

Bridging Cybersecurity and Counterterrorism through Institutional Coupling and Interagency Governance in the Public Sector

Nadiah Khaeriah Kadir¹

¹ Universitas Hasanuddin, Indonesia

Correspondence: nadiahkhaeriah@unhas.ac.id

Article Info

Article History:

Received Aug 15th, 2026

Revised Aug 21th, 2026

Accepted Aug 30th, 2026

Keyword:

Counterterrorism; Cybersecurity;

Cyberterrorism; Institutional

coupling; Public sector.

ABSTRACT

This study examined how governments formally connected cybersecurity and counterterrorism when a security problem crossed both policy domains. A comparative qualitative document analysis was conducted on national laws, strategies, crisis plans, and institutional mandates from Indonesia, Australia, and the United Kingdom that were operative by 2026. The analysis focused on institutional mandates, the division of authority, formal coordination mechanisms, and information or incident coordination. The findings showed that cybersecurity and counterterrorism remained administratively distinct in all three systems, although the points of connection differed. Indonesia relied on separate lead institutions with selective formal bridging. Australia provided a more explicit interface through national counterterrorism and cyber response arrangements. The United Kingdom connected the fields through shared national security institutions, particularly GCHQ and the National Cyber Security Centre. The study concluded that institutional coupling offered a useful way to compare formal cross-domain governance without treating documentary arrangements as evidence of operational effectiveness.



© 2026 The Authors. Published by Punggawa Legacy Center. This is an open access article under the CC BY license (<https://creativecommons.org/licenses/by/4.0/>)

INTRODUCTION

Cybersecurity and counterterrorism are usually administered through different parts of government even when the same incident can engage both fields. A disruptive intrusion into critical infrastructure may begin as a technical cyber incident, then acquire evidence of political violence or terrorist intent. Responsibility can then move across cyber agencies, intelligence bodies, police, crisis managers, and counterterrorism authorities. The administrative problem is not unusual in public policy. Specialization creates expertise, but it also creates boundaries that must be crossed when a threat does not fit neatly within one mandate. Cybersecurity makes this problem especially visible because digital incidents often develop before their legal and security meaning is settled. That uncertainty over classification is also an uncertainty over public authority.

Cyberterrorism research has spent considerable effort on definition, threat credibility, and the distinction between terrorist use of the internet and attacks conducted through cyber means. Jarvis and Macdonald (2015) show how disagreement over the concept persists among researchers. Jarvis, Macdonald, and Nouri (2014) reach a similar conclusion when examining perceptions of the threat. Later work has widened the discussion to national policy and international diplomacy, where broad cyberterrorism language can blur terrorism, information security, and political control (Broeders et al., 2023). These debates remain necessary, but they do not tell us much about how public institutions divide responsibility once cyber and terrorism concerns overlap. The migration of terrorist communication and support activity into anonymous and encrypted digital environments further complicates that boundary because operational practices can move across platforms without fitting neatly into one technical or legal category (Mappaselleng et al., 2025).

Governmental cybersecurity has also become less intelligible as a purely technical function. Public agencies now operate within networks of regulators, intelligence services, police, critical infrastructure operators, and private providers. Boeke (2018) shows that national cyber crisis systems differ in where coordination is located and whether cyber capacity is concentrated or distributed. Chaudhary et al. (2018) describe a related coordination problem created by organizational boundaries in cyber response. More recent work treats institutional design itself as part of cyber crisis governance rather than as background administration. Kianpour and Frantz (2025), for example, examine how authority and coordination are distributed within the European Union cyber crisis framework. The institutional location of coordination can therefore shape which actors meet before a crisis escalates. Adaptive governance research reaches a similar conclusion for emerging security risks (Brass & Sowell, 2021). Related work on digital identity crime also shows how new digital environments can expose gaps in existing criminal policy and create pressure for cross-border and multi-actor responses rather than a purely domestic legal solution (Kadir, 2025).

Public-sector research points in the same direction. Information security governance depends on more than technical controls when responsibility is spread across public organizations (Magnusson et al., 2025). Cybersecurity policy is also becoming more cross-sectoral and whole-of-government in character (Cotta & Righettini, 2026). Regulatory studies show that cyber rules can reshape existing governance relationships rather than merely add technical requirements (Michalec et al., 2022). Governments must therefore decide who acts, who coordinates, and how information moves when several administrative communities hold only part of the relevant authority.

