**Literature Review**

**Title:**

**Cybersecurity Threats in IoT in the Government Sector**

**Student Name:   
Student ID:**

**Table of Contents**

[1 Introduction 2](#_Toc207983405)

[2 Thematic Literature Review 3](#_Toc207983406)

[2.1 Technical Cybersecurity Threats in IoT 3](#_Toc207983407)

[2.2 Governance, Ethics, and Professional Practice 4](#_Toc207983408)

[2.3 Research Design, Methodologies, and Data Analysis in IoT Security Studies 5](#_Toc207983409)

[3 Critical Discussion 6](#_Toc207983410)

[4 Conclusion 8](#_Toc207983411)

[5 Reference List 9](#_Toc207983412)

**Table of Figures**

[Figure 1: Structure of Cybersecurity Threats in IoT in the Government Sector (source: self-made) 3](#_Toc207787551)

# Introduction

Government systems adopting Internet of Things (IoT) technologies have revolutionised the delivery of government services within smart city infrastructures, defence, healthcare, and utilities (see Figure 1). These innovations can make governments more efficient, but they also expose them to sophisticated cyberattacks, such as ransomware, distributed denial-of-service (DDoS) attacks, and advanced persistent threats (Corrêa et al., 2023). The weaknesses of critical infrastructure undermine the national security, trust of the people and stability of their states. This topic was narrowed down by applying a rational approach, which involved a review of the emerging risks in recent studies and a creative approach, which involved the identification of tensions not well studied between national security and civil liberties. The literature search databases included IEEE Xplore, ACM Digital Library and ScienceDirect with the following keywords: IoT cybersecurity, government sector, ethics and governance, but also limited to peer-reviewed publications published after 2015. This is a review that uses both inductive reasoning (to interpret qualitative case studies) and deductive reasoning (to criticise quantitative models), which reflects the scientific method of observation, hypothesis and testing (Fjeld et al., 2020; Finn and Shilton, 2023; Biros, 2020). In line with Saunders, Lewis and Thornhill (2024), this review balances rational approaches, systematic database searches and structured thematic coding, with creative strategies such as iterative refinement of keywords and lateral thinking, ensuring both rigour and originality in framing the research.

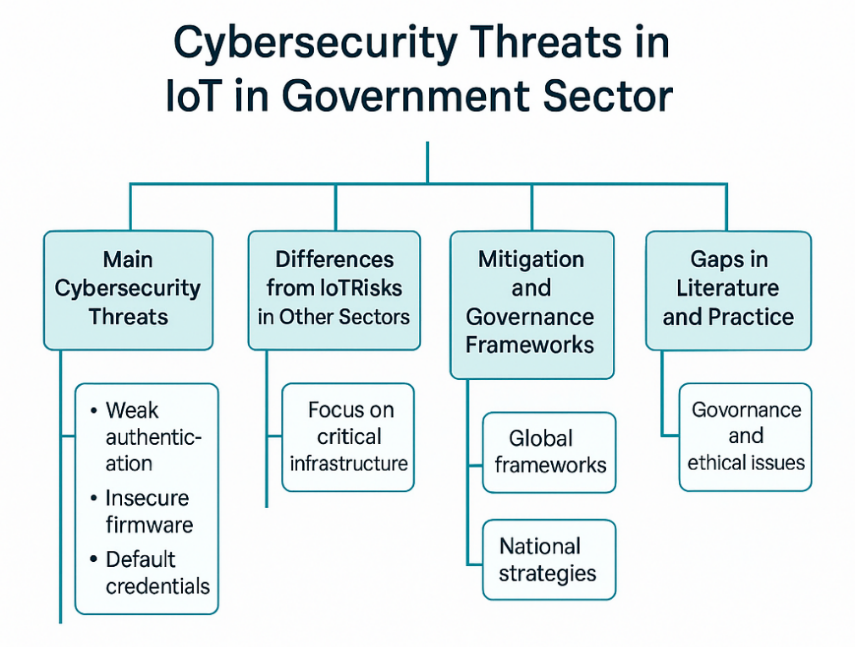


Figure 1: Structure of Cybersecurity Threats in IoT in the Government Sector (source: self-made)

