



Balancing Security and Rights: Constructing a Rule-of-Law Framework for Counter-Terrorism Intelligence Sharing under Holistic National Security

Jiang N^{1*} and Yang N²

¹Law Professor and Director of the Research Center for the Rule of Law in Counter-terrorism, from Law School, Beijing Normal University, China

²PhD Candidate from Law School, Beijing Normal University, China

***Corresponding author:** Na Jiang, Law Professor and Director of the Research Center for the Rule of Law in Counter-terrorism, from Law School, Beijing Normal University, China, Email: 08025@bnu.edu.cn

Mini Review

Volume 11 Issue 3

Received Date: July 27, 2026

Published Date: September 16, 2026

DOI: 10.23880/ijfsc-16000464

Abstract

In the twenty-first century, terrorism has evolved into a highly fluid, networked, and attribution-resistant global risk. Counter-terrorism intelligence sharing has become an indispensable instrument of national security governance, yet its expansion has simultaneously generated profound tensions with fundamental rights to privacy, a fair trial, and data protection. Drawing on risk governance theory and an examination of landmark cases—including the European Court of Human Rights' *Wieder and Guarnieri v. United Kingdom* (2023), the Court of Justice of the European Union's *EncroChat* decision (2024), and China's evolving counter-terrorism legal framework under the Holistic National Security concept—this article argues that the central challenge of modern counter-terrorism intelligence sharing lies not in choosing between security and liberty, but in constructing institutional mechanisms capable of maintaining a "resilient equilibrium" between them. China's Counter-Terrorism Law, National Intelligence Law, and National Security Law collectively establish a legal foundation for intelligence cooperation while explicitly affirming the principles of rule of law and human rights protection. The path forward lies in refining procedural safeguards, strengthening judicial review, and embedding data protection standards into intelligence-sharing mechanisms—thereby transforming counter-terrorism intelligence sharing from a source of rights tension into a model of rule-of-law governance.

Keywords: Counter-Terrorism; Intelligence Sharing; Rule of Law; Holistic National Security; Privacy Rights; Institutional Resilience

Abbreviations

CJEU: Court of Justice of the European Union;

Introduction

Terrorism in the twenty-first century has abandoned linear organizational hierarchies in favor of networked

configurations, shifting from large-scale coordinated attacks to "lone-wolf" or small-cell operations, and increasingly relying on digital platforms for ideological mobilization and operational coordination. This "liquid terrorism" presents a profound governance paradox for states across jurisdictions. If states adhere strictly to traditional criminal law principles requiring actual harm or concrete danger, law enforcement can intervene only after an attack has

occurred or is imminent—rendering prevention ineffective and risking intolerable human costs. Conversely, if criminal law is permitted to advance its point of intervention without meaningful constraint, a broad range of ambiguous pre-incident behaviors—including speech, online activities, financial contributions, and social interactions—may be criminalized [1].

Nowhere is this tension more acute than in the domain of counter-terrorism intelligence sharing. Intelligence sharing is the lifeblood of modern counter-terrorism: it enables early warning, disrupts terrorist networks, and facilitates cross-border cooperation. Yet it also concentrates immense discretionary power in executive and intelligence agencies, operates largely beyond public scrutiny, and poses acute risks to privacy, a fair trial rights, and data protection. The question is not whether intelligence should be shared—the security imperative is undeniable—but how it should be shared within a framework that respects the rule of law and fundamental rights [2,3].

This article examines this question through the lens of China's Holistic National Security approach, as articulated in the Counter-Terrorism Law (2015, amended 2018), the National Intelligence Law (2017), and the National Security Law (2015), alongside relevant international jurisprudence. It argues that China's legal framework already contains the normative resources for constructing a rule-of-law framework for intelligence sharing, but that these resources require further institutional refinement to achieve a “resilient equilibrium” between security effectiveness and rights protection [4].

The Legal Architecture of Intelligence Sharing under Holistic National Security

China's counter-terrorism intelligence-sharing framework rests on a statutory triad that collectively establishes both the mandate for cooperation and the normative boundaries within which it must operate.

The National Security Law: Foundational Principles

The National Security Law (2015) establishes the overarching principle that intelligence work must be conducted “in accordance with the law” while “respecting and safeguarding human rights.” Article 51 provides that “the state shall improve the system for the collection, analysis, and use of intelligence information that is unified in reporting, responsive, accurate, efficient, and smooth in operation, establish a coordination mechanism for intelligence information work, and realize the timely collection, accurate analysis, effective use, and sharing of intelligence information.” This provision explicitly endorses intelligence sharing as a state objective while embedding it

within a framework of legality and coordination [5].

