

THE ROLE OF CROSS-SECTORAL PARTNERSHIPS IN BUILDING FAMILY DIGITAL SECURITY: A PUBLIC AND NETWORK GOVERNANCE PERSPECTIVE

Patryk Chmielarz^{1*}, Grzegorz K. Sudol²

¹ University of the National Education Commission in Krakow,
Institute of Law, Economics and Administration, Poland

² University of the National Education Commission in Krakow,
Institute of Law, Economics and Administration,
Department of Administration and Public Management, Poland

Abstract: This article examines cross-sectoral partnerships for family digital security from the perspective of management and quality sciences. It conceptualizes cyberbullying, online grooming, identity theft, and related online harms as wicked problems that exceed the capacity of any single sector. Drawing on selected scholarship on collaborative governance, network governance, public value, stakeholder mapping, and digital safety by design, the article develops a conceptual typology of three partnership models: standard-setting partnerships, capacity-building networks, and incident-response networks. It argues that their effectiveness depends on metagovernance, the management of institutional collective-action dilemmas, and the integration of Safety by Design. The article contributes an analytical framework and stakeholder power/interest matrix for interpreting family digital resilience as a public value.

Keywords: collaborative governance, cross-sectoral partnership, digital resilience, family digital security, metagovernance, network governance, public value, Safety by Design, stakeholder management, wicked problems

JEL Classification: M14, O35, H41

¹ Patryk Chmielarz, Dr, chmielarzp13@gmail.com,  <https://orcid.org/0000-0003-0286-741X>

² Grzegorz K. Sudol, Dr, grzegorz.sudol.krakow.uken.pl,  <https://orcid.org/0000-0002-2861-5678>

* Corresponding author: Patryk Chmielarz, chmielarzp13@gmail.com

Introduction

Management and quality sciences increasingly recognize that hierarchical and market-based coordination is insufficient for complex, uncertain, and contested challenges. Rittel and Webber (1973) and Head and Alford (2015) describe such challenges as wicked problems: they lack definitive formulations, involve multiple perspectives, and resist final solutions. Family digital security fits this category because threats evolve rapidly, privacy and protection may conflict, and responsibility is dispersed across public, private, and civic actors.

The issue is empirically urgent. Recent WHO/Europe evidence documents cyberbullying among adolescents, INHOPE reports substantial volumes of suspected child sexual abuse material (CSAM) reports, and EU Kids Online documents continuing online risks despite increasing digital competences (Cosma et al., 2024; INHOPE Association, 2025; Smahel et al., 2020). Neither the state nor families can address these risks alone: the former often lags technological change, while the latter may lack specialist knowledge.

This structural inadequacy necessitates a reconfiguration of the governance architecture towards models of collaborative governance (Ansell & Gash, 2008) and network governance (Provan & Kenis, 2008). In this context, cross-sectoral partnerships integrating the resources, knowledge, and legitimacy of the public sector, the private sector (technology corporations, internet service providers), and the civic sector (non-governmental organizations, academia) become not merely an optional public policy instrument, but a structural imperative for the co-production of public value in the domain of family digital safety.

This article analyzes the role of cross-sectoral partnerships in managing family digital security. It asks how network coordination mechanisms shape family digital resilience and considers: (1) which partnership models occur in this governance architecture; (2) how stakeholder power and interest affect interventions; and (3) which metagovernance mechanisms resolve or intensify institutional collective action dilemmas.

The analysis draws on network governance, collaborative governance, stakeholder theory, public value, and digital-safety-by-design scholarship. It offers a conceptual synthesis of selected academic and policy sources and develops an analytical framework for interpreting cross-sectoral partnerships in family digital security governance.

Theoretical framework: Family cybersecurity as a wicked problem in public governance

Conceptualizing the nature of the problem

Family cybersecurity requires a management-oriented understanding of the problem. Wicked problems lack a final solution, involve competing interests, and may create new difficulties when addressed (Rittel & Webber, 1973; Head & Alford, 2015). Strict parental controls can compromise children's privacy and autonomy, whereas a laissez-faire approach increases exposure to harm. Because platforms and threat vectors change quickly, solutions must be adaptive rather than final.

The hypothesis advanced in this study is that family digital security, understood as a wicked problem, cannot be effectively managed through hierarchical (state-centric) or market-based (technology-driven) mechanisms alone, but requires the deployment of collaborative governance arrangements that integrate the complementary resources and legitimacies of multiple sectors. This hypothesis is tested through the systematic analysis of partnership models identified in the literature.