Public administration provides a useful but deliberately limited frame for this problem. Interagency coordination concerns the management of interdependent work across organizations that retain their own authority and expertise. Agranoff and McGuire (2001) place such interdependence at the center of public network management. Christensen and Lægreid (2007) likewise show why whole-of-government arrangements emerge when specialization produces fragmentation. Network governance does not require organizational merger. Different arrangements can connect actors through a lead organization, a coordinating body, or shared structures while leaving core mandates intact (Provan & Kenis, 2008). That distinction matters in security policy, where legal powers and operational roles cannot simply be pooled.

Institutional coupling is used here as a modest analytical lens rather than a new theory or an index of state capacity. It refers to the formal connections that allow separately mandated cybersecurity and counterterrorism institutions to allocate authority, coordinate, and exchange information when their responsibilities intersect. The concept directs attention to the connection between domains without assuming that tighter integration is inherently better. A clear interface may coexist with specialized agencies. A more fragmented architecture may also contain working relationships that are not visible in public documents. The concern is therefore the formal design that governments place on the public record, not the quality of cooperation behind it. This keeps the lens close to arrangements that can actually be observed and compared.

Indonesia, Australia, and the United Kingdom provide useful variation in a small comparative design. All three have national cybersecurity and counterterrorism frameworks, but the domains are connected differently. Indonesia relies on separate national bodies. Australia places important cyber and counterterrorism coordination functions within Home Affairs and national crisis arrangements. The United Kingdom links cyber security to the wider intelligence system through GCHQ and the NCSC. The cases permit comparison of institutional connection without ranking national capability.

The study asks how cybersecurity and counterterrorism responsibilities are formally organized in the three governmental systems and how interagency arrangements connect them when a threat crosses the two policy domains. The contribution is narrow by design. Existing work explains cyber threats, cyber governance, and coordination within security systems. Less comparative attention has been given to the formal bridge between cybersecurity and counterterrorism as established fields of public authority. Treating cyberterrorism as an institutional coordination problem makes that bridge visible and keeps the claim close to evidence that can be observed in laws, strategies, plans, and official mandates.

RESEARCH METHODS

A comparative qualitative document analysis was used because the object of inquiry is formal governmental design. Laws, national strategies, crisis plans, and institutional mandates record how governments assign authority and describe official coordination. Document analysis is well suited to questions of this kind when claims remain tied to what documents can establish (Bowen, 2009). The study does not measure effectiveness, reconstruct confidential practice, or test causal relationships. It compares the public architecture through which cybersecurity and counterterrorism responsibilities are formally connected.

Indonesia, Australia, and the United Kingdom were selected purposively. Each case has a developed national cybersecurity framework, an identifiable counterterrorism framework, and public documents that specify institutional responsibilities. They also provide enough administrative variation to make comparison useful. The cases are not treated as representative of all governmental systems. Their purpose is more limited. They allow the same institutional questions to be asked across three settings without expanding the study into a broad cross-national assessment that the documentary evidence could not support.

The empirical material consists of national-level documents that were in force or publicly operative by 2026 and that directly define institutional mandates, cybersecurity or counterterrorism policy, or formal coordination arrangements. Indonesian sources include Presidential Regulations 28 of 2021 and 47 of 2023, Presidential Regulations 8 and 9 of 2026, and BNPT Regulation 1 of 2026. Australian sources include the 2023 to 2030 Cyber Security Strategy, the 2024 National Counter-Terrorism Plan, the 2025 counterterrorism strategy, the 2025 Australian Cyber Response Plan, and the 2026 Horizon 2 Action Plan. The United Kingdom corpus centers on the National Cyber Strategy 2022 and CONTEST 2023. These documents were chosen because they directly define the arrangements examined rather than merely discuss cyber threats.

