the systemic risks such dependence entails.

In Sweden, the responsibility for cybersecurity within the municipalities is regulated through a combination of national legislation, policy documents and guidelines developed by various authorities. The primary responsibility for cybersecurity rests with each

individual municipality, which are legal entities with significant autonomy. This autonomy means that the municipalities themselves decide how to organise their work within the framework of national laws and regulations. Municipalities' responsibilities are expected to further increase under a forthcoming Cybersecurity Act, through which the Swedish government is preparing to implement the EU NIS2 Directive. It is proposed that the Act will enter into force in 2026 (SOU 2024:18 Government bill under preparation). In particular, the law will tighten requirements for municipalities to establish documented routines and strategies for areas such as risk analysis, incident management and continuity planning.

In the vast majority of municipalities, operational responsibility for coordinating information security efforts, including cybersecurity matters, rests with a local *Chief Information Security Officer* (CISO) (SKR 2019). In the Swedish context, CISOs are not primarily technical practitioners but act as strategic managers who are typically directly involved in drafting and implementing local cybersecurity policies, while formal approval and oversight rests with senior management or elected representatives.

Swedish municipalities carry extensive responsibilities, but they also vary greatly in their capacity to meet these demands. Small municipalities in rural areas face particular challenges in responding to national requirements, while larger municipalities also need to develop strategic solutions to streamline and make their organisations more efficient. As a result, they have developed a strong and growing habit of using inter-municipal cooperation (IMC) in a wide range of areas (Erlingsson, Isaksson, and Persson 2021; Meltzer and Weichselberger 2022). Swedish local government is therefore a particularly suitable case for studying the relationship between IMC and cybersecurity efforts in complex local administrations. IMC in the field of cybersecurity takes many forms – from informal exchanges of experience, to lending personnel, to larger municipalities taking over functions for smaller neighbours, and to joint municipal companies. Private firms may also be consulted, typically in specialised areas or in connection with acute incidents, but such reliance is less common than inter-municipal collaboration, which tends to serve as a more permanent arrangement. Often, several of these modalities occur simultaneously. CISOs are normally central actors in such collaboration, whatever form it takes.

Conducting the analysis in Sweden offers several methodological advantages. All of Sweden's municipalities have the same responsibilities and operate within the same legal structure, but they have widely differing conditions when it comes to size and socio-economic factors. However, even the smaller municipalities are relatively large by European standards, and Swedish municipalities have a high degree of autonomy in deciding how to organise their operations.

3.1. Measuring levels of ambition in relation to cybersecurity – the Cybersecurity Activity Index (CIX)

We will assess the municipalities' levels of ambition with regards to cybersecurity by using policy-based indicators, such as comprehensive security policies, action plans, follow-ups, and the inclusion of cybersecurity in risk assessments. Given the rapid evolution of cybersecurity threats and technologies, our policy-focused approach evaluates how municipalities are addressing current challenges and preparing for future threats (Norris and Mateczun 2025).

This approach also considers the integration of cybersecurity into the general management of IT and risk in the municipality (Soomro, Shah, and Ahmed 2016), highlighting its role in municipal governance and operations. This holistic perspective – in line with Dunn Cavely, et al.'s (2023) emphasis on the social as well as technical dimensions of cyber resilience – is crucial in understanding the prioritisation of cybersecurity within the broader framework of municipal risk management and service delivery.

In the Swedish case, this broader governance environment is shaped by national standards and guidance. Swedish Civil Defence and Resilience Agency (MCF, formerly MSB) issues binding requirements regarding policies for national authorities, but these do not extend to municipalities. Instead, municipalities face strong expectations from central government and professional norms to articulate strategic direction, adopt policies, conduct risk assessments, and evaluate activities. These expectations are reinforced by international standards (e.g. ISO 27001) and MCF's national guidance, which mirrors such standards. While voluntary, this creates a common framework that all municipalities are expected to follow, though with substantial variation in how far they succeed in meeting these expectations.

This study introduces the Cybersecurity Index (CIX) as a measure of the ambition and priority given to cybersecurity in Swedish municipalities, as reflected by their cybersecurity-related policies. CIX assesses the extent to which a municipality has implemented various cybersecurity policies and whether cybersecurity is integrated into general policies for information technology (IT) and risk management.

CIX consists of six binary features, each assigned a value of 1 if met and 0 if not. The first two features assess whether a municipality has information security policies at two levels (Paananen, Lapke, and Siponen 2020): a 'security programme policy' outlining the strategic direction and scope of cybersecurity, and 'issue-specific security policies' for usage and configuration of IT systems (Cram, Proudfoot, and D'Arcy 2017). In the context of Swedish municipalities, there is no distinct terminology for these levels, rather the term 'information security policy' is frequently used for general types of documents, and more specific types of policies are often referred to as an 'instruction' or 'guideline'.

The third and fourth features of CIX assess whether the municipality has a documented action plan and follow-ups for cybersecurity. This addresses whether the municipality has developed concrete actions to strengthen cybersecurity and monitors the effectiveness of previous action plans. Additionally, CIX evaluates whether the municipality deals with cybersecurity issues in its IT policy and Risk and Vulnerability Assessment (RVA). By law, Swedish municipalities are required to conduct regular RVAs that assess the risks associated with their activities and services (Hassel 2012). These latter two features determine whether cybersecurity is integrated into the broader management of IT and risk within the municipality (Soomro, Shah, and Ahmed 2016). The attention to cybersecurity issues in IT policies and RVAs (or not) is operationalised by explicit reference to cybersecurity-related concepts (or the lack thereof), for example: 'cybersecurity', 'information security', 'data protection' and 'cyberattack'.²

Data for the CIX score was collected between October 2022 and April 2023 through requests, sent by email, to all 290 municipalities in Sweden for their latest information security policies, IT policies, action plans, and follow-ups, or their equivalents, whether they had such documents in place, as well as their RVAs. After reminders (in some

cases by phone), we received a response from every municipality. 14 municipalities (5%) did not send us their RVA, citing security reasons.³

As a key dependent variable for our analyses, CIX is thus a composite measure assessing municipalities' commitment and prioritisation of cybersecurity based on a range of indicators. The index is scaled from 0 to 6, with higher scores signifying more advanced cybersecurity practices. Analysis of the CIX from 290 municipalities shows an average score of 2.89 with a standard deviation of 1.26. The median score is 3, reflecting a moderate level of cybersecurity readiness across the municipalities surveyed (Figure 1).