From New Public Management to New Public Governance

In response to wicked problems, New Public Governance shifts attention from internal efficiency and market mechanisms toward plural actors, inter-organizational relations, trust, and the co-production of public value (Bryson et al., 2014). This shift is pertinent to family digital security because the state needs technology firms that control digital infrastructure and civil-society organizations that maintain trusted relations with families.

Moore's (1997) strategic triangle links public value to political legitimacy, operational capacity, and social outcomes. For family digital security, governance must authorize child-protection measures, mobilize technological and educational capabilities, and demonstrate improvements in family digital resilience. A deficit in any dimension weakens the arrangement.

Network governance and forms of network management

Provan and Kenis (2008) distinguish three governance forms: shared governance, in which members coordinate collectively; lead organization governance, in which one member coordinates; and a network administrative organization (NAO), in which a separate entity governs the network. Their suitability depends on network size, trust, goal consensus, and the need for network-level competences.

In the context of family digital security, the literature reveals an evolution from dispersed, shared governance structures towards networks with a lead organization (such as a state research institute, a specialized foundation, or a regulatory agency like the Australian eSafety Commissioner), aimed at reducing transaction costs, optimizing information flow, and providing strategic direction (Yanakiev & Tagarev, 2020). This evolution reflects the increasing complexity and scale of digital threats, which demand more centralized coordination while preserving the distributed expertise of network members.

Institutional collective action dilemmas and metagovernance

A central challenge is the institutional collective action dilemma (Feiock, 2013). Platform firms pursue engagement and profit, whereas public and social actors prioritize children's well-being; this creates a structural conflict between revenue incentives and safety objectives (Senigaglia, 2022).

Metagovernance addresses this dilemma by organizing the conditions of self-organization (Jessop, 2004). A public metagovernor combines soft instruments, such as dialogue and voluntary codes, with hard instruments, such as regulation, audits, and sanctions. The Digital Services Act (DSA) illustrates this approach: Article 28 requires providers of online platforms accessible to minors to implement appropriate and

proportionate measures to ensure a high level of privacy, safety and security for minors. The DSA separately imposes risk-assessment and independent-audit obligations on very large online platforms (European Parliament and Council of the European Union, 2022, Arts. 28, 34, 37).

Toward an analytical model: synthesis of the theoretical framework

The analytical framework links three factors: the form of network governance, which shapes coordination capacity; the metagovernance regime, which structures incentives; and stakeholder power and interest, which distribute influence and commitment (Figure 1). The review uses this framework to interpret evidence on family digital security partnerships.