The National Intelligence Law: Operational Mandate

The National Intelligence Law (2017) operationalizes these principles. Article 2 provides that national intelligence work shall adhere to the Holistic National Security concept, providing intelligence support for preventing and resolving risks endangering national security. Article 8 establishes a foundational constraint: “National intelligence work shall be conducted in accordance with the law, respect and safeguard human rights, and protect the lawful rights and interests of individuals and organizations.” Article 19 further provides that intelligence agencies “shall strictly act in accordance with the law, shall not exceed or abuse their authority, shall not infringe upon the lawful rights and interests of citizens and organizations.”

Critically, however, the National Intelligence Law operates largely within a framework of executive discretion. While it articulates rights-respecting principles, it does not specify detailed procedural mechanisms for oversight, review, or remedy in the context of intelligence sharing [6].

The Counter-Terrorism Law: Intelligence Cooperation

The Counter-Terrorism Law (2015, amended 2018) establishes a dedicated intelligence framework for counter-terrorism. Article 43 provides that “the national counter-terrorism leadership body shall establish a national counter-terrorism intelligence center, implement a cross-departmental and cross-regional intelligence information working mechanism, and coordinate counter-terrorism intelligence information work.” It further mandates that “urgent intelligence information concerning other localities shall be promptly communicated to the relevant localities.”

Article 6 establishes the overarching principle that “counter-terrorism work shall be conducted in accordance with the law, respect and safeguard human rights, and protect the lawful rights and interests of citizens and organizations.” Article 6 further provides that “in counter-terrorism work, citizens' freedom of religious belief and ethnic customs shall be respected, and any discriminatory practices based on region, ethnicity, religion, or other grounds shall be prohibited.”

The Normative Gap

Collectively, these statutes establish a clear legal foundation for intelligence sharing while articulating rights-respecting principles. Yet they also reveal a normative gap. The statutes authorize extensive intelligence cooperation but provide limited procedural guidance on how the tension between security imperatives and rights protection should be resolved in practice. This gap is not unique to China—it is a feature of counter-terrorism law in virtually all

jurisdictions. But it is precisely this gap that generates the risk of institutional drift: intelligence sharing, in the absence of robust procedural and oversight constraints, tends to expand into domains that compromise rights without proportionate security gains.

Intelligence Sharing in Practice: Lessons from Comparative Jurisprudence

Comparative experience reveals both the risks of unconstrained intelligence sharing and the institutional mechanisms that can contain those risks [7].

The EncroChat Decision (CJEU, C-670/22, 2024): Mutual Trust and the Limits of Judicial Scrutiny

On April 30, 2024, the Court of Justice of the European Union (CJEU) delivered its judgment in the EncroChat case (Case C-670/22, *Staatsanwaltschaft Berlin v. M.N.*), arising from a joint French-Dutch police operation that intercepted encrypted communications from a large number of users across multiple countries, leading to thousands of arrests. The Berlin Regional Court referred questions to the CJEU asking whether the transmission of data collected by French investigators using hacking techniques was compatible with fundamental rights.

The CJEU's response was notable for its deference to the principle of mutual trust. The Court held that the transmission of data between member states pursuant to a European Investigation Order is subject only to the rules applicable to a similar procedure within the issuing state. The proportionality of the measure was analyzed solely in light of the law of the issuing state. Crucially, the Court established that national courts are required to disregard information and evidence that is likely to have a preponderant influence on the findings of fact when the accused is not in a position to comment effectively on said evidence.

The EncroChat decision illustrates a central dilemma of cross-border intelligence sharing: the principle of mutual trust, while essential for international cooperation, can operate as a shield against robust judicial scrutiny of rights-infringing measures. When one state's intelligence-gathering practices are insulated from review by the receiving state's courts, the result is a "race to the bottom" in which states have incentives to adopt the least restrictive—or least scrutinized—intelligence practices [8].

Wieder and Guarnieri v. United Kingdom (ECtHR, Applications Nos. 64371/16 and 64407/16, 2023): Extraterritorial Accountability

On September 12, 2023, the European Court of Human Rights (Fourth Section) held the United Kingdom accountable for its digital surveillance activities even when those

activities affect individuals outside the UK's borders. The case concerned alleged interception by GCHQ of electronic communications sent by non-British nationals located outside the UK. The Court's judgment affirmed that states cannot evade human rights scrutiny simply by conducting surveillance extraterritorially—finding a violation of Article 8 of the European Convention on Human Rights due to flaws in the surveillance regime. This principle is of profound significance for intelligence sharing, which increasingly involves the cross-border transfer of surveillance-derived data [9].

