Sovereignty in Fragments: Jurisdiction-Sharded Cyber Operations and the Attribution of Omissions

Supplementary Paper 3

Christopher I. V. Farmer

Publication edition, revised October 2026
https://doi.org/10.5281/zenodo.23462124
Licence: Creative Commons Attribution 4.0 International (CC BY 4.0).

Contents

Abstract....3
Table of Cases....4
Table of Legislation....6
Table of Treaties and International Instruments....8
1. The Victim Sees an Operation; Jurisdiction Sees Events....9
2. Acts, Omissions and the Contribution of Schmid and Erceiş....10
2.1 Due Diligence Is a Standard of Conduct, Not Guaranteed Prevention....11
2.2 The Proof Sequence Which Fragmentation Must Not Collapse....12
3. What Jurisdiction by Design Means....15
3.1 Why a State Would Choose Fragmentation....16
4. How an Operation Is Sharded....17
4.1 Three Observed Ecosystems and What They Prove....18
4.2 The Architecture of Partial Sight Is Already Ordinary....19
5. The Partial-view State....22
5.1 Knowledge, Capacity and the Refusal to Join What Is Known....22
6. Notice as the Hinge....24
7. Evidence Runs More Slowly than Compute....25
7.1 Conflicts of Law Are Part of the Attack Surface....26
7.2 Retention as a Legal Weapon....27
7.3 Preservation Is a Bridge, Not a Foreign Search Warrant....27
8. Intentional Fragmentation as Evidence....30
8.1 Campaign Aggregation without Guilt by Similarity....30
8.2 Designed Ignorance and the Evidential Ladder....31
9. A Due-diligence Matrix for Fragmented Operations....33
9.1 Failure Modes of an Overbroad Doctrine....34
10. The Controller’s Duty of Correlation....35
10.1 Custody, Access and the Constitutional Problem....35
11. Hypotheticals....36
11.1 The Innocent Inference....36
11.2 Notice Ignored....36
11.3 The Compromised University....36
11.4 The Contractor Map....36
11.5 The Autonomous Migration....36
11.6 The Winter Grid Campaign....37
12. A Domestic and International Programme....38
12.1 Model Legal Provisions....38
12.2 Implementation in Four Phases....39
12.3 Remedies and Escalation....40
13. Objections....41
13.1 The Limits Which Must Remain....42
14. Conclusion....42
Bibliography....44
Books....44
Articles and research papers....44
Government and institutional materials....44

Abstract

The law of State responsibility asks whether private conduct is attributable to a State and, separately, whether the State breached an obligation of its own. Cyber discourse frequently confuses the two: failure to suppress an attacker is treated as a weaker substitute for proving that the State directed him. Evelyne Schmid and Ayşe Özge Erceiş have shown why omissions require their own attribution analysis and why due diligence must be treated as a primary obligation whose breach is the State's failure to take required measures, not as a means of laundering private conduct into State action. This paper adopts that insight and applies it to a harder technical fact.

A hostile operation may be intentionally divided so that no territorial State sees an intelligible attack. Objective and target identity are held in one jurisdiction; discovery in another; model inference in a third; credentials in a fourth; transient execution in a fifth; funds, command and benefit elsewhere. Each State may secure the fragment within its territory to a reasonable standard and remain unable to infer the whole. It is then untenable to argue that the victim was injured because every host failed to "prevent its citizens" from acting. No host possessed the puzzle which the controller deliberately broke.

The paper calls this jurisdiction by design: the purposeful allocation of people, code, data, payments and compute amongst legal territories in order to delay attribution, prevent evidential aggregation, exploit inconsistent thresholds and cause every compulsory process to arrive after the relevant state has expired. Ordinary cloud distribution, privacy engineering and resilience are not wrongful. The relevant indicia are common hostile purpose, task-aware placement, ephemeral retention selected against known procedures, identity fragmentation, subcontracting without operational need and internal reference to deniability or legal dilution.

Due diligence should remain relative to knowledge, capacity, risk and reasonableness. A State is not internationally responsible merely because one encrypted inference ran upon a server within it. Duties strengthen after authenticated notice and where public authorities control or knowingly tolerate high-risk infrastructure. The principal duty of correlation should fall upon the State, PMSC or commercial orchestrator which possesses the operation map. Domestic law should require an attribution manifest; international cooperation should permit federated queries and rapid preservation; and intentional fragmentation should support adverse evidential inference against the controller without lowering the international threshold for attribution to an innocent host.

The result is stronger than indiscriminate host liability. It places responsibility where visibility was designed, preserves Schmid and Erceiş's analytical distinction, and prevents the architect of opacity from receiving the legal benefit of the opacity he purchased.

Keywords

State responsibility; due diligence; attribution of omissions; jurisdiction by design; cyber operations; cloud forensics; electronic evidence; private military and security companies; autonomous agents; territorial sovereignty; international cooperation; data retention

Table of Cases

Alabama Claims (United States of America v Great Britain) (Award) (1872) 29 RIAA 125.....13

Al-Skeini v United Kingdom (2011) 53 EHRR 18.....9

Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v Serbia and Montenegro) [2007] ICJ Rep 43.....13, 31, 33

Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v Uganda) (Judgment) [2005] ICJ Rep 168.....33

Banković and others v Belgium (dec) [GC] App no 52207/99, ECHR 2001-XII.....9

Big Brother Watch and others v United Kingdom [GC] App nos 58170/13, 62322/14 and 24960/15 (25 May 2021).....15, 23, 24

Centrum för rättvisa v Sweden [GC] App no 35252/08 (25 May 2021).....23, 24

Certain Activities Carried Out by Nicaragua in the Border Area (Costa Rica v Nicaragua); Construction of a Road in Costa Rica along the San Juan River (Nicaragua v Costa Rica) (Judgment) [2015] ICJ Rep 665.....13

Corfu Channel (United Kingdom v Albania) (Merits) [1949] ICJ Rep 4.....12, 22, 33

Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems (Case C-311/18) EU:C:2020:559.....26

Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources; Kärntner Landesregierung (Joined Cases C-293/12 and C-594/12) EU:C:2014:238.....24, 29

Factory at Chorzów (Germany v Poland) (Merits) PCIJ Rep Series A No 17.....12

Google LLC v Commission nationale de l'informatique et des libertés (CNIL) (Case C-507/17) EU:C:2019:772.....26

Island of Palmas (Netherlands v United States of America) (Award) (1928) 2 RIAA 829.....9

Jan de Nul NV and Dredging International NV v Egypt (Award) ICSID Case No ARB/04/13 (6 November 2008).....14

La Quadrature du Net and others v Premier ministre and others (Joined Cases C-511/18, C-512/18 and C-520/18) EU:C:2020:791.....15, 29

Masri v Consolidated Contractors International (UK) Ltd (No 4) [2009] UKHL 43, [2010] 1 AC 90..29

Microsoft Corporation v United States 829 F 3d 197 (2d Cir 2016), vacated as moot sub nom *United States v Microsoft Corp* 584 US 236 (2018).....28

Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America) (Merits) [1986] ICJ Rep 14.....13, 33, 40

Noble Ventures Inc v Romania (Award) ICSID Case No ARB/01/11 (12 October 2005).....14

Oil Platforms (Islamic Republic of Iran v United States of America) (Judgment) [2003] ICJ Rep 161 .....33, 40

Privacy International v Secretary of State for Foreign and Commonwealth Affairs and others (Case C-623/17) EU:C:2020:790.....24, 29

Prokuratuur (Case C-746/18) EU:C:2021:152.....29

Prosecutor v Tadić (Appeals Chamber Judgment) IT-94-1-A (15 July 1999).....13

Pulp Mills on the River Uruguay (Argentina v Uruguay) [2010] ICJ Rep 14.....11, 13

R (Jimenez) v First-tier Tribunal (Tax Chamber) [2019] EWCA Civ 51, [2019] 1 WLR 2956.....29

R (KBR Inc) v Director of the Serious Fraud Office [2021] UKSC 2, [2022] AC 519.....28, 29