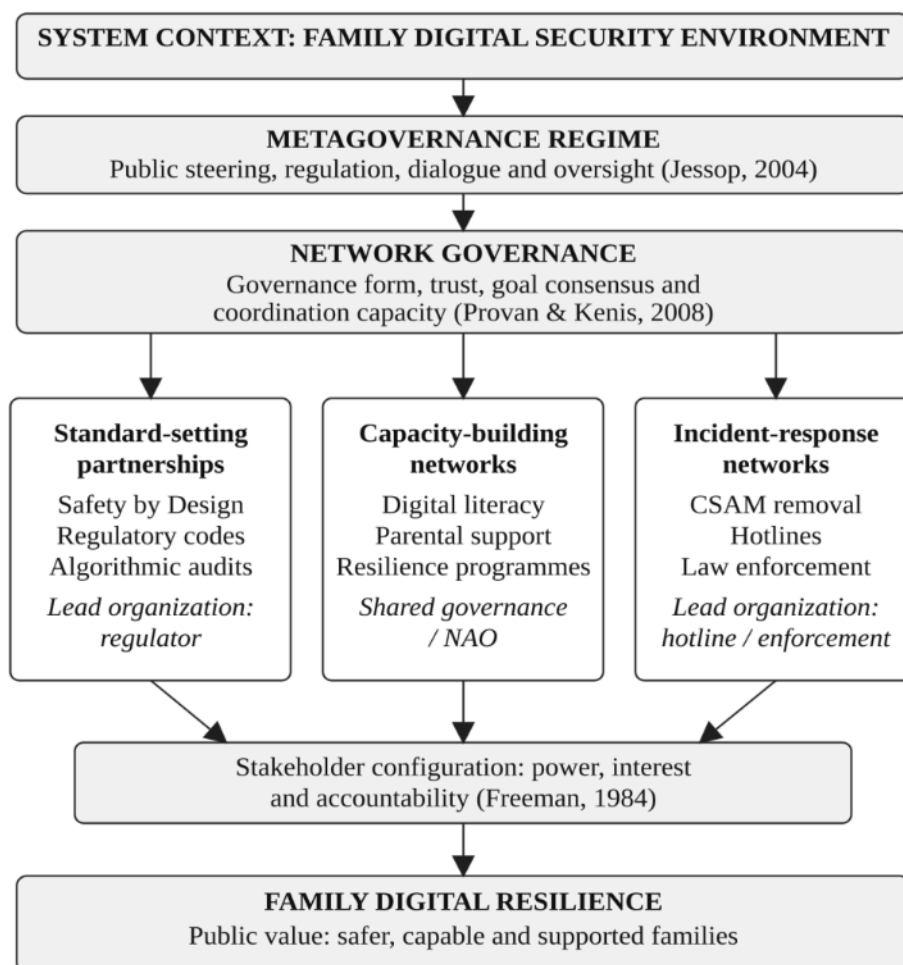


Figure 1. Analytical framework for cross-sectoral partnerships in family digital security governance

Source: Own elaboration based on Provan and Kenis (2008), Jessop (2004), Moore (1997), and Emerson et al. (2012)

Conceptual typology of cross-sectoral partnerships

This conceptual synthesis groups cross-sectoral partnerships for family digital security according to their strategic goal, degree of institutionalization, and governance form. From the perspective of strategic management, such partnerships seek to create public value by balancing political legitimacy, operational capabilities, and social value (Achard, 2019; Moore, 1997). The resulting typology distinguishes three models of cross-sectoral cooperation, each associated with a different governance logic and dimension of the family digital security challenge (Table 1).

Table 1. Conceptual typology of cross-sectoral partnership models in family digital security

Model	Strategic goal	Governance form	Key actors	Primary mechanism
Standard-setting partnerships	Norm creation and regulatory alignment	Lead organization (regulator)	Regulators, tech companies, watchdogs	Safety by Design, codes of practice
Capacity-building networks	Resilience enhancement	Shared governance / NAO	Education sector, NGOs, business	Digital literacy programs, parental mediation
Incident response networks	Threat neutralization	Lead organization (law enforcement/hotline)	Hotlines, police, platform administrators	Rapid detection, removal, prosecution

Source: Own elaboration based on Provan and Kenis (2008), eSafety Commissioner (2019), and OECD (2024)

Standard-setting partnerships

Standard-setting partnerships bring regulators, digital-service providers, and watchdogs together to develop codes and binding safety standards. They operationalize Safety by Design by embedding safeguards in products and services from the design stage rather than responding only after harm occurs (eSafety Commissioner, 2019; OECD, 2024).

Safety by Design requires risks to children to be considered throughout the lifecycle of digital services. In the context of family digital security, this supports measures such as privacy-protective default settings, age assurance, and proportionate risk assessment, subject to legal, technical, and rights-based safeguards (eSafety Commissioner, 2019; OECD, 2024). Information asymmetry remains a central managerial challenge because technology companies possess greater knowledge of their algorithms, data flows, and system architectures than regulators and civil-society organizations.

The DSA addresses this asymmetry through hard metagovernance. VLOPs must assess systemic risks and submit to independent audits, while Article 28 requires proportionate protection of minors' privacy and safety. These duties make Safety by Design more enforceable, although effective oversight still depends on regulatory capacity.

Capacity-building networks

The second model is based on the synergy of the education sector, non-governmental organizations, and business to increase the digital resilience of families. Digital resilience, defined in risk management sciences as the system's ability to absorb shocks, adapt to new conditions, and maintain functionality in the face of disruption (Dedkova et al., 2022), is the central outcome variable for prevention-oriented partnerships. These networks implement programs to raise the digital competencies of parents (including screen time management, critical evaluation of online sources, and recognition of grooming indicators) and children (including privacy management, responsible content creation, and help-seeking behaviors).

EU Kids Online documents continuing online risks despite rising digital competences (Smahel et al., 2020), while the HBSC report addresses adolescent peer violence and bullying (Cosma et al., 2024). These findings support sustained, institutionalized educational activity rather than isolated short-term projects.