# Thematic Literature Review

## Technical Cybersecurity Threats in IoT

The use of Internet of Things (IoT) technology in government systems has posed considerable technical vulnerabilities, in large part because many devices are being developed with few resources. The most common vulnerabilities are weak authentication, ineffective firmware update mechanisms, default credentials, and low encryption standards (Dawson, 2015). Although these weaknesses are an issue in any industry, their impacts in the government context are multiplied since the IoT supports important infrastructures like energy grids, transport systems, healthcare systems, and emergency response. The abuse of these vulnerabilities can have a direct impact on national security, paralyse the economies, and undermine the trust of the population (Park, 2020). DDoS attacks demonstrate this level of risk: hacked IoT devices can be turned into botnets that can bring down public systems on a regional or even national scale. Case studies have been used extensively in research on these vulnerabilities. Wohlin (2021) shows that they can be useful to map complex technical failures, and Priya (2021) underlines what kind of insights they can provide based on the context about what risks are unique to the government. However, both recognise the low level of externalisability of such results; case studies are too small to be used to develop national strategies. Such a methodological shortcoming is an indicator of a larger knowledge gap: until more descriptive and comparative system-level studies are conducted, governments themselves have no evidence base to draw upon to create resilient policy frameworks.

Recent scholarship has no longer focused on technical deficiencies but on organisational resilience. Saunders, Lewis and Thornhill (2024) make the argument that vulnerabilities cannot be completely removed but can be controlled by redundancy, layered defences and active observability. This view is consistent with a systemic approach that would expect the continued development of attacker sophistication. Conversely, Duncan (2020) states that resilience as a concept is not sufficient unless it is integrated with secure-by-design ideas in the acquisitions. The issue of resilience versus prevention, therefore, is not settled in the literature. A different dimension is brought out when we compare the public and the private sectors. IoT malfunctions in healthcare or finance can be a risk to confidentiality and consumer trust, but are institution-specific. By contrast, government IoT failures may either cripple local utilities or impair defence operations. The other paradox is that despite a rigid regulatory landscape, governments resort to commercial off-the-shelf products that are produced through international supply chains (Corrêa et al., 2023). Systemic risks of this dependency are not so clear in the corporate environment. In general, all the literature reduces to the vulnerability on the device level, but it varies in the best approach to deal with it. The resilience engineering vs. secure-by-design discussion is a subset of an even bigger issue: to achieve security of government IoT, not only technical solutions but system models to strike the right balance between prevention, flexibility, and geopolitical reality.

## Governance, Ethics, and Professional Practice

Besides technical weaknesses, the administration framework, ethical standards, and practices affect the cybersecurity of IoT in the government. The government is not the only party that is supposed to ensure the rights of the citizens, and in the process, the most vital services are provided in the healthcare, policing, and surveillance sectors (Jha and Jha, 2024). It is a duality that generates a continuous conflict between innovation and accountability. Ethical ICT research has come to be benchmarked on the Menlo Report, which describes four guiding principles: respect for persons, beneficence, justice, and respect for law and public interest (Finn and Shilton, 2023). These principles applied to government IoT imply that any system must minimise harm, distribute risks equally and seek consent where possible. But such ideals are only limitedly translated into enforceable practice. As Fjeld et al. (2020) show, although there is a general agreement about ethical standards, their application varies across jurisdictions. As Corrêa et al. (2023) also indicate, the governance policies are disjointed and are subject to the political and economic interests of a country, which creates gaps in the cross-border data streams. These gaps weaken the power of groups because their opponents can take advantage of looser regulatory mechanisms. The literature thereby recognises not only that there are standards but that standards are unequally adopted and enforced, weakening their protective effect.

Ethical concerns are even more acute in government circles since surveillance and security imperatives are rather incompatible with democratic accountability. Deckard (2023) poses crucial questions about proportionality, consent, and the loss of civil liberties in case the states take advantage of the mass surveillance facilitated by the IoT. Intrusive practices may be justified by government failures that would otherwise violate the basic right, which is not the case in a private-sector environment, where consumer trust is the main victim of contractual agreement violations. Another issue with professional codes is enforcement. The BCS Code of Conduct implies that IT practitioners should be responsible and act on behalf of the people (BCS, 2022), but, as Dawson (2015) remarks, the ideal and the real are always at a distance. The codes of ethics will always be symbolic unless there are aspects of accountability, such as oversight bodies or other forms of control. Lastly, government IoT governance and ethics are prescriptive rather than definitive. To some extent, they offer a sense of direction, although they do not address the tensions between national security requirements and civil liberties. This opposition is not yet crushed, and governments are elevated to the same plane as the protectors of online security and the potential offenders of citizen rights.