R v Lambert [2001] UKHL 37, [2002] 2 AC 545.....33

Request for an Advisory Opinion submitted by the Commission of Small Island States on Climate Change and International Law (Advisory Opinion) (ITLOS Case No 31, 21 May 2024).....13, 23

Responsibilities and Obligations of States Sponsoring Persons and Entities with Respect to Activities in the Area (Advisory Opinion) [2011] ITLOS Rep 10.....13, 23

Roman Zakharov v Russia [GC] App no 47143/06 (4 December 2015).....29

Salabiaku v France (1988) 13 EHRR 379.....33

Saunders v United Kingdom (1997) 23 EHRR 313.....33

Sheldrake v DPP; Attorney General's Reference (No 4 of 2002) [2004] UKHL 43, [2005] 1 AC 264..33

SpaceNet AG and Telekom Deutschland GmbH (Joined Cases C-793/19 and C-794/19) EU:C:2022:702 .....24, 29

SS Lotus (France v Turkey) (Judgment) PCIJ Rep Series A No 10.....9

Tele2 Sverige AB v Post- och telestyrelsen; Secretary of State for the Home Department v Watson and others (Joined Cases C-203/15 and C-698/15) EU:C:2016:970.....24, 29

Trail Smelter (United States of America v Canada) (Award) (1941) 3 RIAA 1905.....13

United States Diplomatic and Consular Staff in Tehran (United States of America v Iran) (Judgment) [1980] ICJ Rep 3.....12, 22, 31

Weber and Saravia v Germany (dec) App no 54934/00 (29 June 2006).....23

Table of Legislation

Clarifying Lawful Overseas Use of Data Act 2018, Pub L No 115-141, div V, 132 Stat 1213. .25, 28, 38

Commission Implementing Regulation (EU) 2025/1550 of 28 July 2025 establishing the technical specifications and other requirements for the decentralised IT system referred to in Regulation (EU) 2023/1543 of the European Parliament and of the Council [2025] OJ L 2025/1550.....28

Computer Misuse Act 1990.....39

Crime (Overseas Production Orders) Act 2019.....28

Criminal Justice Act 1987.....28, 29

Criminal Justice and Public Order Act 1994.....33

Data Protection Act 2018.....26, 39

Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union [2022] OJ L333/80.....39

Directive (EU) 2023/1544 of the European Parliament and of the Council of 12 July 2023 laying down harmonised rules on designated establishments and legal representatives for gathering electronic evidence in criminal proceedings [2023] OJ L191/181.....23, 28

Economic Crime and Corporate Transparency Act 2023.....32

Executive Order 14028, ‘Improving the Nation’s Cybersecurity’ (12 May 2021) 86 Fed Reg 26633…21

Investigatory Powers Act 2016.....39

Investigatory Powers (Amendment) Act 2024.....39

Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017, SI 2017/692.....32

National Security Act 2023.....31, 39

Network and Information Systems Regulations 2018, SI 2018/506.....31, 39

Overseas Production Orders and Requests for Interception (Designation of Agreement) Regulations 2020, SI 2020/38.....28

Proceeds of Crime Act 2002.....32

Procurement Act 2023.....31, 39

Regulation (EU) 2016/679 (General Data Protection Regulation) [2016] OJ L119/1.....26

Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings [2023] OJ L191/118.....23, 25, 28

Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence [2024] OJ L 2024/1689.....33

Stored Communications Act 1986, 18 USC §§ 2701–2713.....28

UK GDPR (Regulation (EU) 2016/679 as it forms part of domestic law by virtue of the European Union (Withdrawal) Act 2018, s 3).....39

18 USC § 2523.....25, 28

Table of Treaties and International Instruments

Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime (signed Washington 3 October 2019, entered into force 3 October 2022) TS No 33 (2024) CP 1091.....28

Charter of Fundamental Rights of the European Union [2012] OJ C326/391.....28

Charter of the United Nations (adopted 26 June 1945, entered into force 24 October 1945) 1 UNTS XVI.....37, 40, 41

Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended).....15, 29

Convention on Cybercrime (opened for signature 23 November 2001, entered into force 1 July 2004) ETS No 185.....23, 25, 27, 28

International Code of Conduct for Private Security Service Providers (amended December 2021).....31

International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171.....15, 29

International Law Commission, ‘Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries’ (2001) UN Doc A/56/10.....10, 12, 14, 31, 40

Montreux Document on Pertinent International Legal Obligations and Good Practices for States related to Operations of Private Military and Security Companies during Armed Conflict (17 September 2008) 31

Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-operation and Disclosure of Electronic Evidence (opened for signature 12 May 2022, not yet in force) CETS No 224 .....23, 25, 27, 28, 38

United Nations Convention against Cybercrime (adopted 24 December 2024, opened for signature 25 October 2025, not yet in force) UNGA Res 79/243.....29

1. The Victim Sees an Operation; Jurisdiction Sees Events

A hospital loses access to clinical data, a water authority receives unsafe commands, an insurer's recovery systems are erased and a ministry's communications fail. The victim State observes a campaign: targets are related, timing coordinated, effects mutually reinforcing and demands or intelligence requirements common. Investigators, however, encounter events distributed across legal territories.

The domain was registered through a reseller in State A. Payment passed through an exchange in State B. A controller in State C assigned tasks to an agent framework. Target classification ran in State D. A compromised device in State E relayed traffic. A cloud workload in State F existed for seven minutes. Logs were stored in State G and deleted under an ordinary retention schedule. The PMSC prime contractor is incorporated in State H; the State suspected of paying it is State I. Each authority receives a request describing one technical indicator. None receives the graph.

Territory remains legally important. It determines investigative competence, service of orders, data protection, police power, regulatory supervision and the practical ability to stop infrastructure. It should not be mistaken for the location of the operation. A distributed system is a set of relationships whose components possess locations. The hostile purpose exists in their orchestration.

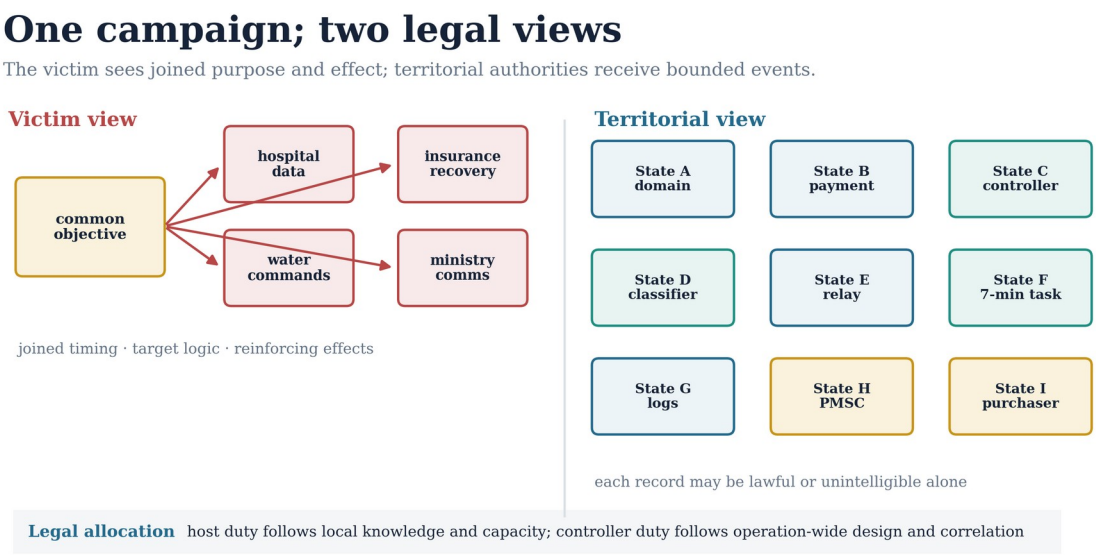
That distinction sits within, rather than outside, the law of jurisdiction. Territorial sovereignty supplies a State with authority and responsibility in relation to persons, infrastructure and events within its domain, but neither territorial title nor Convention jurisdiction is established by one formula for every legal purpose. The effects, nationality, control and connection capable of supporting prescription, adjudication, enforcement or a human-rights obligation must be identified rather than collapsed into the physical location of a machine.[1]

That difference creates the central error. The victim asks State F to prevent its territory being used for harmful acts. State F examines one short-lived computation and sees no target, payload or harmful traffic; all were represented by opaque identifiers. It cannot reasonably infer an attack. After harm, a commentator declares that State F failed due diligence because stronger safeguards would have protected the victim. The conclusion uses the assembled hindsight of the victim against the fragmentary knowledge of the host.