3.2. Measuring inter-municipal collaboration (IMC) – the main independent variables

IMC can manifest in various forms and is influenced by national contexts and by the specific policy area of cooperation. In the Swedish case, while there are some national compilations of different types of collaborations, comprehensive statistics on the prevalence of IMC are not available. Additionally, a significant shortcoming is the lack of information on the degree of intensity of IMC, i.e. how much municipalities actually support each other and depend on one another. Furthermore, there are no compilations of IMC relationships in specific areas like cybersecurity, necessitating separate data collection.

This study employs data from a survey sent to all CISOs or their equivalents across Sweden's 290 municipalities. The survey was carried out in the spring of 2023. Although

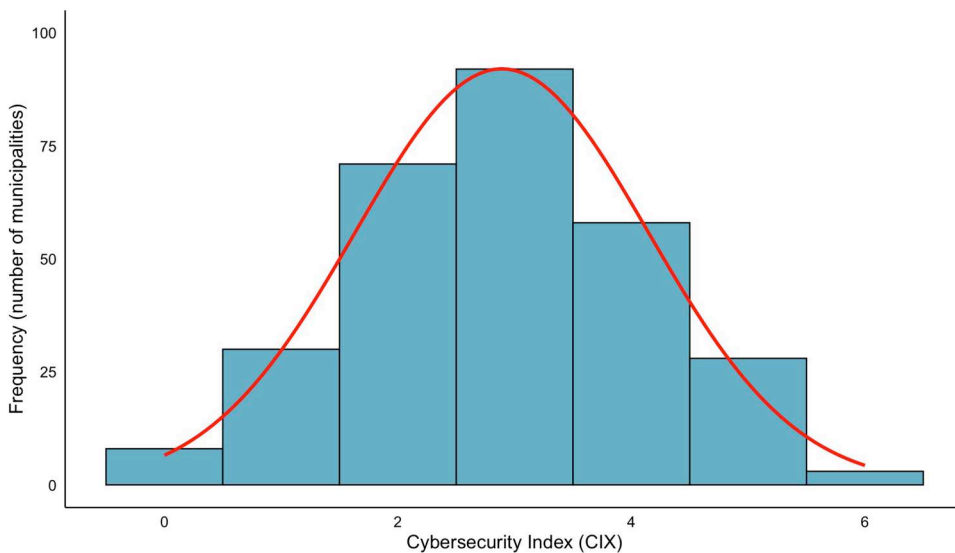


Figure 1. Histogram of the Cybersecurity Index (CIX). Note: This histogram displays the distribution of CIX scores among the 290 Swedish municipalities, overlaid with a normal distribution curve for comparison. The CIX distribution appears roughly symmetric, as evidenced by the skewness value of -0.02 and a kurtosis of 2.66 , indicative of a platykurtic tendency. This symmetry is substantiated by the Shapiro-Wilk test ($W = 0.997$, $p = 0.8759$) and the skewness and kurtosis test ($\chi^2 = 1.64$, $p = 0.44$), both of which imply that the CIX distribution does not significantly deviate from normality. This supports the use of CIX as a variable suitable for parametric analysis in regression models.

the practical aspects of the survey were managed by the Swedish Association of Local Authorities and Regions (SALAR, Swedish: SKR) and its statistics division, we developed most of the questions asked in the survey. We received comprehensive replies from 256 municipalities, equating to an 88% response rate. Of these, 203 (70%) provided complete answers to the question relating to IMC that will be used in this study. The two-part question had the aim of assessing the level of assistance provided by the municipality to others, as well as the extent to which it depended on cybersecurity assistance from other municipalities. Both questions employed a three-tiered response scale indicating whether the municipality did not engage in IMC, provided or received support from other municipalities 'occasionally', or was dependent on the support of others, or conversely, whether other municipalities were reliant on its assistance. The combined responses to these two questions offer an insight into the intensity of collaboration and the symmetry between cooperating parties. The findings derived from these questions will be presented in the first part of the results section below, addressing our first research question.

3.3. Contextual factors and model design

Our analysis will proceed in two steps. In the first step, we aim to discern which municipalities collaborate to varying degrees and identify determinants for whether such collaboration is asymmetric or balanced. In the subsequent step, we turn to our main question of whether the degree of collaboration is associated with how advanced the municipalities' cybersecurity efforts are, as measured through our main dependent variable of CIX. Additionally, it is especially relevant to test whether such a correlation is related to the size of the municipality and whether the collaboration is symmetrical or not. To this end, we also include an interaction model that explicitly tests whether the impact of inter-municipal collaboration on cybersecurity ambitions varies depending on municipal size.