Relevant passages were read against four analytical dimensions. Institutional mandate captures where cybersecurity and counterterrorism responsibilities sit. Division of authority examines whether those responsibilities remain separate or are connected at particular points. Formal coordination covers standing bodies, lead agencies, and cross-government arrangements. Information sharing and incident coordination concern the formal routes through which security information or crisis responsibility can move. The material was entered into a case matrix and compared across these dimensions. Peer-reviewed literature was used to place the findings within research on cyber governance and interagency coordination, but it was not coded as a second empirical dataset.

Public documents reveal formal design, not the full behavior of institutions. A written coordination mechanism does not show how quickly agencies cooperate, how much intelligence they exchange, or whether officials trust one another. Informal practice may also be stronger than the published architecture suggests. Claims are therefore confined to mandate allocation, visible coordination arrangements, and points where responsibility is formally connected or remains separate. Questions about operational performance would require interviews, exercise records, after-action reports, or incident-level evidence that is not used in this study.

RESULTS AND DISCUSSION

Separate Domains with Different Points of Connection

Cybersecurity and counterterrorism remain distinct administrative domains in all three cases. None has merged the two into a single institutional chain. Cyber agencies retain technical, resilience, incident response, or intelligence functions, while counterterrorism systems retain prevention, investigation, disruption, and crisis responsibilities. The important variation lies in where the connection appears. Indonesia shows the clearest separation between lead institutions. Australia makes the connection visible inside national planning and crisis arrangements. The United Kingdom connects the fields through institutions that sit inside the wider national security system. Institutional coupling therefore appears as a relationship between specialized structures rather than the disappearance of specialization.

Indonesia has strengthened both domains without placing them under one lead authority. Presidential Regulation 28 of 2021 assigns national cyber and cryptographic responsibilities to BSSN. Presidential Regulation 47 of 2023 adds a national cyber security strategy and a cyber crisis management framework for state institutions and relevant stakeholders. Counterterrorism is centered

on BNPT under Presidential Regulation 9 of 2026. The 2026 regulation updates BNPT's organizational basis and confirms a coordinating role in counterterrorism. BNPT Regulation 1 of 2026 also formalizes coordination among investigators, prosecutors, corrections personnel, and supporting institutions in terrorism cases. The two policy fields are therefore institutionally substantial on their own terms. The formal architecture is clearer within each field than across the boundary between them.

What is less visible in the Indonesian corpus is a standing cross-domain mechanism that specifically links BSSN and BNPT for a cyber incident with a terrorism dimension. That observation is narrower than claiming an absence of cooperation. Whole-of-government principles and agency mandates can support contact, while operational or classified arrangements may exist outside the documents examined here. Indonesian scholarship has already noted legal ambiguity and institutional overlap in cyberterrorism governance (Siddha & Benarrivo, 2023). Utomo et al. (2025) also identify coordination as a continuing issue. The documentary comparison locates the issue more precisely in the public interface between two otherwise developed institutional systems.

Australia makes that interface easier to observe. The 2024 National Counter-Terrorism Plan contains a specific cyber security section and places cyber coordination inside a wider counterterrorism planning document. It identifies Home Affairs, the Australian Cyber Security Centre, the National Office of Cyber Security, and other agencies as part of the relevant arrangements. The 2023 to 2030 Cyber Security Strategy separately established a stronger national cyber coordination architecture. Horizon 2, launched in June 2026, continues this whole-of-nation approach rather than replacing the institutional framework created under the first horizon.

The 2025 Australian Cyber Response Plan adds an important qualification. AUSCYBERPLAN governs strategic coordination for cyber incidents categorized as crises under the Australian Government Crisis Management Framework. It also recognizes that terrorist incidents have their own National Counter-Terrorism Plan. The same Department of Home Affairs has coordinating responsibilities across these hazard arrangements, but the plans do not collapse into one another. Australia therefore offers a clear example of connection without merger. Cross-domain responsibility is supported by common crisis architecture and a shared departmental location, while different incident types retain their own national plans.

The United Kingdom uses another route. The National Cyber Strategy places the National Cyber Security Centre within GCHQ and assigns it national technical and incident responsibilities. CONTEST 2023 identifies GCHQ as a core security actor and describes the NCSC as the cyber security part of GCHQ. Counterterrorism remains led by the Home Secretary and the Home Office, with Counter Terrorism Policing and MI5 holding distinct roles. GCHQ and the NCSC therefore create an identifiable institutional connection between the cyber and counterterrorism architectures without becoming the single authority for both.