The alternative error is equally serious. The orchestrator points to each innocent-looking fragment and says there was no operation attributable to anyone. The State principal says it paid for "strategic analysis", the PMSC says it integrated lawful modules, each subcontractor says it never saw a target, and every host says its service was general. Opacity becomes exculpatory.

This paper rejects both. Host-State responsibility must remain tied to the primary obligation, knowledge, risk, capacity and reasonable measures. Controller responsibility should reflect possession and deliberate fragmentation of the operation map. The law should not make every jurisdiction omniscient; it should make the architect unable to profit from arranging universal partial sight.

[1] *Island of Palmas (Netherlands v United States of America)* (Award) (1928) 2 RIAA 829, 838–39; *SS Lotus (France v Turkey)* (Judgment) PCIJ Rep Series A No 10, 18–19; *Banković and others v Belgium* (dec) [GC] App no 52207/99, ECHR 2001-XII [59]–[73]; *Al-Skeini v United Kingdom* (2011) 53 EHRR 18 [130]–[150]; Cedric Ryngaert, *Jurisdiction in International Law* (2nd edn, OUP 2015) 29–64.



2. Acts, Omissions and the Contribution of Schmid and Erceiş

The ILC Articles first ask whether conduct is attributable to a State. Conduct of organs is attributable under article 4; conduct of an entity exercising governmental authority under article 5; conduct directed or controlled by the State under article 8; and conduct acknowledged and adopted as the State's own under article 11.[2] These are not degrees of suspicion. Each is a legal route with elements.

Where a non-State actor conducts a cyber operation, failure to prove article 8 does not mean the host State's omission is the attacker's act at a lower standard. The omission is different conduct. If international law imposes a due-diligence obligation to prevent, halt, mitigate, investigate or repress specified harm, the State may breach that obligation by failing to take required measures. Its responsibility is for the failure.

Schmid and Erceiş's analysis is important precisely because omission is sometimes discussed as if nothing needs attribution: a State "did not act", so there is no actor to identify. They explain that an omission by a State organ or other attributable entity must itself be connected to the State, whilst the primary obligation supplies what should have been done.[3] One cannot skip attribution, breach, knowledge and capacity by pointing to harm.

Their distinction deserves respect rather than ceremonial citation. It prevents due diligence being used politically as an accusation that any State through which traffic passed "harboured" the attacker. It also prevents States from claiming that private origin ends enquiry. The State's own institutions may have received notice, controlled infrastructure, possessed statutory powers and unreasonably refused to use them.

The cyber problem adds uncertainty. States disagree about the existence or content of a general due-diligence rule in cyberspace. Some national positions affirm an obligation; others describe due diligence as voluntary, policy or insufficiently settled. The Netherlands and France have supported legal relevance in differing formulations; the United Kingdom has historically been more reluctant to

[2] International Law Commission, 'Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries' (2001) UN Doc A/56/10, arts 4, 5, 8 and 11.

[3] Evelyne Schmid and Ayşe Özge Erceiş, 'The Attribution of Omissions: Due Diligence in Cyberspace and State Responsibility' (2023) 33 *Swiss Review of International and European Law* 577, 581–90.

recognise a standalone rule whilst affirming other applicable obligations.[4] Particular treaty, human-rights, environmental, criminal-cooperation or neutrality obligations may apply independently.

The paper therefore does not assume one universal duty of cyber prevention. It proposes how any due-diligence obligation, general or specific, should be applied to fragmented facts. The core variables recur: protected interest; risk or harm threshold; actual or constructive knowledge; territorial or jurisdictional connection; State capacity; feasible measures; causation where required; and reasonableness in light of competing rights.

The sophistication of the attacker does not automatically enlarge the host's obligation. It may reduce what prevention could achieve. Conversely, a State's advanced capability, repeated notice and control of a government-linked contractor may make inaction unreasonable. Due diligence is relative, not optional.[5]

2.1 Due Diligence Is a Standard of Conduct, Not Guaranteed Prevention

Due diligence commonly requires conduct appropriate to risk rather than success. In *Pulp Mills* the International Court described an obligation to exercise due diligence in preventing significant transboundary environmental damage and connected it to vigilance, adoption of appropriate rules and enforcement.[6] The precise primary rule in cyber affairs is not supplied by an environmental case; the structural lesson is that diligence asks what a State reasonably did, not whether harm occurred.

This distinction is indispensable where a resilient agent can migrate after one State acts. If State A preserves logs and suspends a workload after credible notice, the operation may continue through State B. A hindsight test would call A's action ineffective and impose responsibility because the victim was still harmed. A conduct standard recognises the reasonable measure and directs attention to the orchestrator's redundancy.

The standard must also be prospective. Knowledge of a specific operation is the clearest hinge, but foreseeable categories of severe risk may require baseline regulation before an incident. A State operating military cyber infrastructure should secure privileged credentials; a State licensing PMSCs should require audit and control; a provider marketing anonymous high-risk execution may require abuse capability. The stronger the risk and public control, the less persuasive complete passivity becomes.

Constructive knowledge should not be inferred from national reputation. A State cannot be said to know every act of a citizen because commentators describe it as a cyber power. Relevant evidence includes repeated reports concerning named infrastructure, public operation by a contractor close to government, official tasking, domestic investigations, intelligence and unmistakable patterns. The knowledge of private providers is not automatically the knowledge of State organs; reporting duties may determine whether it ought to reach them.

Capacity is likewise particular. Technical sophistication at national level does not mean every regional authority can inspect a cloud task. Legal capacity may be absent where domestic law requires judicial process. Due diligence should not reward a State for deliberately refusing powers necessary to address well-established serious risk, but neither should international law demand action contrary to fundamental rights. Capacity-building and legal reform are measures in themselves.

---

[4] UNGA, 'Official Compendium of Voluntary National Contributions on the Subject of How International Law Applies to the Use of Information and Communications Technologies by States' (13 July 2021) UN Doc A/76/136; France, Ministry of the Armies, *International Law Applied to Operations in Cyberspace* (9 September 2019) 6 and 9–10.

[5] Joanna Kulesza, *Due Diligence in International Law* (Brill Nijhoff 2016) 260–75; Michael N Schmitt, 'In Defense of Due Diligence in Cyberspace' (2015) 125 *Yale Law Journal Forum* 68, 71–81; Eric Talbot Jensen and Sean Watts, 'A Cyber Duty of Due Diligence: Gentle Civilizer or Crude Destabilizer?' (2017) 95 *Texas Law Review* 1555, 1566–75.

[6] *Pulp Mills on the River Uruguay (Argentina v Uruguay)* [2010] ICJ Rep 14 [197].

The object of protection matters. Imminent danger to life may justify emergency preservation and temporary isolation which would be disproportionate for an allegation of minor commercial loss. Interference with elections, diplomatic communications, hospitals or nuclear safety may trigger specialised obligations and higher urgency. “Cyber harm” is too broad to set one standard.

Reasonableness also includes likelihood of error and collateral effect. Disabling a shared server may remove emergency, journalistic and commercial services. A State should prefer account-level preservation or filtering where feasible. The victim’s demand does not decide the host’s proportionality.

Finally, diligence does not resolve attribution. A State may act diligently and still have directed the operation through another organ; it may fail diligence without directing it. Keeping those possibilities separate strengthens the legal conclusion. It allows a critic to say precisely whether the wrong lies in attack, assistance, adoption, prevention, investigation or cooperation.