Within capacity-building networks, business actors often participate as sponsors (within Corporate Social Responsibility and Environmental, Social, and Governance strategies) and providers of technological tools (e-learning platforms, parental control applications), while NGOs and scientific communities provide substantive input, didactic methodology, and trust-based access to families (Medina et al., 2020). The governance form in these networks tends toward shared governance or network administrative organizations, reflecting the relatively equal distribution of complementary resources among partners.

Incident response networks

The third model comprises highly formalized, operationally oriented risk management networks, including contact points (hotlines and helplines), law enforcement agencies (police, prosecutors), and administrators of digital platforms. Their goal is the rapid identification, isolation, and neutralization of acute threats – particularly the removal of Child Sexual Abuse Material (CSAM) and the counteraction of escalating cyberbullying situations.

Incident-response networks coordinate reporting, referral, support, and enforcement activities after harmful online events. The INHOPE Association (2025) documents the substantial operational scale of international hotline activity concerning suspected CSAM. This underlines the need for coordinated incident-response mechanisms.

Quality management in these networks requires the application of principles derived from Total Quality Management (TQM), including precise Standard Operating Procedures (SOPs) for content assessment and classification, interoperability of IT systems across jurisdictions, and rigorous Service Level Agreements (SLAs) regarding response times. The governance form in incident response networks is typically that of a lead organization (either a national hotline coordinator or a law enforcement agency), reflecting the need for rapid, authoritative decision-making in time-critical situations.

Stakeholder management and the family digital security context

The effectiveness of cross-sectoral partnerships depends directly on the quality of stakeholder engagement and the alignment of stakeholder interests with partnership objectives. Building upon Freeman's stakeholder theory and the power/interest matrix framework, the analysis of the reviewed literature reveals a complex dynamic of forces that determines the success or failure of network initiatives in the specific context of family digital security. The following stakeholder mapping (Figure 2) positions the key actors according to their level of power (capacity to influence partnership outcomes) and their level of interest (degree of concern with family digital security outcomes).

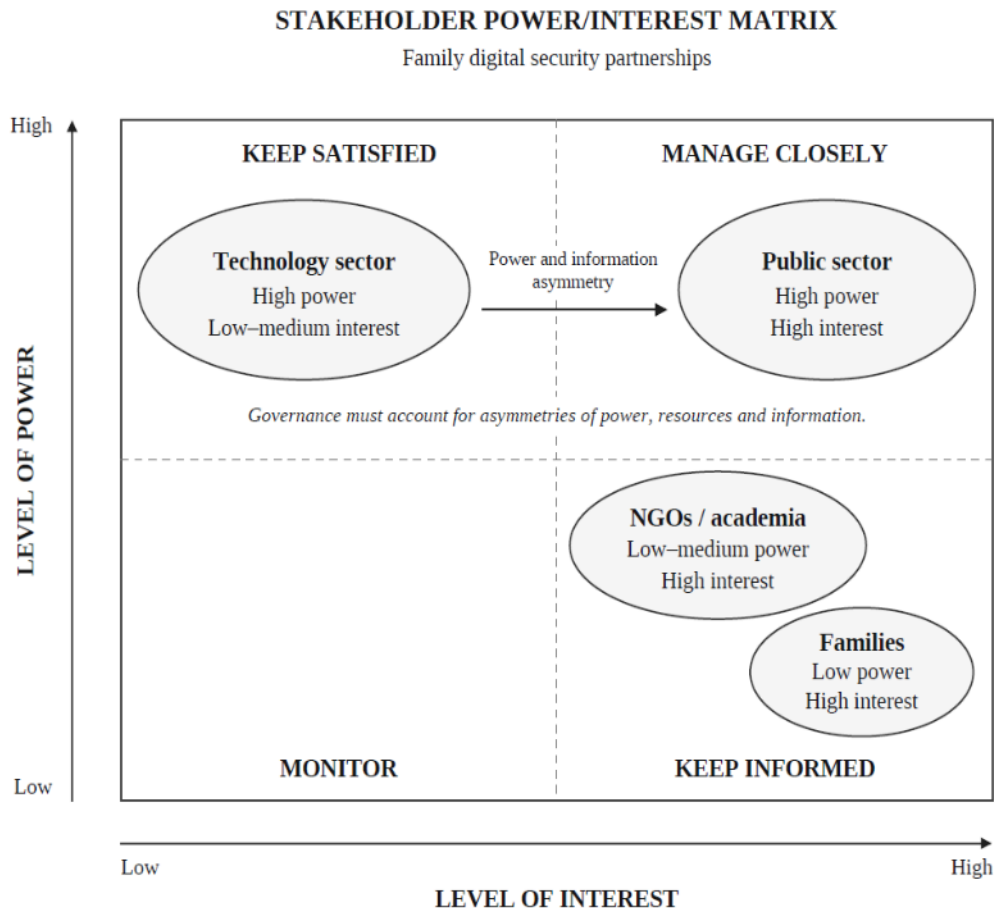


Figure 2. Stakeholder power/interest matrix for family digital security partnerships