Administrative location differs across the three systems. Indonesia retains separate lead bodies and relies mainly on broader interagency links. Australia places several coordinating functions within Home Affairs and connects the domains through national plans and crisis arrangements. The United Kingdom relies more on a shared intelligence and national security node. Similar functional needs are therefore handled through different structures, which accords with research showing that cyber crisis governance can operate through several network forms rather than one preferred model (Boeke, 2018).

Table 1 Comparative Institutional Architecture of Cybersecurity and Counterterrorism Governance

Dimension	Indonesia	Australia	United Kingdom
Main cyber authority	BSSN under Presidential Regulation 28 of 2021, supported by the national cyber security and crisis framework in Presidential Regulation 47 of 2023	National Cyber Security Coordinator and National Office of Cyber Security in Home Affairs, alongside ACSC and ASD	NCSC within GCHQ, with cross-government responsibilities set out in the National Cyber Strategy
Main counterterrorism authority	BNPT under Presidential Regulation 9 of 2026, with law enforcement coordination supported by BNPT Regulation 1 of 2026	Home Affairs and the Counter-Terrorism Coordination Centre, ANZCTC, AFP, ASIO, and state and territory partners	Home Office and the Home Secretary, with Counter Terrorism Policing, MI5, GCHQ, and other national security partners
Division of authority	Cybersecurity and counterterrorism remain under separate lead institutions	Cyber and counterterrorism retain distinct operational mandates within linked federal and crisis arrangements	Cyber and counterterrorism retain distinct operational chains within an overlapping national security architecture

Dimension	Indonesia	Australia	United Kingdom
Formal coordination	BSSN centered cyber coordination and BNPT centered terrorism coordination	National Cyber Security Coordinator, ANZCTC, National Counter-Terrorism Plan, and AUCYBERPLAN	Cross-government cyber leadership and Home Office counterterrorism coordination, with GCHQ and NCSC present in the wider security system
Cross-domain interface	Visible mainly through broader interagency principles and mandates rather than a dedicated public BSSN and BNPT mechanism	Visible through Home Affairs, the cyber section of the National Counter-Terrorism Plan, and linked national crisis plans	Visible through GCHQ and NCSC across cyber and counterterrorism strategy while specialist operational roles remain separate

Sources. Government of Indonesia 2021, 2023, 2026a, 2026b. BNPT 2026. Australian Government 2023, 2024, 2025a, 2025b, 2026. UK Government 2022. UK Home Office 2023.

Authority when an Incident Changes Institutional Meaning

A cyber incident does not enter government with a stable administrative label. Technical responders may initially know that systems have been disrupted without knowing whether the actor is criminal, state-linked, ideological, or terrorist. Lewallen (2021) shows how emerging technologies can create uncertainty over problem definition and policy authority. That uncertainty is especially relevant here. The institutional question is not only who has cyber authority and who has counterterrorism authority. It is how the governmental system handles the point at which new information changes the meaning of the incident and activates another set of legal or security responsibilities. A system can be well prepared inside each domain and still leave the transition between them less explicit.

Australia makes this transition most explicit in the reviewed public material. AUCYBERPLAN states that it applies to qualifying cyber incidents regardless of malicious intent or origin, while terrorist incidents are governed by the National Counter-Terrorism Plan. This separates initial cyber coordination from later threat classification without leaving both processes institutionally unrelated. Home Affairs remains an important coordinating location and the counterterrorism plan itself recognizes cyber security responsibilities. The arrangement is not proof of seamless handover in practice. It does, however, show that the public architecture anticipates more than one hazard framework and specifies where those frameworks sit.

The Indonesian documents describe strong domain-specific responsibilities but provide less detail on this kind of transition. BSSN has a national role in cyber security and crisis management. BNPT has national counterterrorism and coordination functions. Yet the reviewed instruments say more about coordination inside each domain than about the formal movement of a cyber incident into a terrorism process. That gap in documentary specificity should not be converted into a claim about weak operational coordination. It means only that the cross-domain handover is less visible in the public rules and strategies selected for this study.