In both steps, it is essential to incorporate control variables. This ensures that the effects we observe are credible and not spurious. A significant control variable relates to the role of the CISO, specifically the extent of the CISO's responsibilities based on two questions from the survey: *Does your municipality have a role tasked with coordinating or leading the overall information security efforts within the municipality as an organisation?*; and *Approximately what proportion of their working hours does the person in this role dedicate to information security work on average per week?* Responses were received from 233 municipalities (80%), 89% of which had a CISO. In certain metropolitan municipalities, multiple individuals may bear the responsibility for cybersecurity even though a single officer is designated as primarily accountable. Contrastingly, in most smaller municipalities, the CISO function is a part-time commitment for one person. For the purposes of this analysis, we will use the time allocated to CISOs as an independent variable. Accordingly, the 11% of municipalities without a CISO will be assigned a value of 0. Those representing the 33% who indicated 1–10 h will be assigned a value of 10, the 12% indicating 11–20 h will receive 20, the 8% indicating 21–30 h will receive 30, and the 30% indicating 31–40 h will receive 40. A minority who affirmed the presence of a CISO but remained non-committal about the time invested are categorised with the median value of 30.

In addition, we have incorporated several potentially relevant control variables. These variables comprise: taxable income per capita in 2023 (which serves as a robust indicator

of the economic status of the population); the percentage of commuters in 2023 (indicative of the degree to which the municipality as a whole relies on a larger nearby municipality); unemployment rates in 2023; the population in 2020 (the variable is logged in order to mitigate the impact of outliers); the number of IT professionals among the daytime population in 2021 (which may potentially provide insights into the availability of expertise in the field of cybersecurity); and changes in taxable income between 2021 and 2023 (as a measure of local growth, indicating whether the municipality's economic development is positive or negative).

4. Results

Our first research question delves into inter-municipal collaboration (IMC) within the realm of cybersecurity: its extent, symmetry and explanatory factors. The analysis draws upon responses from our survey of CISOs and thus relies on information directly from the key individuals in each municipality with the most comprehensive knowledge on this matter.

The question was formulated as follows: *Municipalities can engage in various collaborative relationships with other municipalities in their cybersecurity efforts. Which of the following options best describes the municipality when considering the last three years?* Responses were solicited for *Regarding the municipality's support to other municipalities* and *Regarding the municipality's dependence on other municipalities*.

Regarding providing support to others, the findings revealed that 20% of the municipalities indicated that they had not provided any support to other municipalities; 73% provided support and practical assistance; while 7% disclosed that one or more other municipalities are entirely or primarily dependent on the cybersecurity work carried out by their municipality. Regarding dependence on support from others, the results showed that 9% reported being entirely or primarily dependent on the information security efforts provided by other municipalities, 67% occasionally seek support and practical assistance, and 24% stated they had not received support from other municipalities in their cybersecurity efforts.

Two primary facets emerge from these outcomes. Firstly, the overall extent of collaboration, irrespective of its direction, was assessed in a measure referred to henceforth as *the COL-score* (which is short for collaboration). About 14% of municipalities reported no collaboration at all, scored as $COL = 0$; 16% indicated some level of collaboration (scored as 1); while a substantial 63% indicated a moderate level of collaboration (scored as 2); 3% of municipalities displayed a high level of collaboration (scored as 3); with roughly 4% engaging in extensive and pivotal collaboration (scored as 4). Municipalities with $COL = 4$ rely fully on support from others, while, in turn, other municipalities depend on their assistance. The mean *COL-score* across municipalities stands at 1.7, indicating a general tendency towards moderate collaboration. The second inference pertains to the degree of interdependence between municipalities and whether this relationship is neutral or asymmetric (henceforth referred to as the *AB-score*). Based on the data, approximately 12% can be classified as *Alpha* municipalities, signifying that they provide more support than they receive. Conversely, 8% can be termed as *Beta* municipalities, indicating they receive more support than they contribute. The vast majority, 80%, maintain a reciprocal stance in their collaboration.

In summary, our findings underscore the notable prevalence of IMC in Swedish municipalities regarding cybersecurity, with one in five municipalities actively participating in collaborative efforts. Importantly, a substantial proportion of this collaboration is characterised by symmetry, with municipalities mutually supporting and engaging with one another. While there are instances of Alpha and Beta municipalities, the overarching pattern remains one of symmetrical collaboration.

In the regression models presented in Table 1, we explore the factors shaping the scope of IMC, as measured by the COL-score (Model A4, OLS regression), and the degree of asymmetry in collaboration, as indicated by the AB-score (Model A2 for Alpha municipalities, and Model A3 for Beta municipalities, both logit regression). In the initial model (A1), we investigate the extent to which explanatory variables contribute to explaining the presence of CISO and the extent of their workload. Subsequently, in the following two models, where the COL-score and AB-score serve as dependent variables, the CISO's workload is incorporated as an independent variable. In addition, to address the possibility that the effects of inter-municipal collaboration vary depending on the size of the municipality, we include an interaction term between population size (log) and the scope of inter-municipal collaboration. Both variables are mean-centred before creating the interaction term. This allows us to test whether collaboration has a different impact on municipalities of different sizes, while also reducing collinearity and improving the interpretability of the coefficients.

The results in Table 1 indicate that the presence and workload of a CISO can be significantly explained by the factors included in the model (adjusted $R^2 = 0.31$). Not surprisingly, we find that CISOs are likely to have a heavier workload in larger municipalities.

Table 1. Explaining the CISO's working hours (OLS regression: b-values and robust standard errors) and the degree and nature of IMC (logit regression: log odds and standard errors).