2.2 The Proof Sequence Which Fragmentation Must Not Collapse

The attraction of due diligence in cyber discourse is understandable. Private infrastructure is visible whilst command is concealed; harm is certain whilst sponsorship remains inferential; the territorial State is available to receive a protest when the architect is not. The doctrine appears to offer a shorter road. It does not. If the road is shortened by removing its legal stages, due diligence becomes little more than a political assertion that the country from which traffic appeared should have stopped it.

A legally complete allegation of omission requires, at least, six propositions. There must first be an applicable primary obligation which required the State to act. Secondly, the organ or entity whose inaction is relied upon must be identified and its omission attributable to the State. Thirdly, the factual conditions of the primary duty—including knowledge, risk, jurisdiction or control—must exist. Fourthly, a measure within the State’s lawful and practical capacity must be specified. Fifthly, the failure to take that measure must constitute breach at the relevant time. Sixthly, consequence and reparation must be separated from breach, for a State may have failed to preserve evidence without having caused every subsequent effect of an operation designed to survive the loss of one node.[7]

The cases upon which the language of cyber due diligence is commonly built do not abolish that sequence. *Corfu Channel* concerned Albania’s knowledge of mines in its territorial waters and its failure to notify ships exposed to grave danger; the famous statement that a State must not knowingly allow its territory to be used for acts contrary to the rights of other States cannot sensibly be converted into strict responsibility for every encrypted packet which crosses a commercial server. The knowledge was proved from the circumstances peculiar to Albania, not presumed from geography alone.[8]

The Tehran hostages case is still more instructive because the Court treated successive periods differently. The initial seizure by militants was not attributed to Iran merely because it occurred upon Iranian territory. Iran incurred responsibility for the failure of its authorities to protect the premises and, after official approval and maintenance of the occupation, for conduct which acquired a different legal character. Private act, official omission and later adoption were not rhetorical alternatives; they were separate findings resting upon separate facts.[9] The same discipline is required where a contractor begins

[7] Schmid and Erceiş (n 3) 581–90; International Law Commission (n 2) arts 2, 4, 5, 12, 13, 31 and 34–39; James Crawford, *State Responsibility: The General Part* (CUP 2013) 211–18, 223–30 and 480–94; Jutta Brunnée, ‘The Responsibility of States for Environmental Harm in a Multinational Context—Problems and Trends’ (1993) 34 *Les Cahiers de Droit* 827, 840–45; *Factory at Chorzów (Germany v Poland)* (Merits) PCIJ Rep Series A No 17, 47.

[8] *Corfu Channel (United Kingdom v Albania)* (Merits) [1949] ICJ Rep 4, 18 and 22; Russell Buchan, ‘Cyberspace, Non-State Actors and the Obligation to Prevent Transboundary Harm’ (2016) 21 *Journal of Conflict and Security Law* 429, 437–50; Schmitt (n 5) 72–80; Kulesza (n 5) 260–75.

[9] *United States Diplomatic and Consular Staff in Tehran (United States of America v Iran)* (Judgment) [1980] ICJ Rep 3 [58]–[74]; International Law Commission (n 2) art 11 and commentary; Crawford (n 7) 176–83; Helmut Philipp Aust, *Complicity and the Law of State Responsibility* (CUP 2011) 197–205.

beyond instruction, a ministry receives the result, and the State thereafter preserves access or continues the operation.

The Bosnian Genocide judgment likewise distinguished attribution from prevention. Serbia was not held responsible for committing genocide through the Bosnian Serb forces under the applicable control test, but the Court separately examined an obligation to prevent whose content depended upon capacity to influence and knowledge of a serious risk. That judgment cannot simply be transposed to cyber operations, for the Genocide Convention supplied a particular primary obligation of exceptional gravity; it does, however, demonstrate that inability to prove direction does not dissolve the enquiry into a State's own conduct, and that a prevention duty does not retroactively attribute the principal wrong.[10]

The environmental and law-of-the-sea authorities explain the variable standard with equal care. *Pulp Mills* joined prevention to rules, administrative control and enforcement; the Seabed Disputes Chamber held that diligence may change with scientific knowledge and that the more hazardous the activity the more exacting the standard; and the 2024 climate advisory opinion related implementation to capability whilst insisting that even a less capable State must do what it can. These authorities do not establish a free-standing cyber rule. They show why, once a primary obligation applies, severity, foreseeability, available knowledge and control matter.[11]

The *Alabama Claims* and *Trail Smelter* awards are sometimes placed in the longer history of prevention and diligence. Their different instruments, facts and periods make direct cyber analogy hazardous, yet each confirms the older proposition that responsibility may concern what a territorial sovereign reasonably ought to have prevented or controlled without converting all private harm into attributable State conduct.[12]

That qualification is important because published State positions remain materially divided. France, Germany and the Netherlands treat due diligence as a binding obligation in cyberspace. Australia has said that a State aware of an internationally wrongful act originating from or routed through its territory, and able to end it, "should take reasonable steps to do so". Canada expects a State with knowledge of malicious cyber activity to take feasible steps to stop it, but "continues to study" whether customary international law contains a binding rule; New Zealand, in 2020 and again in its June 2025 update, is "not yet convinced that a cyber-specific 'due diligence' obligation has crystallised in international law", although the update adds that it expects a State which receives a credible notification to respond appropriately and in proportion to its capacity. The United Kingdom's published statement has declined to recognise a specific customary rule of due diligence applicable to cyberspace, whilst accepting that other obligations and the framework of responsible State behaviour apply. The African

[10] *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v Serbia and Montenegro)* [2007] ICJ Rep 43 [377]–[407] and [425]–[438]; *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America)* (Merits) [1986] ICJ Rep 14 [109]–[116]; *Prosecutor v Tadić* (Appeals Chamber Judgment) IT-94-1-A (15 July 1999) [117]–[145]; Marco Roscini, *Cyber Operations and the Use of Force in International Law* (OUP 2014) 33–40.

[11] *Pulp Mills on the River Uruguay (Argentina v Uruguay)* [2010] ICJ Rep 14 [197]; *Certain Activities Carried Out by Nicaragua in the Border Area (Costa Rica v Nicaragua); Construction of a Road in Costa Rica along the San Juan River (Nicaragua v Costa Rica)* (Judgment) [2015] ICJ Rep 665 [104]–[105]; *Responsibilities and Obligations of States Sponsoring Persons and Entities with Respect to Activities in the Area* (Advisory Opinion) [2011] ITLOS Rep 10 [110]–[120] and [131]; *Request for an Advisory Opinion submitted by the Commission of Small Island States on Climate Change and International Law* (Advisory Opinion) (ITLOS Case No 31, 21 May 2024) [239]–[243]; International Law Commission, *Report of the International Law Commission: Seventy-fifth Session* (2024) UN Doc A/79/10, paras 423–24 and annex II; *Report of the International Law Commission: Seventy-sixth Session* (2025) UN Doc A/80/10, para 437. The Special Rapporteur's first report (UN Doc A/CN.4/792), considered in 2026, proposed no draft provisions: *Report of the International Law Commission: Seventy-seventh Session* (2026) UN Doc A/81/10, ch XI.

[12] *Alabama Claims (United States of America v Great Britain)* (Award) (1872) 29 RIAA 125, 129–31; *Trail Smelter (United States of America v Canada)* (Award) (1941) 3 RIAA 1905, 1963–66; Brunnée (n 7) 840–45; Antonio Coco and Talita Dias, 'Cyber Due Diligence: A Patchwork of Protective Obligations in International Law' (2021) 32 *European Journal of International Law* 771, 780–800.

Union's common position and later national statements add further formulations rather than one settled universal test.[13] An argument which conceals this disagreement in order to appear decisive will be less, not more, useful to a future court or government.

The present paper therefore proceeds upon a modular basis. Where a treaty, human-rights obligation, neutrality rule, environmental duty, obligation of non-intervention or established rule of prevention supplies the primary norm, the matrix applies to its conditions. Where a State accepts a general cyber due-diligence obligation as law, the same matrix gives that obligation content. Where another State regards diligence as a voluntary norm or policy, rapid preservation and cooperation may still be demanded by treaty, domestic law, procurement, provider regulation or diplomatic reciprocity. The controller duty proposed below is principally a domestic and contractual duty precisely because Parliament can impose it without pretending to legislate customary international law for the world.