## Research Design, Methodologies, and Data Analysis in IoT Security Studies

The existing literature about IoT cybersecurity in the government utilises a variety of different methodological frameworks, each with its own advantages and disadvantages. Yogar and Sabarna (2025) also highlight that the existing designs are not commensurate with the complexity of the interconnected IoT ecosystems and their implications for national security. Most of the evidence is based on case studies that are useful in investigating contextual information about breaches or vulnerabilities. Wohlin (2021) demonstrates that case studies are useful in the research of software engineering, and Priya (2021) suggests that they can reveal socio-technical dynamics in the use of IoT by governments. However, the results of case studies are local and lack external validity, which introduces reliability and generalisability concerns to larger national infrastructures. Another handy differentiation in the literature is between exploratory and descriptive designs. Exploratory research, generally qualitative, finds emerging weaknesses but not prevalence or severity. Descriptive techniques, on the other hand, use surveys, statistical models or simulations to characterise trends across systems. Descriptive, generalisable research, however, does not exist in large quantities, and so policy-making is constrained in the evidence it can provide. This is a methodological asymmetry: exploratory research is inductive in its arguments, where theory is built by observing data, and descriptive and statistical research is deductive in its arguments, where theory is tested against data (Saunders, Lewis and Thornhill, 2024). A lack of one or the other will push the field in either of the two directions of either deep but imprecise insights or general but shallow generalisations.

Most of the government IoT security research is based on qualitative studies of interviews and reports, as these provide descriptive insights with a low degree of reliability and reproducibility. However, even though statistical methods, such as hypothesis testing and inferential modelling (Berenson et al., 2019), are more effective in strengthening rigour, they do not generalise. Mixed-methods research provides the answer, as it provides the depth of qualitative and the generalisability of quantitative methods (Ahmad and Yunos, 2012), but it is not actively used. This kind of unbalanced approach to methodology creates fragmented evidence, which sabotages policymaking. More importantly, this reflection points to the necessity of methodological pluralism and is reflected in the Unit 2 process of transforming general research ideas into viable, ethical and well-crafted proposals.

# Critical Discussion

The body of knowledge regarding IoT cybersecurity in government is rich, but uneven, with shared themes but methodological and conceptual gaps. Technically, there is no limit to the risks that researchers can find at the device level, including a flawed authentication system, insecure firmware, and default credentials (Dawson, 2015). It is this convergence that highlights the critical nature of dealing with design flaws, but the scope of the analysis of these risks is quite different. The number of case studies with contextual information on breaches is large (Wohlin, 2021; Priya, 2021), but the small scale restricts the generalisation potential and the applicability of national policies. On the other hand, descriptive surveys and threat catalogues offer a larger coverage, but fail to represent systemic resilience and therefore have less power to explain. Such disproportionality may be observed in the example of the Mirai botnet attack because people concentrated on the technical malfunctions of the time and not structural lessons on resiliency and prevention (Carr, 2017).

The same tendency of partial coverage is observed in ethical and governance frameworks. Normative frameworks propagate concepts of beneficence, justice, and accountability of Menlo Report, and AI ethics, but are not necessarily applied in practice (Finnand Shilton, 2023; Fjeld et al., 2020). Corrêa et al. (2023) show that fragmentation across jurisdictions creates regulatory loopholes, and Deckard (2023) points to the unresolved paradox that governments are the very ones that protect digital security and, at the same time, can be the most dangerous with regard to civil liberties through mass surveillance. Ethical ideals, therefore, offer a narrative to follow, but they are not enforceable when the national security imperative is in the spotlight.

The literature is characterised by a qualitative and quantitative gap methodologically. Qualitative research is best at identifying new risks and contextual influences but has poor reliability and generalisability. Statistical modelling and hypothesis testing can enhance validity and replicability, but not the enrichment of the context (Berenson et al., 2019). Saunders, Lewis and Thornhill (2024) endorse these restrictions, but methodological pluralism is the sole exception, although mixed-methods studies can address these restrictions through the concept of triangulation (Ahmad and Yunos, 2012). Taken together, the literature shows that integration is needed on technical, ethical and methodological levels. Good research not only needs to list threats but also evaluate governance structures and test resilience measures in terms of qualitative richness and quantitative rigour. Such synthesis is the only way evidence-based approaches can strike the fine balance between national security vulnerability and civil liberties. To avoid a purely descriptive survey, this review follows Dawson’s (2015) guidance on critical evaluation, explicitly contrasting methodologies, highlighting contradictions across studies, and identifying gaps that warrant future research.