Dependent variable Model	CISO's workload (hours per week 0–40)	Alpha municipality (= 1)	Beta municipality (= 1)	The COL-score (Scope of IMC 0–4)
	OLS	Logit	Logit	OLS
	A1	A2	A3	A4
Population 2020 (log)	40.96*** (5.89)	1.74 (2.32)	–2.88 (3.00)	–0.23 (0.50)
Taxable income per inhabitant 2023	7.53 (9.94)	6.65* (3.02)	–1.34 (5.80)	–2.92** (0.89)
Commuters, share of population 2023	–10.54** (3.98)	–4.34** (1.52)	3.98† (2.20)	0.23 (0.31)
Unemployment 2023	–2.76 (5.21)	0.28 (1.70)	2.41 (2.13)	–0.39 (0.40)
Rural municipality	0.77 (3.10)	–0.93 (1.14)	1.43 (1.01)	0.27 (0.25)
Change in taxable income 2021–23	–9.40 (7.41)	–0.23 (2.34)	3.63† (2.21)	0.60 (0.50)
Number of IT professionals/ 1,000 inh. 2021	17.12* (7.22)	–0.94 (3.35)	–54.49 (39.37)	0.51 (0.50)
CISO – share of full time (0–1)	–	0.08 (0.94)	–1.81† (1.10)	0.47* (0.22)
Constant	15.32** (4.72)	–2.31 (1.51)	–4.61* (1.87)	1.68*** (0.34)
Adj R ²	0.31			0.09
Pseudo R ²		0.19	0.21	
N (number of municipalities)	233	202	202	214

Standard errors in parentheses, † $p < 0.10$, * $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$.

Additionally, controlling for this variable shows that the workload of CISOs is inversely related to the municipality's reliance on neighbouring municipalities, as indicated by commuting patterns. The presence and workload of CISOs also correspond with the proportion of IT professionals in the local labour force.

The models explaining the likelihood of municipalities being classified as Alpha or Beta have pseudo R^2 of 0.19 and 0.21 respectively. The results show that commuting data is a valid predictor of Alpha or Beta status. Municipalities with a lower share of commuters are more likely to be Alpha, while those with a higher share tend to be Beta. This underlines the fact that municipalities in close proximity to larger dominant neighbours often find assurance in their support. Moreover, economically more prosperous municipalities often fall into the Alpha category. A marginal effect, significant only at the 0.10 level, suggests that municipalities with CISOs who have a lower workload are more likely to be Beta municipalities.

In Model A4, economically less advantaged municipalities exhibit higher levels of inter-municipal collaboration. There is a slight, yet significant, positive effect of the CISO's presence on the collaboration scope score, suggesting that municipalities with active CISOs are inclined to collaborate more. This finding is notable, as it implies that the absence of CISOs, or CISOs with lighter workloads, do not necessarily translate into a greater need for collaboration among municipalities.

Although Model A4 shows relatively modest explanatory power, (adjusted $R^2 = .09$), the findings are largely interpretable and meaningful. The validation of the collaboration indicators confirms their usefulness in the subsequent critical phase of the analysis. We proceed to address our second research question, exploring how the extent and nature of inter-municipal collaboration (IMC) impact on municipalities' cybersecurity aspirations.

The outcomes of this analysis are presented in [Table 2](#). In the first model (B1), we explore the effects of our control variables on the Cybersecurity Index (CIX). In the second model (B2), we introduce the IMC indicators alongside the control variables, allowing us to observe how the results evolve and test our hypothesis. Finally, Model B3 incorporates an interaction between municipal size and the scope of IMC.

The results presented in [Table 2](#) demonstrate that our explanatory variables in Model B1 explain 12% of the variance in the CIX. A substantial correlation is apparent between the size of a municipality and how advanced its cybersecurity initiatives are; larger municipalities have notably progressed further in their cybersecurity pursuits. In contrast, municipalities facing high unemployment rates tend to have lower CIX scores, and somewhat surprisingly, the same trend is observed in municipalities with economically prosperous populations. Additionally, there is a moderate, yet significant, positive impact caused by the presence and workload of CISOs on the CIX, although the effect is less marked than anticipated.

Model B2 provides the test of our first hypothesis (H1). Once collaboration indicators are introduced, however, the results are striking; neither the scope nor the symmetry of inter-municipal collaboration shows any discernible association with cybersecurity ambitions. Model B3 extends this analysis by testing our second hypothesis (H2) through an interaction between municipal size and collaboration. The interaction is not statistically significant, indicating that the absence of an IMC effect applies across municipalities regardless of size. Taken together, these findings suggest that collaboration, at

Table 2. Explaining the level of ambition of Swedish municipalities' cybersecurity efforts (CIX-index), OLS-regression (b-values and robust standard errors).

Dependent variable Model	CIX		
	B1	B2	B3
Population 2020 (log)	2.82*** (0.64)	2.98*** (0.75)	
Taxable income per inhabitant 2023	-2.18* (1.07)	-2.75 [†] (1.52)	-2.76 [†] (1.53)
Commuters, share of population 2023	0.31 (0.40)	0.36 (0.51)	0.34 (0.50)
Unemployment 2023	-0.84 [†] (0.50)	-1.20* (0.54)	-1.16* (0.54)
Rural municipality = 1	-0.18 (0.27)	-0.11 (0.33)	-0.12 (0.33)
Change in taxable income 2021–23	0.40 (0.64)	0.53 (0.68)	0.52 (0.69)
Number of IT professionals/1,000 inh. 2021	1.20 (0.82)	-0.89 (0.74)	-0.83 (0.74)
CISO – share of full time (0–1)	0.54* (1.86)	0.50 [†] (1.57)	0.47 (0.30)
Alpha municipality = 1		-0.06 (0.26)	-0.08 (0.26)
Beta municipality = 1		-0.30 (0.36)	-0.30 (0.36)
COL-score – Scope of IMC 0–1		0.23 (0.42)	
Population 2020 (log, centered)			3.00*** (0.76)
Scope of IMC (centred)			0.20 (0.41)
Population × Scope of IMC			-1.70 (2.69)
Constant	1.97*** (0.44)	1.97** (0.48)	3.12*** (0.52)
Adj R ²	0.12	0.12	0.12
N (number of municipalities)	233	202	202

Standard errors in parentheses, [†] $p < 0.10$, * $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$.

least in its present form, does not enhance municipalities' cybersecurity ambitions, whether in smaller or larger local governments.