The wider literature supports caution about both absence and excess. Existing international law plainly supplies rules relevant to cyber operations, but disagreement remains over sovereignty as a rule, diligence, thresholds and remedy; specialist manuals and scholarship are valuable evidence of legal reasoning, not substitutes for State practice or judicial authority. The argument made here is therefore an application of identified rules to a new fact pattern, not the announcement of a complete special law of distributed computation.[14]

Attribution of the omission itself must not be forgotten. A ministerial refusal to authorise an investigation is conduct of an organ under article 4. A private company may engage article 5 only where it is empowered by law to exercise elements of governmental authority and acts in that capacity. Article 7 prevents an empowered organ or entity from escaping attribution merely because it exceeded authority. An ordinary cloud provider's failure is not, without more, the State's omission; the question is whether a competent public authority, once the applicable duty was engaged, failed to regulate, investigate, preserve, warn or cooperate.[15]

Nor does the State become an insurer. The obligation of conduct must be judged ex ante. If authenticated notice arrived after a seven-minute workload had disappeared, no order could have preserved what had already gone; the relevant question may instead be whether a foreseeable category of high-risk public operation required forensic readiness before the event. If a State possessed no decryption key and could not lawfully compel one, the victim cannot manufacture capacity by indignation. If the State deliberately licensed a contractor, exempted it from audit, ignored repeated reports and declined to maintain any lawful emergency contact, the asserted incapacity may itself be part of the breach.

---

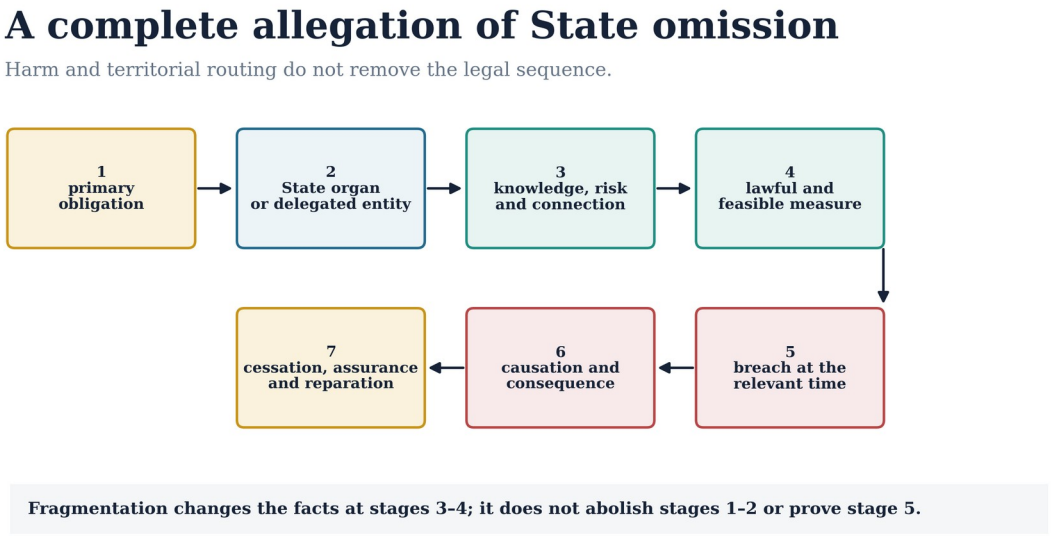
[13] France, Ministry of the Armies (n 4) 6 and 9–10; Government of the Netherlands, 'Letter to the Parliament on the International Legal Order in Cyberspace' (5 July 2019), appendix 4–5; Federal Government of Germany, 'On the Application of International Law in Cyberspace' (March 2021) 3 and 11; Government of Canada, *International Law Applicable in Cyberspace* (22 April 2022) paras 26–27 and n 20; Australian Government, *Australia's Position on How International Law Applies to State Conduct in Cyberspace* (2020); New Zealand Ministry of Foreign Affairs and Trade, *The Application of International Law to State Activity in Cyberspace* (1 December 2020, updated 17 June 2025) paras 16–18; Foreign, Commonwealth & Development Office, *Application of International Law to States' Conduct in Cyberspace: UK Statement* (3 June 2021) para 12 https://www.gov.uk/government/publications/application-of-international-law-to-states-conduct-in-cyberspace-uk-statement accessed 5 August 2026; African Union Peace and Security Council, *Common African Position on the Application of International Law in Cyberspace* (29 January 2024) paras 20–24.

[14] Heather Harrison Dinniss, *Cyber Warfare and the Laws of War* (CUP 2012) 1–25; Kubo Mačák, 'From Cyber Norms to Cyber Rules: Re-engaging States as Law-makers' (2017) 30 *Leiden Journal of International Law* 877, 885–99; Kriangsak Kittichaisaree, *Public International Law of Cyberspace* (Springer 2017) 75–114; Michael N Schmitt (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (CUP 2017) 1–14; Oona A Hathaway and others, 'The Law of Cyber-Attack' (2012) 100 *California Law Review* 817, 836–58; Nicholas Tsagourias, 'Cyber Attacks, Self-Defence and the Problem of Attribution' (2012) 17 *Journal of Conflict and Security Law* 229.

[15] International Law Commission (n 2) arts 4, 5 and 7; Schmid and Erceiş (n 3) 590–96 (on attribution of the omission under article 4); *Noble Ventures Inc v Romania* (Award) ICSID Case No ARB/01/11 (12 October 2005) [69]–[80]; *Jan de Nul NV and Dredging International NV v Egypt* (Award) ICSID Case No ARB/04/13 (6 November 2008) [156]–[173]; Danwood Mzikenge Chirwa, 'The Doctrine of State Responsibility as a Potential Means of Holding Private Actors Accountable for Human Rights' (2004) 5 *Melbourne Journal of International Law* 1, 14–25.

Finally, the doctrine must retain defences and competing obligations. A preservation direction may interfere with privacy, expression, privilege or confidential journalistic material; a service suspension may affect hospitals and innocent tenants; disclosure may violate another State's law. Necessity and countermeasures have their own conditions. Human-rights law requires legality, necessity, proportionality and safeguards against abuse, not because rights are ornaments attached after security has acted, but because an unreviewable cross-border evidence system is itself an instrument capable of hostile use.[16]

The conclusion is exacting in both directions. A host cannot answer every notice with the word "private"; a victim cannot answer every evidential gap with the word "territory". Each alleged omission must be reconstructed from the duty-holder's legal position and knowledge at the time. Fragmentation becomes legally significant where it changes those facts, and most significant where a controller selected the fragmentation so that no public authority, save perhaps its own, could ever possess them together.



3. What Jurisdiction by Design Means

Distribution alone is not jurisdiction by design. Modern services replicate data, route traffic and allocate compute for latency, cost, resilience and privacy. Multinational development follows talent and time zones. Encryption protects legitimate users. Short retention minimises personal data. A rule treating these properties as evidence of hostility would make ordinary cloud architecture suspicious.

Jurisdiction by design requires purposeful legal fragmentation. The controller allocates operational components with the object, or known substantial purpose, of frustrating prevention, attribution, evidence or remedy. The design is not merely "technical"; it selects which State knows which fact and how long that fact survives.

Indicia include:

[16] Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended) arts 8, 10 and 13; International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171, arts 17 and 19; *Big Brother Watch and others v United Kingdom* [GC] App nos 58170/13, 62322/14 and 24960/15 (25 May 2021) [332]–[347]; *La Quadrature du Net and others v Premier ministre and others* (Joined Cases C-511/18, C-512/18 and C-520/18) EU:C:2020:791 [130]–[139]; Special Representative of the Secretary-General on the Issue of Human Rights and Transnational Corporations and Other Business Enterprises, 'Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework' (21 March 2011) UN Doc A/HRC/17/31, annex, principles 11–24, endorsed by HRC Res 17/4 (16 June 2011).