British documents make the transition legible through overlapping national security institutions rather than a single cross-domain plan. The NCSC can manage nationally significant cyber incidents and draw on GCHQ's wider intelligence position. CONTEST places GCHQ within the counterterrorism system while leaving investigation and domestic counterterrorism leadership with other bodies. A cyber incident that acquires a terrorism dimension can therefore encounter institutions already present in both architectures. The documents do not reveal the operational threshold for that change in classification. They do show that the cyber and counterterrorism systems are not institutionally strangers to one another.

Coordination without Claims of Effectiveness

Formal coordination appears in every case, but its documentary form differs. Indonesia relies on BSSN and BNPT as strong domain anchors and formalizes coordination within each field. Australia uses standing federal arrangements, a national cyber coordinator, the Australia-New Zealand Counter-Terrorism Committee, and linked crisis plans. The United Kingdom uses cross-government cyber leadership alongside Home Office counterterrorism coordination and the intelligence position of GCHQ. Table 1 records these arrangements without assigning a score. A score would imply a measurement model that the documents cannot justify and would turn descriptive differences into unsupported claims about institutional quality.

Information sharing requires the same restraint. Emergency governance research has long shown that interagency communication and boundary-spanning relationships matter during complex events (Kapucu, 2006). Multiplex networks can also connect agencies through more than one type of relationship (Kapucu & Hu, 2016). Counterterrorism research reaches a similar conclusion because

intelligence, policing, and emergency functions depend on coordination across organizations (Strom & Eyerman, 2007). Cyberterrorism exercises have likewise shown the organizational importance of interagency collaboration (Solansky & Beck, 2009). None of that literature permits a public strategy document to stand in for observed information flow. The present study therefore treats information-sharing provisions as institutional design only.

That distinction matters for Indonesia in particular. Existing cyberterrorism studies have raised concerns about fragmented authority, legal uncertainty, and the relationship among BSSN, BNPT, police, and other institutions (Setiawan, 2020). Masyhar et al. (2023) emphasize the additional complications created by international cooperation. The official documents used here support a narrower finding. Indonesia has increasingly formalized cybersecurity governance and counterterrorism coordination, but their public cross-domain interface is less explicit than the connections visible in Australia or through the British GCHQ and NCSC structure. The evidence does not support a claim that Indonesian agencies cooperate less effectively in real incidents.

Cybersecurity governance extends beyond security agencies. Carr (2016) shows how national cyber strategies depend on public and private relationships around critical infrastructure. Savaş and Karataş (2022) describe cyber governance as spanning several institutional levels, while Hossain et al. (2025) identify organizational constraints in local-government cybersecurity. Huang et al. (2021) show that cyber risk governance can cross state, corporate, and national boundaries. These relationships are not the focus here, but they place the cybersecurity and counterterrorism interface inside a larger governance environment.

What Institutional Coupling Adds to the Cyberterrorism Debate

Cyberterrorism becomes analytically different when the unit of attention moves from the attacker to the state. Definitions remain contested and the empirical frequency of high-impact cyberterrorism remains difficult to establish. Yet governments cannot postpone institutional allocation until conceptual disputes disappear. A serious cyber incident may require technical response before intent is known, and terrorism authorities may become relevant only after intelligence or investigative information develops. Institutional coupling captures this administrative condition. It asks whether the governmental architecture contains recognizable routes between policy domains that were designed around different problems. A similar difficulty appears in criminological explanation more broadly, where concepts developed around offline offending do not always transfer cleanly to new digital settings (Kadir, 2026). The institutional problem examined here follows the same logic because administrative mandates built for separate policy fields must still operate when the threat crosses both.

The three cases do not form a hierarchy. A more visible connection is not automatically a better one. Tight integration can blur legal responsibility, while separation can preserve expertise and accountability. Public management research has long treated coordination as a problem of managing interdependence rather than eliminating organizational boundaries (Agranoff & McGuire, 2001). Provan and Kenis (2008) likewise show that network governance can be organized in different ways. The comparative findings fit that view. Governments can connect cybersecurity and counterterrorism through common departments, shared national security institutions, linked plans, or broader interagency mechanisms without producing a single administrative model.