4.1. Control analyses and limitations of the study

When expected effects are not observed in an analysis, it naturally raises questions about potential deficiencies in the model, or the variables used. Measuring the degree and nature of IMC in a specific field like cybersecurity across an entire country presents inherent challenges. These include identifying metrics that adequately capture the complexity of municipal collaboration and accurately represent ambition levels in cybersecurity. Such methodological difficulties likely explain the absence of previous studies investigating the impact of collaboration on municipal cybersecurity efforts. Consequently, we lack a body of prior research with which to compare our findings directly.

To address these challenges, we undertook additional control analyses. This included testing various alternative models, adjusting control variables, and exploring different formats of key variables. One such test examined the potential for horizontal policy diffusion by correlating municipalities' CIX scores with those of their neighbours. However, no consistent correlations were identified, suggesting that horizontal

diffusion is not a significant factor in explaining variations in municipal cybersecurity. Furthermore, in relation to H2 we conducted robustness checks examining potential moderating effects of key municipal characteristics, including size, urban-rural classification, and other contextual factors. These analyses revealed no significant interaction effects between IMC and these variables, nor any consistent patterns suggesting that collaboration enhances cybersecurity efforts in specific types of municipalities.

While these findings highlight the methodological difficulties inherent in studying IMC, they also underscore the robustness of our chosen approach. Our metrics, though not exhaustive, are independently measured and grounded in established policy-based frameworks. Within the regression models, they demonstrate a reasonable degree of interpretability in relation to the explanatory factors included. Ultimately, we believe our method provides a reliable and valid foundation for analysing the relationship between IMC and cybersecurity.

5. Conclusions and discussion

The aim of this study has been to investigate whether IMC contributes to strengthening cybersecurity in local government. We formulated two hypotheses: H1, that IMC would increase the likelihood of municipalities developing cybersecurity measures, and H2, that such effects would be stronger in smaller municipalities. Our analyses, however, did not support either hypothesis.

The main conclusions of the analysis are clear and unequivocal: Swedish municipalities do indeed collaborate extensively with each other on cybersecurity issues. In most cases, this collaboration is reciprocal, i.e. they both provide and receive support in equal measure, even though there are notable asymmetrical exceptions, with some municipalities fully dependent on others.

However, none of the anticipated positive effects of IMC on the levels of ambition that municipalities have for cybersecurity, as measured by our policy-based index CIX, were observed, and this was even the case for smaller municipalities, where IMC was expected to be most beneficial.

The results of our study regarding the non-existent collaboration effects contribute to the existing body of literature on IMC. It has often been pointed out that, on occasion, parts of this field are overly optimistic in tone, with many making the presumption that collaboration always results in positive outcomes. Our findings thus resonate with a more critical and nuanced segment of the literature on IMC, which underscores potential challenges and limitations inherent in collaborative efforts, and outlines several conditions that must be met for success (e.g. Blåka 2017; Blåka, Jacobsen, and Morken 2023; Dahlberg and Helin 2017; Elston, Bel, and Wang 2023; Löfström 2010; Luca and Modrego 2021). Furthermore, the literature on IMC has primarily focused on the effects of collaboration in terms of cost reduction and efficiency (Silvestre, Marques, and Gomes 2018; Tavares and Feiock 2018). Other types of effects have been studied to varying degrees. This study contributes to the IMC literature pertaining to an area where previous studies are largely lacking: the effects of collaboration in relation to policy development and quality management.

Although experienced researchers in the field of IMC, who are well-acquainted with its complexities, may not find the results of this study particularly surprising, the results

nevertheless prompt significant considerations for the sparse literature on municipal cybersecurity (Preis and Susskind 2022; Vestad and Yang 2023). While this literature highlights collaboration as an important strategy (Fusi, Jung, and Welch 2023; Hatcher, Meares, and Heslen 2020; Li and Liao 2018), the effectiveness of IMC has not been empirically examined in this context before. Given the high level of collaboration engaged in by nearly all municipalities, our findings suggest a need to critically re-evaluate collaborative strategies in municipal cybersecurity management.

The absence of positive impacts from IMC on municipal cybersecurity also emphasises the necessity for a more critical examination of collaboration strategies from a resilience perspective. It is reasonable to question whether it makes sense for municipalities to prioritise collaboration rather than develop their own internal capacity for managing cybersecurity. This is particularly relevant for IMC with asymmetric relations (cf. Arntsen, Torjesen, and Karlsen 2021), where some municipalities have found themselves entirely dependent on the support of others. The risk with all forms of collaboration is that participation is voluntary, and there is a clear danger in relying too much on others who are not obligated to help in critical situations.

However, an obvious caveat to consider is that collaboration might yield benefits beyond those addressed by our policy-based cybersecurity index (CIX). While policies and strategies are certainly widely emphasised as crucial tools for cybersecurity (e.g. Norris et al. 2023), the work in this field encompasses far more than can be documented and measured through policy-based indicators. This includes daily technical information exchanges and informal contacts that enhance resilience, as well as backup capabilities in times of crisis. Future research should therefore delve deeper into how IMC can contribute to these aspects, ideally through in-depth qualitative case studies.