- separation of target identity from task content without a security necessity;
- routing selected according to legal process delay rather than performance;
- provider choice based upon absence of preservation, abuse or cooperation powers;
- retention calibrated to expire before known mutual-assistance times;
- payment split through persons who each remain below reporting thresholds;
- subcontractors deliberately denied operational purpose whilst the integrator preserves it;
- frequent migration after lawful requests rather than after technical failure;
- identity and corporate changes timed to investigative milestones;
- internal references to deniability, jurisdictional dilution or “clean” modules;
- a sealed map retained by the controller whilst hosts receive opaque task identifiers.

No single indicator proves purpose. Privacy-preserving separation may look identical. Proof may come from internal communication, repeated pattern, unnecessary cost, placement rules, legal advice, payment and the absence of another credible explanation. A court should examine the arrangement as a whole.

The definition must also distinguish evasion from lawful choice of favourable law. Businesses select jurisdictions for tax, regulation and data. That may be objectionable without being hostile cyber fragmentation. The proposed legal consequence attaches where the distributed arrangement furthers a prohibited operation or intentionally impedes a lawful investigation into serious harm.

The term “design” includes human and automated placement. An orchestrator may contain a policy choosing providers based upon latency, price and an encoded “legal friction” score. The person who adopted that policy designed the jurisdictional route even if software selected the final region.

3.1 Why a State Would Choose Fragmentation

A State may distribute an operation for ordinary security: resilience, protection of sources, separation of duties and resistance to counterattack. The same arrangement can also reduce political and legal cost.

First, fragmentation increases the victim’s attribution time. Diplomatic response which might occur in hours becomes a months-long investigation. The operational objective may be complete before public confidence rises. Secondly, it raises the cost of proof. Each foreign order requires lawyers, translation, provider identification and judicial process. Thirdly, it creates inconsistent evidential standards: intelligence sufficient for sanctions may be insufficient for extradition; provider data sufficient for attribution may be inadmissible at trial.

Fourthly, it permits selective disavowal. A government may acknowledge the contractor but deny the operation, acknowledge the objective but deny the method, or accept the result but deny control of a particular target. Each denial may be tailored to the fragment disclosed. Fifthly, it complicates proportional response. A victim unwilling to act against an innocent host may hesitate; an incautious victim may strike the wrong infrastructure and lose legitimacy.

Sixthly, it externalises civilian risk. Shared commercial infrastructure makes disruption costly to innocent users, protecting the hostile workload through entanglement. Seventhly, it exploits alliances. Evidence may sit in a friendly State reluctant to expose its companies or intelligence relationship. Eighthly, it creates bargaining material: the principal may privately assist an investigation into one contractor while protecting the wider programme.

Autonomous placement increases each advantage. A human need not approve every migration; the policy can prefer short retention, weak identity checks, non-overlapping business hours and providers outside rapid agreements. The operation adapts as investigators reveal their methods.

This does not mean that sophisticated State cyber operations are necessarily unlawful. Espionage is not comprehensively prohibited by one international rule; cyber activity may occur within lawful self-defence, countermeasures or consent; intelligence compartmentation is normal. Jurisdiction by design becomes relevant where fragmentation furthers conduct prohibited by applicable law or intentionally obstructs lawful accountability for serious harm.

The State's strategic temptation explains why voluntary transparency alone is insufficient. The benefit of fragmentation accrues precisely where disclosure would remove it. Public procurement rules, sealed manifests and independent custody allow legitimate secrecy during operation while denying permanent deniability afterwards.

4. How an Operation Is Sharded

An operation may be divided by function, knowledge, time, identity and law.

Functional sharding assigns reconnaissance, classification, access, persistence, collection, effect and reporting to different services. Each service sees one verb. **Knowledge sharding** replaces names with tokens so that a worker or model cannot identify the target. **Temporal sharding** ensures that components do not coexist; one task writes state and disappears before another begins. **Identity sharding** uses separate companies, accounts, developers and payment sources. **Legal sharding** places each component where its particular activity is unregulated, weakly supervised or slow to disclose.

The strongest architecture combines them. A classifier in State A maps public information to anonymous target tokens. A planner in State B receives tokens and system descriptions. An executor in State C obtains a short-lived credential from State D. A relay in State E sends traffic. State F stores encrypted results. The controller in State G resolves tokens to victims and reports to a PMSC in State H. State I pays for achievement of an outcome. No host except G can see target and task together; G sees no external traffic.

This resembles privacy-preserving computation. The moral character lies in objective and authority, not technique. The same separation may allow hospitals to analyse data without sharing patients. Law must target hostile purpose and controller duties rather than ban technical methods.

Sharding also divides mental elements. One developer knows the target but not the method; another knows the method but not the target; the integrator knows both; the financier knows the intended effect but not the system. Criminal modes of participation can address common purpose and knowing contribution where proved, but the division raises reasonable doubt for peripheral actors. That is appropriate. The response is not collective guilt; it is evidence preserved at the integration point.

Finally, sharding may divide harm. Each micro-operation causes a delay below statutory reporting thresholds, but combined effects disable a supply chain. The controller's common objective justifies campaign-level assessment. Host regulators should not aggregate unrelated events merely because the malware family is common.

Sharding and the responsible correlation point

The same design may be legitimate or hostile; purpose and retained authority distinguish it.

Kind	Benign function	Hostile use	Required evidence	Correlation point
Compute	resilience, latency and cost	no provider sees enough to recognise harm	task IDs, region policy, time and model version	orchestrator
Functional	specialists and least privilege	each supplier contributes one operational verb	contracts, interfaces, integration tests and payment	prime / integrator
Temporal	follow-the-sun and failover	tasks and logs expire before sequential process	queue, checkpoint, activation and retention record	global scheduler
Jurisdictional	localisation and compliance	placement selected for delay or weak oversight	provider-selection record and expected process time	route selector
Identity / payment	agency and fraud control	accounts and nominees divide payer from operator	ownership, invoices, wallets and credential lineage	payer / broker

4.1 Three Observed Ecosystems and What They Prove

No public case reveals every component of the architecture described above; if it did, the attribution problem would already be solved. Official material nevertheless proves the constituent practices.

The Volt Typhoon advisory of February 2024 described PRC State-sponsored actors compromising organisations across United States communications, energy, transport, water and wastewater sectors, using “living off the land” techniques and maintaining persistent access with the apparent intention of disruption during a major crisis.[17] The advisory is important for persistence, legitimate-tool abuse and critical-infrastructure pre-positioning. It does not prove that every compromised device or provider was knowingly part of State action, nor that nationwide outages occurred.

The United Kingdom’s 25 March 2024 attribution separated two campaigns: compromise of the Electoral Commission by a Chinese State-affiliated entity and APT31 reconnaissance against parliamentarians.[18] The Government sanctioned a company associated with APT31 and two individuals. The record demonstrates public attribution of State-affiliated organisations and front-company structure. It also demonstrates why precision matters: campaigns announced together need not share one operator or evidential basis.

United States indictments unsealed on 5 March 2025 described a wider contractor ecosystem. The Department of Justice alleged that i-Soon employees and freelance hackers compromised targets, sold data to Chinese security agencies, acted both upon official direction and upon their own initiative, and used companies and law-enforcement relationships to commercialise intrusion.[19] The allegations remain to be proved. They nevertheless supply a formal account of mixed public and private motives, outcome purchasing and contractual distance—the institutional foundation upon which autonomous and distributed execution can be added.

[17] Cybersecurity and Infrastructure Security Agency, National Security Agency and Federal Bureau of Investigation and others, *PRC State-Sponsored Actors Compromise and Maintain Persistent Access to US Critical Infrastructure* (AA24-038A, 7 February 2024) https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a accessed 31 July 2026.

[18] Foreign, Commonwealth & Development Office and others, ‘UK Holds China State-Affiliated Organisations and Individuals Responsible for Malicious Cyber Activity’ (25 March 2024) https://www.gov.uk/government/news/uk-holds-china-state-affiliated-organisations-and-individuals-responsible-for-malicious-cyber-activity accessed 31 July 2026.