Pietrzak, Bychawska-Siniarska and Others v. Poland (ECtHR, Applications Nos. 72038/17 and 25237/18, 2024): Abstract Review of Surveillance Regimes

On May 28, 2024, the European Court of Human Rights ruled in *Pietrzak, Bychawska-Siniarska and Others v. Poland* that Poland's Anti-Terrorism Act surveillance regime violated the right to privacy. Significantly, the Court considered it possible to examine the impugned provisions in abstracto—that is, to assess the compatibility of statutory surveillance frameworks with human rights standards even in the absence of a specific individual complaint. The Court condemned Poland regarding its operational control regime and the retention and use of communications data under the Anti-Terrorism Act, finding inadequate safeguards against arbitrariness and abuse. This abstract review capacity is a powerful institutional mechanism for constraining intelligence regimes before they generate concrete rights violations.

Gillan and Quinton v. United Kingdom (ECtHR, Application No. 4158/05, 2010): The Standard of Reasonable Suspicion

In *Gillan and Quinton v. the United Kingdom* (Application No. 4158/05, judgment final on June 28, 2010), the European Court of Human Rights examined the UK's stop-and-search powers under the Terrorism Act 2000. The applicants were stopped and searched by police using powers that did not require reasonable suspicion. The Court found that the absence of any obligation on the part of the examining officer to show "reasonable suspicion" made it difficult for persons to have the lawfulness of the search reviewed, constituting a violation of Article 8. This case establishes that even preventive counter-terrorism measures must be anchored in objective criteria and subject to meaningful judicial oversight—a principle directly applicable to intelligence-sharing regimes that operate on the basis of predictive risk assessments rather than concrete evidence [10].

Comparative Implications

These cases reveal a common pattern: intelligence sharing, when unconstrained by robust procedural and judicial safeguards, tends to expand into domains that

compromise fundamental rights. The institutional response varies across jurisdictions, but certain common elements emerge: (1) independent judicial review of intelligence-gathering and sharing practices; (2) meaningful procedural rights for affected individuals, including the right to be informed and to challenge measures; (3) data protection standards that limit the purposes for which intelligence can be used and shared; and (4) extraterritorial accountability for intelligence activities.

Constructing a Resilient Framework: Toward Institutional Equilibrium

Drawing on the normative resources within China's existing legal framework and the lessons of comparative experience, this article proposes a framework for counter-terrorism intelligence sharing organized around four principles: legality, proportionality, procedural fairness, and accountability.

Legality: Clear Legal Authorization and Defined Scope

The principle of legality requires that intelligence-sharing activities be authorized by clear, accessible, and foreseeable legal provisions. China's Counter-Terrorism Law, National Intelligence Law, and National Security Law collectively provide such authorization. However, the scope of authorized intelligence sharing could be further specified. Legislative or judicial guidance should clarify: (1) the categories of intelligence that may be shared; (2) the purposes for which shared intelligence may be used; (3) the conditions under which intelligence may be shared with foreign or international partners; and (4) the duration for which shared intelligence may be retained [11].

Proportionality: Balancing Security and Rights

The principle of proportionality requires that intelligence-sharing measures be necessary and proportionate to the security threat they seek to address. This requires a shift from a "risk elimination" mindset to a "risk governance" approach. Intelligence sharing should be targeted at specific, identifiable threats rather than serving as a mechanism for generalized surveillance or suspicion. As the German Federal Constitutional Court has held in its data retention jurisprudence (BVerfGE 125, 260), preventive measures must be directed at "serious threats to fundamental legal interests demonstrated by concrete factual circumstances"—a standard of "proximity to real danger" that prevents the generalization and abuse of preventive powers [12].

Procedural Fairness: Rights to Information, Challenge, and Remedy

Perhaps the most critical dimension of a rule-of-law framework for intelligence sharing is procedural fairness.

Affected individuals should have: (1) the right to be informed of intelligence-sharing measures that affect them, subject to legitimate national security exceptions; (2) the right to challenge such measures before an independent body; and (3) the right to an effective remedy if their rights have been violated.

China's legal framework already contains elements of such procedural protection. The Counter-Terrorism Law provides for judicial review administrative review of terrorist designations, and the National Intelligence Law prohibits the abuse of authority and infringement of lawful rights. However, these provisions could be strengthened by establishing: (1) a specialized review mechanism for intelligence-sharing decisions, analogous to the UK's Independent Reviewer of Terrorism Legislation; (2) clear procedures for individuals to challenge intelligence-based restrictions; and (3) robust data protection standards that limit the purposes for which shared intelligence may be used [13].