Notes

1. The literature on IMC interchangeably uses the terms '*cooperation*' and '*collaboration*' to indicate the interactions between municipalities. In this article, we will consistently use '*collaboration*' (although many of the studies we refer to prefer '*cooperation*') to emphasise the concrete, action-oriented nature of the interactions we are examining, differentiating from potentially less tangible forms of cooperation.
2. A list of over 100 search terms resulted in the Swedish equivalents of the following terms being identified in IT policies and RVAs: 'antivirus program', 'cyberattack', 'cybercrime', 'cybercriminal', 'cyber defence', 'cyberthreat', 'cybersecurity', 'data protection', 'data security', 'DDOS attack', 'disinformation', 'hacker', 'information security', 'IT attack', 'IT crime', 'IT incident', 'IT security', 'encryption', 'malware', 'phishing', 'ransomware', 'spam', 'trojan', and 'overload attack'.
3. For municipalities that did not provide their RVA, the CIX feature was coded as 0, treating missing information as absence of the feature. As robustness checks, we also constructed versions of the index where the RVA feature was excluded altogether or where missing values were imputed with the mean. All approaches yielded highly consistent results, and the overall findings and interpretations remain unchanged.

Acknowledgements

We thank the municipalities that participated in the cybersecurity survey conducted in collaboration with the Swedish Association of Local Authorities and Regions (SALAR). In particular, we would like to express our appreciation to Jonas Nilsson, Information Security Manager at the Swedish

Association of Local Authorities and Regions, for his valuable cooperation in the design of the survey. Finally, we thank the anonymous reviewers for their constructive and insightful comments. The authors used OpenAI's GPT models (ChatGPT, versions GPT-4 to GPT-5) for English language editing and translation support.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Funding

This work was supported by Vetenskapsrådet [Grant Numbers 2021-06310 and 2022-05405]; Svenska Forskningsrådet Formas [Grant Number 2021-02229].

References

- Aldag, Austin M., Mildred E. Warner, and Germà Bel. 2019. "It Depends on What You Share: The Elusive Cost Savings from Service Sharing." *Journal of Public Administration Research and Theory* 30 (2): 275–289. <https://doi.org/10.1093/jopart/muz023>.
- Arntsen, Bjørnulf, Dag Olaf Torjesen, and Tor-Ivar Karlsen. 2021. "Asymmetry in Inter-Municipal Cooperation in Health Services – How Does it Affect Service Quality and Autonomy?" *Social Science & Medicine* 273:113744. <https://doi.org/10.1016/j.socscimed.2021.113744>.
- Atoum, Issa, Ahmed Otoom, and Amer Abu Ali. 2014. "A Holistic Cyber Security Implementation Framework." *Information Management & Computer Security* 22 (3): 251–264.
- Axon, Louise, Jamie Saunders, Patricia Esteve-González, Julia Carver, William Dutton, Michael Goldsmith, and Sadie Creese. 2024. "Private-Public Initiatives for Cybersecurity: The Case of Ukraine." *Journal of Cyber Policy* 9 (3): 399–422. <https://doi.org/10.1080/23738871.2025.2451256>.
- Azmi, Riza, William Tibben, and Khin Than Win. 2018. "Review of Cybersecurity Frameworks: Context and Shared Concepts." *Journal of Cyber Policy* 3 (2): 258–283. <https://doi.org/10.1080/23738871.2018.1520271>.
- Baba, Hiroki, and Yasushi Asami. 2020. "Municipal Population Size and the Benefits of Inter-Municipal Cooperation: Panel Data Evidence from Japan." *Local Government Studies* 46 (3): 371–393. <https://doi.org/10.1080/03003930.2019.1624257>.
- Bel, Germà, and Mildred E. Warner. 2015. "Inter-Municipal Cooperation and Costs: Expectations and Evidence." *Public Administration* 93 (1): 52–67. <https://doi.org/10.1111/padm.12104>.
- Blåka, Sara. 2017. "Does Cooperation Affect Service Delivery Costs? Evidence from Fire Services in Norway." *Public Administration* 95 (4): 1092–1106. <https://doi.org/10.1111/padm.12356>.
- Blåka, Sara, Dag Ingvar Jacobsen, and Tone Morken. 2023. "Service Quality and the Optimum Number of Members in Intermunicipal Cooperation: The Case of Emergency Primary Care Services in Norway." *Public Administration* 101 (2): 447–462. <https://doi.org/10.1111/padm.12785>.
- Boholm, Max, Johan Berlin, and David Karlsson. Forthcoming. "Cybersecurity." In *The Elgar Encyclopedia of Local and Regional Governments: A Global Perspective*, edited by J. Edwin Benton and John Kincaid. Cheltenham: Edward Elgar Publishing.
- Caldarulo, Mattia, Jared Olsen, and Mary K. Feeney. 2024. "Oversharing: The Downside of Data Sharing in Local Government." *Public Administration* 102 (4): 1647–1664. <https://doi.org/10.1111/padm.12993>.
- Carr, Madeline. 2016. "Public-Private Partnerships in National Cyber-security Strategies." *International Affairs* 92 (1): 43–62. <https://doi.org/10.1111/1468-2346.12504>.
- Cepparulo, Alessandra, and Antonello Zanfei. 2021. "The Diffusion of Public eServices in European Cities." *Government Information Quarterly* 38 (2): 101561. <https://doi.org/10.1016/j.giq.2020.101561>.