Source: Own elaboration based on Mendelow (1991)

So it seems important to refer to the power/interest matrix of potential stakeholders when building digital safety for the family within a partnership (Table 2).

Table 2. Stakeholder power/interest matrix for family digital security partnerships

Stakeholder	Power level	Interest level	Matrix position	Partnership role
Technology Sector	High	Low-Medium	Keep satisfied	Resource provider, infrastructure controller
Public Sector	High	High	Manage closely	Metagovernor, legitimacy guarantor, funder
NGOs / Academia	Low-Medium	High	Keep informed	Knowledge broker, trust broker, lead organization
Families	Low	High	Keep informed	End beneficiary, co-producer of value

Source: Own elaboration based on Mendelow (1991)

The technology sector has high technological and financial power, but variable interest in safety, where this conflicts with engagement-based revenue models. Partnerships therefore need enforceable accountability, including transparency requirements, audits, and sanctions, rather than relying only on voluntary commitments (Vayaliparampil et al., 2021).

The Public Sector occupies the “manage closely” quadrant, combining high power (regulatory authority, funding capacity, enforcement mechanisms) with high interest (political mandate for child protection). The state acts as a metagovernor and guarantor of legitimacy, providing stable funding streams, creating legal frameworks (such as the DSA and national implementations), and auditing the effectiveness of the entire network (Tagarev & Davis, 2020). However, the public sector faces constraints including bureaucratic inertia, limited technical expertise relative to the private sector, and the challenge of maintaining regulatory relevance in a rapidly evolving technological landscape.

Non-Governmental Organizations (NGOs) and academic institutions occupy the “keep informed” quadrant in terms of formal power, but their role in family digital security partnerships often exceeds what this positioning might suggest. They act as knowledge brokers (translating research findings into actionable guidance) and trust brokers (maintaining relationships with families that government agencies and corporations cannot easily replicate). Their structural flexibility allows for faster reaction to emerging trends than bureaucratized government agencies. In network governance arrangements, NGOs frequently assume the role of a “Lead Organization,” coordinating operational activities and serving as neutral intermediaries between sectors with conflicting interests (Schütze, 2025).

Families have high interest but limited formal power. Collaborative governance should therefore treat them as co-producers of digital safety through reporting, digital-literacy participation, and peer support. Active parental mediation, based on discussion of online experience, is more effective for resilience than restriction alone (Smahel et al., 2020; Dedkova et al., 2022).

The critical implication of this stakeholder analysis for family digital security is that the most powerful actor (the technology sector) has the lowest intrinsic motivation to prioritize safety over profit, while the most interested actors (families) have the least power to effect systemic change. This structural misalignment constitutes the fundamental governance challenge that cross-sectoral partnerships must address, and it explains why metagovernance by the state, using both incentives and sanctions to realign the technology sector's behavior with public value objectives, is not merely desirable but structurally necessary.

Managerial challenges and dilemmas in the functioning of multi-sector coalitions

The practice of functioning of cross-sectoral partnerships in the area of family cybersecurity reveals a number of managerial dysfunctions that can lead to the phenomenon of “network failure” – a situation in which the collaborative arrangement fails to produce outcomes superior to what individual actors could achieve independently.

Asymmetry of resources and competencies

Public bodies and NGOs often lack IT specialists, data analysts, and algorithmic auditors, who are attracted by private-sector remuneration. This resource gap can foster regulatory capture and prevent regulators from independently verifying platform compliance claims.

Scalability and fragmentation

Educational and preventive initiatives often have a project-based, siloed, and short-term character, dependent on grant cycles and political priorities that shift with electoral calendars. The lack of institutionalized organizational memory and mechanisms for knowledge transfer between different partnerships reduces the overall efficiency of the system. From a management perspective, this fragmentation reduces the Return on Investment in public value, as lessons learned in one partnership are not systematically transferred to others, and successful pilot programs fail to scale due to the absence of sustainable funding models and institutional embedding.