# Conclusion

The literature confirms that government IoT systems have systemic technical vulnerabilities, including insecure firmware, default credentials, and are susceptible to DDoS attacks (RQ1) and have higher risks than those associated with the private sector because of their national and geopolitical impact (RQ2). Ethical codes and governance frameworks, including the Menlo Report and AI principles, are the rules that remain incomplete and are not always implemented (RQ3). Qualitative case studies used as a methodology have restricted the generalisability of the results, and quantitative methods are not well utilised, creating gaps in validity and reliability (RQ4). The emerging line of study should employ mixed methods, focus on secure-by-design procurement, and integrate ethical governance with resilience engineering in attaining the middle ground between security and civil liberties. These research questions were not generated arbitrarily but refined through a systematic narrowing process from Unit 1 topics, using Unit 2 guide questions to ensure relevance, feasibility, and ethical alignment, reflecting the structured logic of an early research proposal.

# ****Reference List****

Ahmad, R. and Yunos, Z., 2012. The application of mixed methods in developing a cyber terrorism framework. *Journal of Information Security*, *3*(3), pp.209-214.

BCS, 2022. *BCS Code of Conduct | BCS*. www.bcs.org. Available at: https://www.bcs.org/membership-and-registrations/become-a-member/bcs-code-of-conduct/.

Berenson, M.L., Levine, D.M., Szabat, K.A. and Stephan, D.F., 2019. *Basic business statistics: Concepts and applications*. Pearson.

Biros, D., 2020. The challenges of new information technology on security, privacy and ethics. *Journal of the Midwest Association for Information Systems (JMWAIS)*, *2020*(2), p.1.

Carr, M., 2017. The Role of Transnational Expert Associations in Governing the Cybersecurity Risks of the Internet of Things.

Corrêa, N.K., Galvão, C., Santos, J.W., Del Pino, C., Pinto, E.P., Barbosa, C., Massmann, D., Mambrini, R., Galvão, L., Terem, E. and de Oliveira, N., 2023. Worldwide AI ethics: A review of 200 guidelines and recommendations for AI governance. *Patterns*, *4*(10).

Dawson, C., 2015. Projects in Computing and Information Systems 3rd edn: A Student's Guide.

Deckard, R., 2023. *What are ethics in AI? | BCS*. www.bcs.org. Available at: https://www.bcs.org/articles-opinion-and-research/what-are-ethics-in-ai/.

Duncan, R., 2020. What does ‘secure by design’actually mean?. *Network Security*, *2020*(8), pp.18-19.

Finn, M. and Shilton, K., 2023. Ethics governance development: The case of the Menlo Report. *Social Studies of Science*, *53*(3), pp.315-340.

Fjeld, J., Achten, N., Hilligoss, H., Nagy, A. and Srikumar, M., 2020. Principled artificial intelligence: Mapping consensus in ethical and rights-based approaches to principles for AI. *Berkman Klein Center Research Publication*, (2020-1).

Jha, R.K. and Jha, M., 2024. Optimizing E-Government Cybersecurity through Artificial Intelligence Integration. *Journal of Trends in Computer Science and Smart Technology*, *6*(1), pp.67-87.

Park, Y., 2020. Development and Evaluation of a Security Agent for Internet of Things.

Priya, A., 2021. Case study methodology of qualitative research: Key attributes and navigating the conundrums in its application. *Sociological Bulletin*, *70*(1), pp.94-110.

Saunders, M.N., Lewis, P. and Thornhill, A., 2024. Research Methods for Business Students.

Wohlin, C., 2021. Case Study Research in Software Engineering—It is a Case, and it is a Study, but is it a Case Study?. *Information and Software Technology*, *133*, p.106514.

Yogar, B.N.A. and Sabarna, M.A.N., 2025. Bibliometric Analysis of Research Trends in Data Security and Privacy for E-Government Implementation in Indonesia. *Agile Governance and Innovation Measurement Journal*, *2*(1), pp.15-25.