Recent cybersecurity governance research reinforces this reading. Magnusson et al. (2025) identify governance and organizational issues as persistent public-sector security concerns. Kianpour and Frantz (2025) show how cyber crisis arrangements distribute authority across multiple centers rather than relying on a simple hierarchy. Cotta and Righettini (2026) find that cybersecurity increasingly requires coordinated policy mixes across sectors and government functions. These studies do not address the same empirical question as the present article. They nevertheless help explain why a cyberterrorism problem can be institutionally important even when the research design does not measure attacks. The object is the governmental arrangement that must handle an uncertain cross-domain event. The shared concern is institutional coordination under conditions that do not fit a single administrative silo.

Table 2 summarizes the observed patterns in qualitative terms. Indonesia is best described as having parallel domain structures with selective formal bridging. Australia shows a more explicit connection through Home Affairs, national plans, and crisis coordination. The United Kingdom connects the domains through shared national security institutions while maintaining separate operational responsibilities. These labels are descriptive shorthand only. They do not constitute a

typology with fixed categories, and they should not be read as levels of maturity. Their value is practical. They make differences in the location of formal connection easier to compare without pretending that documentary evidence can establish performance.

Table 2 Cross-Case Patterns of Institutional Coupling

Analytical question	Indonesia	Australia	United Kingdom	Cross-case reading
Where does connection occur	Between separate domain institutions through broader government coordination	Within Home Affairs, federal coordination, and linked national plans	Through shared national security and intelligence institutions	The connection can sit at different administrative points
How is authority preserved	Separate lead bodies remain visible	Separate plans and operational mandates remain in place	Cyber, police, intelligence, and Home Office roles remain differentiated	Coupling does not require merger
How visible is incident transition	Less directly specified in the reviewed public instruments	More directly anticipated through different hazard plans and common coordination	Visible through institutional overlap, although operational thresholds are not public	Transition between policy domains is a central governance issue
Descriptive pattern	Parallel domain structures with selective bridging	Explicit cross-domain connection through plans and coordination	Shared national security nodes with specialized roles	Descriptive differences only, not maturity levels

CONCLUSION

Cybersecurity and counterterrorism remain separate fields of public authority in Indonesia, Australia, and the United Kingdom, but they are not institutionally isolated. Indonesia has distinct BSSN and BNPT centered structures and increasingly formal coordination within each domain. Australia connects the fields more visibly through Home Affairs, the National Counter-Terrorism Plan, cyber coordination arrangements, and AUSCYBERPLAN. The United Kingdom relies on shared national security institutions, particularly GCHQ and the NCSC, while keeping counterterrorism leadership and operational responsibilities differentiated. The comparison therefore finds different locations of institutional connection rather than different levels of effectiveness. Institutional coupling provides a simple way to examine those connections without turning formal documents into measures they cannot support. The concept draws attention to mandate allocation, authority boundaries, interagency coordination, and the movement of information or incident responsibility. It also keeps cyberterrorism within a public affairs frame. The relevant question is not only whether terrorists can conduct cyber operations. Government must also be able to decide which institution leads when a cyber event begins to carry a terrorism dimension. That administrative transition is visible to different degrees in the three systems examined here.

The limits of the study are equally important. Public strategies and legal instruments cannot show whether coordination is fast, trusted, or effective under operational pressure. Interviews, after-action reports, exercises, and incident records would be needed for those claims. A larger comparative study could also examine whether similar forms of connection appear in other administrative systems. The present analysis does not attempt that step. Its contribution is narrower and more defensible. It shows how three governments formally bridge cybersecurity and counterterrorism while preserving specialized institutions, and it identifies the cross-domain interface as a legitimate object of public governance research.