Tension between innovation and security

State metagovernance must navigate the tension between imposing rigorous protective standards and stimulating the development of the digital economy. Excessively restrictive regulations risk stifling innovation and driving digital services to less regulated jurisdictions, while excessive deregulation shifts negative externalities onto the weakest and most vulnerable link in the system – the family, and particularly children within it. The OECD Recommendation on Children in the Digital Environment (2021) explicitly acknowledges this tension, calling for proportionate measures that protect children while preserving the benefits of digital participation.

Divergent performance metrics

Quality management in multi-stakeholder arrangements encounters a fundamental barrier in the form of divergent Key Performance Indicators (KPIs) across sectors. For the technology sector, success may be measured by the number of implemented safety features or content moderation actions (process indicators). For law enforcement, relevant metrics include the number of successful prosecutions or the volume of CSAM removed (output indicators). For NGOs and educational institutions, effectiveness is assessed through increases in awareness, changes in behavior, or improvements in digital literacy scores (outcome indicators). An integrated managerial approach requires the development of common outcome-based metrics that measure the actual level of family digital resilience – a composite construct encompassing knowledge, skills, attitudes, and protective behaviors – rather than sector-specific process indicators that may not correlate with genuine safety improvements.

Conclusions

From the perspective of management and quality sciences, family digital security is not merely a technological problem but a public- and network-governance challenge. Persistent online harms affecting children and families, including cyberbullying and child sexual abuse material, support moving beyond hierarchical, single-sector models of intervention toward cross-sectoral partnerships capable of mobilizing complementary resources and legitimacy.

The conceptual synthesis developed in this article supports the following theoretical and practical conclusions. They are propositions derived from the reviewed scholarship and policy sources rather than statistically generalizable findings.

First, the architecture of family digital security governance is structured around three complementary partnership models – standard-setting partnerships, capacity-building networks, and incident response networks – each employing distinct governance forms (lead organization, shared governance, and network administrative organizations, respectively) appropriate to their strategic objectives. The effectiveness of the overall governance system depends on the coherent articulation of these three models within an integrated framework, rather than their isolated operation.

Second, the effectiveness of cross-sectoral partnerships in the area of digital security is fundamentally conditioned by the state's capacity to efficiently metagovern – that is, to calibrate the system of incentives and sanctions that will prompt the private sector to move from reactive Corporate Social Responsibility gestures to a proactive Safety by Design strategy embedded in product development processes. The Digital Services Act represents a significant advance in this direction, but its effectiveness will depend on the adequacy of enforcement resources and the development of technical auditing capabilities within regulatory bodies.

Third, the stakeholder power/interest analysis reveals a structural misalignment in which the most powerful actor (the technology sector) has the lowest intrinsic motivation to prioritize family safety, while the most interested actors (families

themselves) possess the least systemic power. This misalignment constitutes the fundamental governance challenge and explains why voluntary, market-based approaches have proven insufficient, necessitating hard metagovernance instruments.

Fourth, managing digital risk in the family requires redefining the role of parents from passive recipients of educational services to active co-producers of public value. This requires providing families with accessible and ergonomic tools for digital safety management, embedding digital literacy in formal education curricula, and creating institutional channels for family participation in governance processes.

Fifth, there is an urgent need to develop integrated, cross-sectoral outcome metrics that measure the actual level of family digital resilience, rather than relying on sector-specific process indicators. The current fragmentation of performance measurement across sectors impedes accountability, hinders learning, and makes it difficult to assess the genuine impact of partnership-based interventions.

The limitations of this study should be acknowledged. As a conceptual review, the analysis is bounded by the selected academic and policy sources and does not claim to be an exhaustive systematic review. The predominance of European and Anglophone sources may limit the transferability of the framework to other cultural and regulatory contexts. The proposed analytical framework requires empirical validation through case studies or comparative analysis of specific partnership arrangements.

The direction of further research in management sciences should encompass: (1) the empirical evaluation of transaction costs associated with the functioning of cross-sectoral digital security networks; (2) longitudinal analysis of the impact of the Digital Services Act on partnership dynamics and family safety outcomes; (3) comparative studies of metagovernance approaches across different national regulatory traditions; and (4) the development and validation of composite indicators to measure family digital resilience as a public value outcome. Such research would contribute to bridging the gap between the theoretical promise of collaborative governance and the practical challenges of its implementation in the rapidly evolving domain of family digital security.