- Christensen, Kristoffer Kjærgaard, and Karen Lund Petersen. 2017. "Public-Private Partnerships on Cyber Security: A Practice of Loyalty." *International Affairs* 93 (6): 1435–1452. <https://doi.org/10.1093/ia/iix189>.
- Craig, Anthony J. S., Richard A. I. Johnson, and Max Gallop. 2022. "Building Cybersecurity Capacity: A Framework of Analysis for National Cybersecurity Strategies." *Journal of Cyber Policy* 7 (3): 375–398. <https://doi.org/10.1080/23738871.2023.2178318>.
- Cram, W. Alec, Jeffrey G. Proudfoot, and John D'Arcy. 2017. "Organizational Information Security Policies: A Review and Research Framework." *European Journal of Information Systems* 26:605–641.
- Dahlberg, Tomi, and Ari Helin. 2017. "How IT Governance Practices Contribute to Inter-Municipal ICT Cooperation and Its Benefits." *International Journal of IT/Business Alignment and Governance* 8 (2): 62–79. <https://doi.org/10.4018/IJITBAG.2017070104>.
- Dunn Caveltly, Myriam. 2025. *The Politics of Cyber-Security*. 1st ed. New York: Routledge.
- Dunn Caveltly, Myriam, Christine Eriksen, and Benjamin Scharte. 2023. "Making Cyber Security More Resilient: Adding Social Considerations to Technological Fixes." *Journal of Risk Research* 26 (7): 801–814. <https://doi.org/10.1080/13669877.2023.2208146>.
- Dunn-Caveltly, Myriam, and Manuel Suter. 2009. "Public-Private Partnerships are no Silver Bullet: An Expanded Governance Model for Critical Infrastructure Protection." *International Journal of Critical Infrastructure Protection* 2 (4): 179–187. <https://doi.org/10.1016/j.ijcip.2009.08.006>.
- Eloff, Jan Hendrik Petrus, and Maria Magdalena Eloff. 2005. "Information Security Architecture." *Computer Fraud & Security* 11:10–16.
- Elston, Thomas, and Germà Bel. 2023. "Does Inter-Municipal Collaboration Improve Public Service Resilience? Evidence from Local Authorities in England." *Public Management Review* 25 (4): 734–761. <https://doi.org/10.1080/14719037.2021.2012377>.
- Elston, Thomas, Germà Bel, and Han Wang. 2023. "If It Ain't Broke, Don't Fix It: When Collaborative Public Management Becomes Collaborative Excess." *Public Administration Review* 83 (6): 1737–1760. <https://doi.org/10.1111/puar.13708>.
- Erlingsson, Gissur Ó, David Karlsson, Richard Öhrvall, and Jessika Wide. 2025. *Swedish Local Democracy at the Crossroads. Understanding the Past to Reform the Future*. Cham: Palgrave Macmillan.
- Erlingsson, Gissur Ó., Zeth Isaksson, and Bo Persson. 2021. *Mellankommunal samverkan: Vad är känt om dess effekter? En inventering av kunskapsläget*. Norrköping: CKS, Linköpings universitet.
- Ferro, Enrico, and Maddalena Sorrentino. 2010. "Can Intermunicipal Collaboration Help the Diffusion of E-Government in Peripheral Areas? Evidence from Italy." *Government Information Quarterly* 27 (1): 17–25. <https://doi.org/10.1016/j.giq.2009.07.005>.
- Fusi, Federica, Heyjie Jung, and Eric Welch. 2023. "Technological Vulnerability and Knowledge of Cyber-Incidents: Threats to Innovativeness in Local Governments?" *Public Management Review* 27 (3): 545–571. <https://doi.org/10.1080/14719037.2023.2250362>.
- Gasco Hernandez, Mila. 2024. "Reflections on Three Decades of Digital Transformation in Local Governments." *Local Government Studies* 50 (6): 1028–1040. <https://doi.org/10.1080/03003930.2024.2410830>.
- Hassel, Henrik. 2012. "Risk and Vulnerability Analysis in Practice: Evaluation of Analyses Conducted in Swedish Municipalities." *Natural Hazards* 63:605–628.
- Hatcher, William, Wesley L. Meares, and John Heslen. 2020. "The Cybersecurity of Municipalities in the United States: An Exploratory Survey of Policies and Practices." *Journal of Cyber Policy* 5 (2): 302–325. <https://doi.org/10.1080/23738871.2020.1792956>.
- Helin, Ari. 2020. *Inter-Organisational IT Governance – A Case Study of Municipal ICT Cooperation*. Turku: University of Turku.
- Holmström, Anton, and Christine Große. 2025. "Not All Heroes Wear Capes: Cyber Resilience of the Social Administration at a Swedish Municipality." *Risk, Hazards & Crisis in Public Policy* 16 (3): e70024. <https://doi.org/10.1002/rhc3.70024>.
- Hudson, Bob, Brian Hardy, Melanie Henwood, and Gerald Wistow. 1999. "In Pursuit of Inter-Agency Collaboration in the Public Sector." *Public Management: An International Journal of Research and Theory* 1 (2): 235–260. <https://doi.org/10.1080/14719039900000005>.