REFERENCES

- Agranoff, R., & McGuire, M. (2001). Big questions in public network management research. *Journal of Public Administration Research and Theory*, 11(3), 295–326. <https://doi.org/10.1093/oxfordjournals.jpart.a003504>
- Boeke, S. (2018). National cyber crisis management. Different European approaches. *Governance*, 31(3), 449–464. <https://doi.org/10.1111/gove.12309>
- Bowen, G. A. (2009). Document analysis as a qualitative research method. *Qualitative Research Journal*, 9(2), 27–40. <https://doi.org/10.3316/QRJ0902027>
- Brass, I., & Sowell, J. H. (2021). Adaptive governance for the Internet of Things. Coping with emerging security risks. *Regulation & Governance*, 15(4), 1092–1110. <https://doi.org/10.1111/rego.12343>
- Broeders, D., Cristiano, F., & Weggemans, D. (2023). Too close for comfort. Cyber terrorism and information security across national policies and international diplomacy. *Studies in Conflict & Terrorism*, 46(12), 2426–2453. <https://doi.org/10.1080/1057610X.2021.1928887>

- Carr, M. (2016). Public-private partnerships in national cyber-security strategies. *International Affairs*, 92(1), 43–62. <https://doi.org/10.1111/1468-2346.12504>
- Chaudhary, T., Jordan, J., Salomone, M., & Baxter, P. (2018). Patchwork of confusion. The cybersecurity coordination problem. *Journal of Cybersecurity*, 4(1), ty005. <https://doi.org/10.1093/cybsec/tyy005>
- Christensen, T., & Lægreid, P. (2007). The whole-of-government approach to public sector reform. *Public Administration Review*, 67(6), 1059–1066. <https://doi.org/10.1111/j.1540-6210.2007.00797.x>
- Cotta, B., & Righettini, M. S. (2026). Governing cybersecurity in the digital age. Mapping comprehensive policy mixes with the Nodality-Authority-Treasure-Organization lens. *Review of Policy Research*, 43(4), e70113. <https://doi.org/10.1111/ropr.70113>
- Hossain, S. T., Yigitcanlar, T., Nguyen, K., & Xu, Y. (2025). Cybersecurity in local governments. A systematic review and framework of key challenges. *Urban Governance*, 5. <https://doi.org/10.1016/j.ugj.2024.12.010>
- Huang, K., Madnick, S., Choucri, N., & Zhang, F. (2021). A systematic framework to understand transnational governance for cybersecurity risks from digital trade. *Global Policy*, 12(5), 625–638. <https://doi.org/10.1111/1758-5899.13014>
- Jarvis, L., & Macdonald, S. (2015). What is cyberterrorism. Findings from a survey of researchers. *Terrorism and Political Violence*, 27(4), 657–678. <https://doi.org/10.1080/09546553.2013.847827>
- Jarvis, L., Macdonald, S., & Nouri, L. (2014). The cyberterrorism threat. Findings from a survey of researchers. *Studies in Conflict & Terrorism*, 37(1), 68–90. <https://doi.org/10.1080/1057610X.2014.853603>
- Kadir, Z. K. (2025). Kejahatan Berbasis Identitas Digital: Menggagas Kebijakan Kriminal untuk Dunia Metaverse. *Jurnal Litigasi Amsir*, 12(2), 124–137.
- Kadir, Z. K. (2026). Old Explanations, New Crimes? Testing the Portability of Criminological Theory in the Digital Age. *Al-Zayn: Jurnal Ilmu Sosial & Hukum*, 4(4), 20463–20475. <https://doi.org/10.61104/alz.v4i4.12119>
- Kapucu, N. (2006). Interagency communication networks during emergencies. Boundary spanners in multiagency coordination. *The American Review of Public Administration*, 36(2), 207–225. <https://doi.org/10.1177/0275074005280605>
- Kapucu, N., & Hu, Q. (2016). Understanding multiplexity of collaborative emergency management networks. *The American Review of Public Administration*, 46(4), 399–417. <https://doi.org/10.1177/0275074014555645>
- Kianpour, M., & Frantz, C. (2025). Analysis of institutional design of European Union cyber incident and crisis management as a complex public good. *Regulation & Governance*, 19(4), 1037–1062. <https://doi.org/10.1111/rego.12640>
- Lewallen, J. (2021). Emerging technologies and problem definition uncertainty. The case of cybersecurity. *Regulation & Governance*, 15(4), 1035–1052. <https://doi.org/10.1111/rego.12341>
- Magnusson, L., Iqbal, S., Elm, P., & Dalipi, F. (2025). Information security governance in the public sector. Investigations, approaches, measures, and trends. *International Journal of Information Security*, 24, 177. <https://doi.org/10.1007/s10207-025-01097-x>
- Mappaselleng, N. F., Kadir, N. K., Ahmad, A. K., Kadir, Z. K., & Normiati. (2025). Beyond the Surface: Exploring the Next Level of Terrorism on the Dark Web. *Jambura Law Review*, 7(1), 309–335. <https://doi.org/10.33756/jlr.v7i1.26150>
- Masyhar, A., Utari, I. S., Usman, U., & Sabri, A. Z. S. A. (2023). Legal challenges of combating international cyberterrorism. The NCB Interpol Indonesia and global cooperation. *Legality*, 31(2), 344–366. <https://doi.org/10.22219/ljih.v31i2.29668>
- Michalec, O., Milyaeva, S., & Rashid, A. (2022). Reconfiguring governance. How cyber security regulations are reconfiguring water governance. *Regulation & Governance*, 16(4), 1325–1342. <https://doi.org/10.1111/rego.12423>
- 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>