Accountability: Oversight and Transparency

Accountability requires that intelligence-sharing activities be subject to effective oversight—both internal (within the executive branch) and external (by judicial or parliamentary bodies). China's legal framework provides for internal oversight through the hierarchical structure of intelligence agencies and the coordinating role of the national counter-terrorism leadership body. However, external oversight mechanisms could be further developed. The United Nations has emphasized the importance of "mainstreaming human rights and embedding data-protection and privacy safeguards into counter-terrorism efforts," a principle that applies with particular force to intelligence sharing [14-20].

Conclusion: From Security Imperative to Rule-of-Law Governance

The central argument of this article is that the maturity of a counter-terrorism legal order ultimately depends not on whether it becomes more powerful, but on whether it becomes more resilient—capable of absorbing the pressures of risk governance while preserving the foundational integrity of the rule of law. Intelligence sharing, precisely because it is indispensable to modern counter-terrorism and because it concentrates extraordinary discretionary power in executive agencies, must be governed by a framework that combines security effectiveness with robust rights protection [21-25].

China's legal framework—anchored in the Holistic National Security concept and articulated through the Counter-Terrorism Law, National Intelligence Law, and National Security Law—contains the normative resources for constructing such a framework. The path forward lies in institutional refinement: clarifying the scope and purposes

of intelligence sharing, strengthening procedural safeguards for affected individuals, and developing effective oversight mechanisms that can hold intelligence agencies accountable while preserving the confidentiality essential to their work [26-29].

In the end, the question is not whether security or rights should prevail—both are indispensable. The question is whether we can construct institutional mechanisms capable of maintaining a dynamic equilibrium between them. This is the central challenge—and the central opportunity—of counter-terrorism intelligence sharing in the twenty-first century.

References

1. Husak D (2008) Overcriminalization: The limits of the criminal law. Oxford, Oxford University Press, UK.
2. Ashworth A, Zedner L (2014) Preventive justice. Oxford, Oxford University Press, UK.
3. Dyzenhaus D (2008) The compulsion of legality. In: Ramraj VV Emergencies and the Limits of Legality. Cambridge, Cambridge University Press, UK.
4. Fletcher GP (2006) The indefinable concept of terrorism. *J Int Crim Justice* 4(5): 894-911.
5. (2010) *Holder v Humanitarian Law Project*, 561 US 1.
6. (1961) *Scales v United States*, 367 US 203.
7. (2013) *United States v Mehanna*, 735 F3d 32 (1st Cir 2013).
8. (2020) *United States v Alhaggagi*, 978 F3d 693 (9th Cir 2020).
9. (2021) *United States v Kourani*, 6 F4th 345 (2d Cir 2021).
10. Anti-Terrorism and Effective Death Penalty Act of 1996, Pub. L. No. 104-132, 110 Stat. 1214.
11. (2001) *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001*, Pub. L. No. 107-56, 115 Stat. 272.
12. (2004) *Intelligence Reform and Terrorism Prevention Act of 2004*, Pub. L. No. 108-458, 118 Stat. 3638.
13. 18 U.S.C. § 2339B.
14. German Criminal Code (Strafgesetzbuch), § 129a.
15. Judgment of February 15, 2006, 1 BvR 357/05, 115 BVerfGE 118 (German Federal Constitutional Court—Aviation Security Act decision).
16. Judgment of March 2, 2010, 1 BvR 256/08 et al., 125 BVerfGE 260 (German Federal Constitutional Court—data retention decision).
17. Terrorism Act 2006 (UK), c. 11.
18. Terrorism Prevention and Investigation Measures Act 2011 (UK), c. 23.
19. Case C-670/22, *Staatsanwaltschaft Berlin v. M.N. (EncroChat)*, Judgment of the Court of Justice of the European Union (Grand Chamber).
20. *Wieder and Guarnieri v. the United Kingdom*, Applications Nos. 64371/16 and 64407/16, Judgment of the European Court of Human Rights (Fourth Section).
21. *Pietrzak, Bychawska-Siniarska and Others v. Poland*, Applications Nos. 72038/17 and 25237/18, Judgment of the European Court of Human Rights.
22. *Gillan and Quinton v. the United Kingdom*, Application No. 4158/05, Judgment of the European Court of Human Rights.
23. *A and Others v. the United Kingdom*, Application No. 3455/05, Judgment of the European Court of Human Rights.
24. *Klass and Others v. Germany*, Application No. 5029/71, Judgment of the European Court of Human Rights.
25. *Roman Zakharov v. Russia*, Application No. 47143/06, Judgment of the European Court of Human Rights.
26. *Big Brother Watch and Others v. the United Kingdom*, Applications Nos. 58170/13 et al., Judgment of the European Court of Human Rights.
27. Counter-Terrorism Law of the People's Republic of China.
28. National Intelligence Law of the People's Republic of China.
29. National Security Law of the People's Republic of China.