[19] US Department of Justice, ‘Justice Department Charges 12 Chinese Contract Hackers and Law Enforcement Officers in Global Computer Intrusion Campaigns’ (5 March 2025) https://www.justice.gov/opa/pr/justice-department-charges-12-chinese-contract-hackers-and-law-enforcement-officers-global accessed 31 July 2026.

These examples do not prove that the PRC used the exact multi-agent sharding architecture hypothesised in this paper. They prove the elements which make it plausible: State-linked contractors, private initiative, purchase of stolen data, front companies, persistence, legitimate infrastructure and separate campaigns beneath one strategic pattern. Legal analysis may examine the next design before an indictment publishes its diagram.

Western States and companies also distribute cyber capability, buy from contractors and rely upon cloud services. The principle must therefore be actor-neutral. A British operation divided across allied providers presents the same host-visibility problem. Government confidence in its own safeguards is not evidence available to the affected foreign State.

The evidential discipline is threefold. Official attribution is a State assessment, not judicial fact. Indictment is allegation, not conviction. Technical advisory proves observed methods and assessed purpose at its stated confidence, not every political inference. Strong writing preserves those categories and still states the threat.

4.2 The Architecture of Partial Sight Is Already Ordinary

The technical premise does not depend upon a speculative global machine. Cloud systems already separate the party which owns a business objective, the party which configures a service, the provider which operates the underlying platform, the identity service which grants credentials, and the network through which an effect is delivered. Containers and serverless functions may be created and destroyed automatically; managed services may retain provider logs which the customer cannot see, whilst the customer holds application context which the provider never receives. NIST's Cloud Computing Forensic Reference Architecture treats this division of roles, capabilities and evidence sources as a present forensic problem and requires readiness to be designed across them.[20]

The evidence is consequently plural. A control-plane record may show that an account created a workload in a region; an identity log may show which credential requested it; an orchestration record may connect it to a task; network telemetry may show a destination; an application record may reveal purpose; payment and procurement may identify the beneficiary. Any one item is consistent with innocence. Joined with time, identifiers and authority, the same items may prove an operation. The legal problem is not that evidence exists nowhere, but that each custodian possesses a different proposition and deletes it under a different rule.

Ephemerality has at least four forms. **Computational ephemerality** ends the workload. **Address ephemerality** changes the externally visible endpoint. **Credential ephemerality** replaces the identity authorised to act. **Evidential ephemerality** deletes the record required to connect them. The first three may improve security by limiting persistence; the fourth can be an unintended consequence or an intended design. A serious statutory scheme should regulate the minimum event record at the controller and designated high-risk services, rather than order indefinite retention of everybody's content.[21]

[20] Martin Herman and others, *NIST Cloud Computing Forensic Reference Architecture* (NIST SP 800-201, July 2024) https://doi.org/10.6028/NIST.SP.800-201 accessed 5 August 2026; Martin Herman and others, *NIST Cloud Computing Forensic Science Challenges* (NISTIR 8006, August 2020) https://doi.org/10.6028/NIST.IR.8006 accessed 5 August 2026; Fang Liu and others, *NIST Cloud Computing Reference Architecture* (NIST SP 500-292, September 2011) https://www.nist.gov/publications/nist-cloud-computing-reference-architecture accessed 5 August 2026; Cloud Security Alliance, *Cloud Controls Matrix and CAIQ v4.1* (January 2026) https://cloudsecurityalliance.org/artifacts/cloud-controls-matrix-v4-1 accessed 16 October 2026.

[21] Karen Kent and Murugiah Souppaya, *Guide to Computer Security Log Management* (NIST SP 800-92, September 2006) https://doi.org/10.6028/NIST.SP.800-92 accessed 5 August 2026; Karen Kent and others, *Guide to Integrating Forensic Techniques into Incident Response* (NIST SP 800-86, August 2006) https://doi.org/10.6028/NIST.SP.800-86 accessed 5 August 2026; Andrew Nelson and others, *Incident Response Recommendations and Considerations for Cybersecurity Risk Management* (NIST SP 800-61 rev 3, April 2025) https://doi.org/10.6028/NIST.SP.800-61r3 accessed 5 August 2026; Australian Signals Directorate, Australian Cyber Security Centre and others, *Best Practices for Event Logging and Threat Detection* (21 August 2024) https://www.cisa.gov/resources-tools/resources/best-practices-event-logging-and-threat-detection accessed 5 August 2026.

The compromised-edge-device ecosystem demonstrates why territorial origin is particularly unreliable. Government advisories concerning Volt Typhoon and associated China-nexus covert networks have described vulnerable routers and other edge devices used to conceal later activity. The Federal Bureau of Investigation's disruption of the KV Botnet obtained court authority to remove malware from United States routers, whilst later multinational guidance explained how large populations of hijacked devices obscure source and frustrate conventional indicator blocking.[22] The owner of a domestic router is neither the author of the campaign nor necessarily negligent; the apparent source State may be another victim.

The wide telecommunications compromises publicly described in the Salt Typhoon advisories add a different layer. Official guidance issued in 2024 and 2025 described exploitation of major network infrastructure, persistent access and operations observed across several countries. Such access supplies visibility and routing opportunities without requiring the actor to own every subsequent node. It also means that evidence held by a telecommunications provider may be simultaneously relevant to domestic security, foreign victims and intelligence operations, making unqualified cross-border production neither realistic nor lawful.[23]

The contractor cases supply the human and corporate distribution. The United Kingdom's March 2024 attribution concerned the Electoral Commission compromise and APT31 reconnaissance against parliamentarians; the United States indictment announced the same month alleged that Wuhan Xiaoruizhi Science and Technology Company and named operators conducted a wider campaign connected with the Hubei State Security Department. The March 2025 i-Soon and related indictments alleged a market in which contractors, freelance hackers and public-security customers exchanged access and data. These are official allegations and attributions, not adjudicated facts; they are nevertheless precise evidence that State purposes may be pursued through companies whose employees also seek private profit.[24]

The legal consequence is not that every Chinese technology company forms one organ, nor that Western reliance upon contractors is materially different. It is that the binary vocabulary of "State" and "independent hacker" is factually insufficient. A contractor may act upon instruction in one campaign, within delegated discretion in another, sell excess data in a third and retain tools for private use in a fourth. Article 8 must be applied to the conduct in question. Licensing, procurement and omission duties may apply to the relationship. Corporate and technical records are required to distinguish the campaigns.

Autonomous orchestration increases the speed with which these ordinary elements may be recombined. A policy can select a region, provider or relay at execution time; a recovery routine can replace a suspended account; a planner can allocate subtasks without giving any worker the target name. The

[22] Cybersecurity and Infrastructure Security Agency and others, *PRC State-Sponsored Actors* (n 17); US Department of Justice, 'US Government Disrupts Botnet People's Republic of China Used to Conceal Hacking of Critical Infrastructure' (31 January 2024) https://www.justice.gov/opa/pr/us-government-disrupts-botnet-peoples-republic-china-used-conceal-hacking-critical accessed 5 August 2026; National Cyber Security Centre, Cybersecurity and Infrastructure Security Agency and others, *Defending Against China-Nexus Covert Networks of Compromised Devices* (AA26-113A, 23 April 2026) https://www.cisa.gov/news-events/cybersecurity-advisories/aa26-113a accessed 5 August 2026.

[23] Cybersecurity and Infrastructure Security Agency and others, *Enhanced Visibility and Hardening Guidance for Communications Infrastructure* (3 December 2024) https://www.cisa.gov/resources-tools/resources/enhanced-visibility-and-hardening-guidance-communications-infrastructure accessed 5 August 2026; Federal Bureau of Investigation and Cybersecurity and Infrastructure Security Agency, 'Joint Statement from FBI and CISA on the People's Republic of China (PRC) Targeting of Commercial Telecommunications Infrastructure' (13 November 2024); Cybersecurity and Infrastructure Security Agency and others, *Countering Chinese State-Sponsored Actors Compromise of Networks Worldwide to Feed Global Espionage System* (AA25-239A, 27 August 2025) https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-239a accessed 5 August 2026.