- Savaş, S., & Karataş, S. (2022). Cyber governance studies in ensuring cybersecurity. An overview of cybersecurity governance. *International Cybersecurity Law Review*, 3, 7–34. <https://doi.org/10.1365/s43439-021-00045-4>
- Setiawan, D. A. (2020). Cyber terrorism and its prevention in Indonesia. *Jurnal Media Hukum*, 27(2), 267–283. <https://doi.org/10.18196/jmh.v27i2.9237>
- Siddha, A., & Benarrivo, R. (2023). Counter cyber terrorism governance in Indonesia. *Khazanah Sosial*, 5(2), 359–367. <https://doi.org/10.15575/ks.v5i2.26414>
- Solansky, S. T., & Beck, T. E. (2009). Enhancing community safety and security through understanding interagency collaboration in cyber-terrorism exercises. *Administration & Society*, 40(8), 852–875. <https://doi.org/10.1177/0095399708326345>
- Strom, K. J., & Eyerman, J. (2007). Interagency coordination in response to terrorism. Promising practices and barriers identified in four countries. *Criminal Justice Studies*, 20(2), 131–147. <https://doi.org/10.1080/14786010701396871>
- Utomo, E. S., Zulfa, E. A., Yuliatiningtyas, S., Rofi'i, M. S., & Barton, G. (2025). Governing cyberterrorism in Indonesia. Resilience and gaps in the Draft Cybersecurity Law RUU KKS 2025. *Indonesia Law Review*, 15(3), 155–179. <https://doi.org/10.15742/ilrev.v15n3.2>
- Australia-New Zealand Counter-Terrorism Committee. (2024). National Counter-Terrorism Plan. Fifth edition. Australian Government.
- Australian Government Department of Home Affairs. (2023). 2023–2030 Australian Cyber Security Strategy.
- Australian Government Department of Home Affairs. (2025a). A Safer Australia. Australia's Counter-Terrorism and Violent Extremism Strategy 2025.
- Australian Government Department of Home Affairs. (2025b). Australian Cyber Response Plan. AUSCYBERPLAN Version 1.
- Australian Government Department of Home Affairs. (2026). Horizon 2 Action Plan for the 2023–2030 Australian Cyber Security Strategy.
- Badan Nasional Penanggulangan Terorisme. (2026). Regulation No. 1 of 2026 on coordination among law-enforcement actors in terrorism criminal cases.
- Government of Indonesia. (2021). Presidential Regulation No. 28 of 2021 on the National Cyber and Crypto Agency.
- Government of Indonesia. (2023). Presidential Regulation No. 47 of 2023 on the National Cyber Security Strategy and Cyber Crisis Management.
- Government of Indonesia. (2026a). Presidential Regulation No. 8 of 2026 on the National Action Plan for Preventing and Countering Violent Extremism Leading to Terrorism 2026–2029.
- Government of Indonesia. (2026b). Presidential Regulation No. 9 of 2026 on the National Counterterrorism Agency.
- UK Government. (2022). National Cyber Strategy 2022.
- UK Home Office. (2023). CONTEST. The United Kingdom's Strategy for Countering Terrorism 2023.