- Kuhlmann, Sabine, and Moritz Heuberger. 2023. "Digital Transformation Going Local: Implementation, Impacts and Constraints from a German Perspective." *Public Money & Management* 43 (2): 147–155. <https://doi.org/10.1080/09540962.2021.1939584>.
- Li, Zhen, and Qi Liao. 2018. "Economic Solutions to Improve Cybersecurity of Governments and Smart Cities via Vulnerability Markets." *Government Information Quarterly* 35 (1): 151–160. <https://doi.org/10.1016/j.giq.2017.10.006>.
- Loughlin, John, Frank Hendriks, and Anders Lidström. 2010. *The Oxford Handbook of Local and Regional Democracy in Europe*. Oxford: Oxford University Press.
- Luca, Davide, and Felix Modrego. 2021. "Stronger together? Assessing the causal effect of inter-municipal cooperation on the efficiency of small Italian municipalities." *Journal of Regional Science* 61 (1): 261–293. <https://doi.org/10.1111/jors.12509>.
- Löfström, Mikael. 2010. "Inter-organizational collaboration projects in the public sector: a balance between integration and demarcation." *The International Journal of Health Planning and Management* 25 (2): 136–155. <https://doi.org/10.1002/hpm.1003>.
- Mattisson, Ola. 2017. "Local Government Cooperation: A Better Way to Respond to Conditions?" In *Modernizing the Public Sector*, edited by Irvine Lapsley and Hans Knutsson, 151–164. Abingdon: Routledge.
- Meltzer, Isabell. 2024. *Strategiska samarbeten – roller, relationer och risker i mellankommunala samarbeten*. Gothenburg: University of Gothenburg, School of Public Administration.
- Meltzer, Isabell, and Gustaf Kastberg Weichselberger. 2022. *Fyra år med mellankommunala samarbeten*. KFi: Gothenburg.
- Montin, Stig. 2015. "Municipalities, Regions, and County Councils: Actors and Institutions." In *The Oxford Handbook of Swedish Politics*, edited by Pierre Jon, 367–382. Oxford: Oxford University Press.
- Newlove-Eriksson, Lindy, Giampiero Giacomello, and Johan Eriksson. 2018. "The Invisible Hand? Critical Information Infrastructures, Commercialisation and National Security." *The International Spectator* 53 (2): 124–140.
- Norris, Donald F., Laura Mateczun, William Hatcher, Wesley L. Meares, and John Heslen. 2023. "Local Government Cyber Insecurity: Causes and Recommendations for Improvement." *Public Administration Review* 84 (4): 651–659. <https://doi.org/10.1111/puar.13743>.
- Norris, Donald F., and Laura K. Mateczun. 2022. "Cyberattacks on Local Governments 2020: Findings from a Key Informant Survey." *Journal of Cyber Policy* 7 (3): 294–317. <https://doi.org/10.1080/23738871.2023.2178319>.
- Norris, Donald F., and Laura K. Mateczun. 2025. "Adoption of Cybersecurity Policies at the Grassroots: 2022." *Journal of Cyber Policy* 10 (1): 13–33. <https://doi.org/10.1080/23738871.2025.2512459>.
- Paananen, Hanna, Michael Lapke, and Mikko Siponen. 2020. "State of the Art in Information Security Policy Development." *Computers & Security* 88:101608.
- Preis, Benjamin, and Lawrence Susskind. 2022. "Municipal Cybersecurity: More Work Needs To Be Done." *Urban Affairs Review* 58 (2): 614–629. <https://doi.org/10.1177/1078087420973760>.
- Schoenefeld, Jonas J., Mikael Hildén, Kai Schulze, and Jaana Sorvali. 2023. "What Motivates and Hinders Municipal Adaptation Policy? Exploring Vertical and Horizontal Diffusion in Hessen and Finland." *Regional Environmental Change* 23 (2): 53. <https://doi.org/10.1007/s10113-023-02048-9>.
- Silvestre, Hugo Consciência, Rui Cunha Marques, and Ricardo Corrêa Gomes. 2018. "Joined-up Government of Utilities: a Meta-review on a Public-Public Partnership and Inter-Municipal Cooperation in the Water and Wastewater Industries." *Public Management Review* 20 (4): 607–631. <https://doi.org/10.1080/14719037.2017.1363906>.
- SKR. 2019. *Kommunernas informationssäkerhetsarbete*. Stockholm: Sveriges kommuner och regioner.
- Sandstig, Gabriella, Max Boholm, and Johan Berlin. 2026. "Paradox of Cybersecurity? The Democratic Deficit in Municipal Work to Raise Citizens' Risk Awareness." *International Journal of Emergency Services*, <https://doi.org/10.1108/IJES-05-2025-0029>.
- Solansky, Stephanie T., and Tammy Beck. 2021. "Interorganizational Information Sharing: Collaboration During Cybersecurity Threats." *Public Administration Quarterly* 45 (1): 105–122.
- Soomro, Zahoor Ahmed, Mahmood Hussain Shah, and Javed Ahmed. 2016. "Information Security Management Needs More Holistic Approach: A Literature Review." *International Journal of Information Management* 36 (2): 215–225.

- SOU 2024:18. Nya regler om cybersäkerhet. Delbetänkande av Utredningen om genomförande av NIS2 – och CER-direktiven. [Committee Report of the Inquiry on the Implementation of the NIS2 and CER Directives]. Ministry of Justice, Sweden.
- Strebel, Michael Andrea, and Pirmin Bundi. 2023. "A Policy-Centred Approach to Inter-Municipal Cooperation." *Public Management Review* 25 (10): 1859–1880. <https://doi.org/10.1080/14719037.2022.2051065>.
- Struk, Michal, and Eduard Bakoš. 2021. "Long-Term Benefits of Intermunicipal Cooperation for Small Municipalities in Waste Management Provision." *International Journal of Environmental Research and Public Health* 18 (4): 1449.
- Tavares, Antonio F., and Richard C. Feiock. 2018. "Applying an Institutional Collective Action Framework to Investigate Intermunicipal Cooperation in Europe." *Perspectives on Public Management and Governance* 1 (4): 299–316.
- Teles, Filipe, and Pawel Swianiewicz. 2018. *Inter-Municipal Cooperation in Europe*. London: Palgrave Macmillan.
- Vestad, Arnstein, and Bian Yang. 2023. "Municipal Cybersecurity – A Neglected Research Area? A Survey of Current Research." Paper presented at the proceedings of the International Conference on Cybersecurity, Situational Awareness and Social Media, Singapore, 2023.
- Wasserfallen, Fabio. 2018. "Policy Diffusion and European Public Policy Research." In *The Palgrave Handbook of Public Administration and Management in Europe*, edited by Edoardo Ongaro and Sandra Van Thiel, 621–633. London: Palgrave Macmillan.
- Wouters, Stijn, Marijn Janssen, Veiko Lember, and Joep Crompvoets. 2023. "Strategies to Advance the Dream of Integrated Digital Public Service Delivery in Inter-organizational Collaboration Networks." *Government Information Quarterly* 40 (1): 101779. <https://doi.org/10.1016/j.giq.2022.101779>.