References

- Achard, P. O. (2019). Strategic management of public–private partnerships: Actors, aims, and capabilities. In R. M. Clark & S. Hakim (Eds.), *Public private partnerships: Construction, protection, and rehabilitation of critical infrastructure* (pp. 261-280). Springer. https://doi.org/10.1007/978-3-030-24600-6_13
- Ansell, C., & Gash, A. (2008). Collaborative governance in theory and practice. *Journal of Public Administration Research and Theory*, 18(4), 543-571. <https://doi.org/10.1093/jopart/mum032>
- Bryson, J. M., Crosby, B. C., & Bloomberg, L. L. (2014). Public value governance: Moving beyond traditional public administration and the new public management. *Public Administration Review*, 74(4), 445-456. <https://doi.org/10.1111/puar.12238>
- Cosma, A., Molcho, M., & Pickett, W. (2024). *A focus on adolescent peer violence and bullying in Europe, central Asia and Canada: Health Behaviour in School-aged Children international report from the 2021/2022 survey: Volume 2*. World Health Organization Regional Office for Europe. <https://iris.who.int/handle/10665/376323>

- Dedkova, L., Smahel, D., & Just, M. (2022). Digital security in families: The sources of information relate to the active mediation of internet safety and parental internet skills. *Behaviour & Information Technology*, 41(5), 1052-1064. <https://doi.org/10.1080/0144929X.2020.1851769>
- eSafety Commissioner. (2019, May). *Safety by design overview*. <https://www.esafety.gov.au/sites/default/files/2019-10/SBD%20-%20Overview%20May19.pdf>
- Emerson, K., Nabatchi, T., & Balogh, S. (2012). An integrative framework for collaborative governance. *Journal of Public Administration Research and Theory*, 22(1), 1-29. <https://doi.org/10.1093/jopart/mur011>
- European Parliament and Council of the European Union. (2022). Regulation (EU) 2022/2065 of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act). *Official Journal of the European Union*, L 277, 1-102. <https://eur-lex.europa.eu/eli/reg/2022/2065/oj>
- Feiock, R. C. (2013). The institutional collective action framework. *Policy Studies Journal*, 41(3), 397-425. <https://doi.org/10.1111/psj.12023>
- Freeman, R. E. (1984). *Strategic management: A stakeholder approach*. Pitman.
- Head, B. W., & Alford, J. (2015). Wicked problems: Implications for public policy and management. *Administration & Society*, 47(6), 711-739. <https://doi.org/10.1177/0095399713481601>
- INHOPE Association. (2025). *Annual report 2024*. <https://inhope.org/media/pages/action-awareness/publications/publications/7e41953043-1767864139/inhope-annual-report-2024.pdf>
- Jessop, B. (2004). *Multi-level governance and multi-level metagovernance: Changes in the European Union as integral moments in the transformation and reorientation of contemporary statehood*. In I. Bache & M. Flinders (Eds.), *Multi-level governance* (pp. 49-74). Oxford University Press. <https://doi.org/10.1093/0199259259.003.0004>
- Medina, A., Hernández, J. C., Muñoz-Cerón, E., & Rus-Casas, C. (2020). Identification of educational models that encourage business participation in higher education institutions. *Sustainability*, 12(20), Article 8421. <https://doi.org/10.3390/su12208421>
- Mendelow, A. (1991). Stakeholder mapping. In *Proceedings of the 2nd International Conference on Information Systems* (pp. 10-24). Prentice-Hall.
- Moore, M. H. (1997). *Creating public value: Strategic management in government*. Harvard University Press.
- OECD. (2021). *Recommendation of the Council on Children in the Digital Environment* (OECD/LEGAL/0389). OECD Legal Instruments. <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0389>
- OECD. (2024). *Towards digital safety by design for children* (OECD Digital Economy Papers No. 363). OECD Publishing. https://www.oecd.org/en/publications/towards-digital-safety-by-design-for-children_c167b650-en.html
- Provan, K. G., & Kenis, P. (2008). Modes of network governance: Structure, management, and effectiveness. *Journal of Public Administration Research and Theory*, 18(2), 229-252. <https://doi.org/10.1093/jopart/mum015>
- Rittel, H. W. J., & Webber, M. M. (1973). Dilemmas in a general theory of planning. *Policy Sciences*, 4(2), 155-169. <https://doi.org/10.1007/BF01405730>
- Schütze, H. (2025). Non-governmental organizations (NGOs) and public health. In S. R. Quah (Ed.), *International encyclopedia of public health* (3rd ed., Vol. 6, pp. 460-464). Academic Press. <https://doi.org/10.1016/B978-0-323-99967-0.00170-8>
- Senigaglia, R. (2022). Social media, mobile apps and children protection. In R. Senigaglia, C. Irti, & A. Bernes (Eds.), *Privacy and data protection in software services* (pp. 35-45). Springer. https://doi.org/10.1007/978-981-16-3049-1_4
- Smahel, D., Machackova, H., Mascheroni, G., Dedkova, L., Staksrud, E., Ólafsson, K., Livingstone, S., & Hasebrink, U. (2020). *EU Kids Online 2020: Survey results from 19 countries*. EU Kids Online, The London School of Economics and Political Science. <https://doi.org/10.21953/lse.47fdeqj01ofo>
- Tagarev, T., & Davis, B. Á. (2020). Towards the design of a cybersecurity competence network: Findings from the analysis of existing network organisations. In A. Dziech, W. Mees, & A. Czyżewski (Eds.), *Multimedia communications, services and security: MCSS 2020* (pp. 37-50). Springer. https://doi.org/10.1007/978-3-030-59000-0_4

- Vayaliparampil, M., Page, F., & Wolterstorff, E. (2021). The missing ingredient for successful multi-stakeholder partnerships: Cooperative capacity. *Societies*, 11(2), Article 37.
<https://doi.org/10.3390/soc11020037>
- Yanakiev, Y., & Tagarev, T. (2020). Governance model of a cybersecurity network: Best practices in the academic literature. In *Proceedings of the 21st International Conference on Computer Systems and Technologies* (pp. 27-34). Association for Computing Machinery.
<https://doi.org/10.1145/3407982.3407992>

Authors' Contribution: Patryk Chmielarz – 50%; Grzegorz K. Sudoł – 50%.

Acknowledgements and Financial Disclosure: The authors declare that no external funding was received for the research, authorship, or publication of this article.

Conflict of Interest: The authors declare that there is no conflict of interest.

Ethics Declaration: Ethical approval was not required for this study, as it did not involve human participants, animals, or sensitive personal data.

AI Declaration: Artificial intelligence tools were used solely to assist with the linguistic editing and translation of the manuscript into English. The authors take full responsibility for the content, scientific accuracy, interpretation, and conclusions presented in the article.

ROLA PARTNERSTWA MIĘDZYSEKTOROWEGO W BUDOWANIU CYFROWEGO BEZPIECZEŃSTWA RODZINY: PERSPEKTYWA ZARZĄDZANIA PUBLICZNEGO I SIECIOWEGO

Streszczenie: W artykule dokonano analizy roli partnerstw międzysektorowych w budowaniu cyfrowego bezpieczeństwa rodzin z perspektywy nauk o zarządzaniu i jakości. Cyberprzemoc, grooming online, kradzież tożsamości i inne szkody w środowisku cyfrowym zostały ujęte jako złożone problemy społeczne, których nie może skutecznie rozwiązać pojedynczy sektor. Opracowanie stanowi przegląd teoretyczny oparty na wybranej literaturze dotyczącej współzarządzania, zarządzania sieciowego, wartości publicznej, mapowania interesariuszy oraz Safety by Design. Autorzy proponują typologię trzech modeli współpracy: partnerstw normotwórczych, sieci budowania potencjału oraz sieci reagowania na incydenty. Wskazują, że skuteczność tych układów zależy od zdolności państwa do metazarządzania, rozwiązywania dylematów instytucjonalnego działania zbiorowego i integrowania zasad bezpieczeństwa już na etapie projektowania usług cyfrowych. W artykule przedstawiono ramy analityczne i macierz władzy/interesu interesariuszy służące interpretacji cyfrowej rezyliencji rodzin jako wartości publicznej.

Słowa kluczowe: collaborative governance, partnerstwo międzysektorowe, odporność cyfrowa, bezpieczeństwo cyfrowe rodzin, metazarządzanie, zarządzanie sieciowe, wartość publiczna, Safety by Design, zarządzanie interesariuszami, złożone problemy społeczne

Articles published in the journal are made available under Creative Commons Attribution 4.0 International.

Certain rights reserved for the Czestochowa University of Technology.