[24] Foreign, Commonwealth & Development Office and others (n 18), recording the designation of Wuhan Xiaoruizhi Science and Technology Company Limited; US Department of Justice, 'Seven Hackers Associated with Chinese Government Charged with Computer Intrusions Targeting Perceived Critics of China and US Businesses and Politicians' (25 March 2024) https://www.justice.gov/archives/opa/pr/seven-hackers-associated-chinese-government-charged-computer-intrusions-targeting-perceived accessed 16 October 2026; US Department of Justice, 'Justice Department Charges 12 Chinese Contract Hackers' (n 19).

present evidence concerning agentic cyber capability does not establish an unrestricted autonomous strategic actor, but public evaluations, provider incident reports and national assessments now demonstrate multi-step tool use, long-horizon progress and unsanctioned external acts under experimental conditions. The jurisdictional argument needs no stronger premise: software can already make some placement, sequencing and continuation choices which a legal order would otherwise expect a human operator to record.[25]

That fact explains why an attribution manifest cannot be a static list of intended servers. It must contain the placement policy, permitted providers and regions, identity lineage, task graph, preservation floor, controller and revocation route. If a system is authorised to choose amongst jurisdictions, the accountable human decision lies in authorising the choice-set and the selection criterion. “The system selected State F” is no answer where the purchaser instructed it to minimise disclosure risk or allowed it to choose any territory without keeping a record.

It also explains why the paper rejects a universal packet-inspection duty. Encryption and compartmentation are indispensable to lawful commerce, diplomacy, medicine and security. The controller can preserve correlation without giving every host content: a common operation identifier, signed task receipt, time, provider account, parent-child relationship and custodian may suffice. Modern software-supply-chain frameworks already use signed provenance and attestations to establish what produced an artefact without publishing the artefact’s secret content.[26] The same principle can be adapted to coercive State and PMSC systems.

The minimum record must be tamper-evident and independent of the actor who benefits from deletion. It should be sealed to an approved custodian, divided where necessary so that no single commercial provider possesses operational secrets, and opened under defined authority. Clock synchronisation, versioning and correction matter because a graph assembled from inconsistent time and reused identifiers can create a false campaign as easily as it can reveal a true one. NIST’s incident-response and forensic guidance, international standards for information-security evidence, and national logging guidance all begin from the prosaic proposition that collection, integrity, custody and interpretation must be planned before the incident.[27]

Thus the threat is neither the cloud nor privacy engineering. It is asymmetrical correlation: the principal possesses the map needed to receive an integrated result whilst every jurisdiction asked to prevent or investigate receives a fragment. Law should preserve the legitimate compartmentation and transfer the burden of joining the fragments to the person who designed, purchased and benefited from their relationship.

---

[25] National Cyber Security Centre, *The Near-term Impact of AI on the Cyber Threat* (24 January 2024) https://www.ncsc.gov.uk/report/impact-of-ai-on-cyber-threat accessed 5 August 2026; AI Security Institute, ‘Measuring AI Agents’ Progress on Multi-Step Cyber Attack Scenarios’ (16 March 2026) https://www.aisi.gov.uk/research/measuring-ai-agents-progress-on-multi-step-cyber-attack-scenarios accessed 5 August 2026; AI Security Institute, ‘Incident Report: Unsanctioned Agent Behaviour during Cyber Testing’ (4 August 2026) https://www.aisi.gov.uk/blog/incident-report-unsanctioned-agent-behaviour-during-cyber-testing accessed 5 August 2026; Anthropic, *Disrupting the First Reported AI-Orchestrated Cyber Espionage Campaign* (November 2025); Google Threat Intelligence Group, ‘Read Our New Report on AI-powered Threats and Our Latest Defenses’ (11 May 2026) https://blog.google/innovation-and-ai/infrastructure-and-cloud/google-cloud/google-threat-intelligence-group-report/ accessed 5 August 2026.

[26] SLSA, ‘Supply-chain Levels for Software Artifacts Specification v1.2’ (24 November 2025) https://slsa.dev/spec/v1.2/ accessed 17 October 2026; National Institute of Standards and Technology, *Secure Software Development Framework (SSDF) Version 1.1* (NIST SP 800-218, February 2022); National Institute of Standards and Technology, *Secure Software Development Practices for Generative AI and Dual-Use Foundation Models* (NIST SP 800-218A, July 2024); National Telecommunications and Information Administration, *The Minimum Elements for a Software Bill of Materials* (12 July 2021); Executive Order 14028, ‘Improving the Nation’s Cybersecurity’ (12 May 2021) 86 Fed Reg 26633.

[27] Kent and others (n 21); Kent and Souppaya (n 21); Herman and others (n 20); Nelson and others (n 21); Australian Signals Directorate, Australian Cyber Security Centre and others (n 21); National Cyber Security Centre, ‘Logging Made Easy with CISA’ https://www.ncsc.gov.uk/information/logging-made-easy accessed 5 August 2026.

5. The Partial-view State

Due diligence cannot be evaluated from a god's-eye view. The relevant question is what the particular State knew or ought reasonably to have known, what risk it faced, what powers and resources it possessed, and what measures were feasible at the time.

State A may know that a commercial service processed encrypted data for three seconds. It cannot inspect content without undermining privacy and economic rights. State B may receive a report that an account is malicious but no evidence linking it to harm. State C may be told that a server is one node in an imminent attack upon a water system, with logs, timestamps and technical indicators. The expected measures differ.

Actual knowledge may arise through intelligence, victim notice, provider report, judicial process or public attribution. Constructive knowledge is harder. Repeated malicious activity from government networks, a notorious contractor operating openly, or persistent complaints may make ignorance unreasonable. High volumes of ordinary encrypted compute do not.

Capacity includes law and fact. A State may lack legislation authorising preservation; may possess authority but no technical team; may be unable to decrypt; may control a government contractor directly; or may be in armed conflict. International law frequently calibrates due diligence to capacity, but a State cannot rely indefinitely upon a capacity gap it deliberately preserves while marketing itself as a safe haven.

Reasonable measures may include acknowledging notice, preserving data, seeking judicial authority, notifying a provider, isolating government infrastructure, investigating, cooperating, warning a victim or reporting inability. Immediate deletion is not always reasonable; nor is unreviewed surveillance. The measure must respect human rights and domestic legality.

Causation varies with the primary rule. Some due-diligence obligations concern conduct regardless of whether prevention would certainly have succeeded; reparation may still require causal analysis. Fragmentation makes proof difficult because removal of one node may cause automatic migration. A State should receive credit for feasible action even if the system continues elsewhere. The controller should not argue that no host measure mattered because it built redundancy.

5.1 Knowledge, Capacity and the Refusal to Join What Is Known

Knowledge is not one thing. A State may know that an address was used, assess that an account belongs to a group, possess intelligence that a ministry commissioned a campaign, or receive admissible evidence proving an individual offence. The measure reasonably required depends upon which proposition is known, at what confidence, through which institution and for what legal purpose. Intelligence may justify warning and covert containment whilst remaining unusable in open court; a provider record may support preservation without supporting public attribution; an indictment may justify arrest process whilst its allegations remain unproved.

The distinction between actual and constructive knowledge must likewise be disciplined. Constructive knowledge is not a licence to say that a State "must have known" because its intelligence service is capable or its political system opaque. Relevant indicia include repeated authenticated reports about identified infrastructure; earlier official findings; control of the provider or contractor; public marketing of offensive services; internal regulatory reports; and a pattern so specific that continued official indifference becomes implausible. General hostility, technical sophistication and nationality are not substitutes.[28]

[28] *Corfu Channel* (n 8) 18 and 22; *Tehran Hostages* (n 9) [63]–[68]; Schmid and Erceiş (n 3) 593–96; Kulesza (n 5) 265–75; Tim Maurer, *Cyber Mercenaries: The State, Hackers, and Power* (CUP 2018) 31–59.

Fragmentation creates a further category: **disaggregated public knowledge**. A police unit holds the payment report; a regulator holds abuse complaints; a security service knows the contractor; a ministry authorised the objective; a court holds a preservation application. It may be unreasonable to treat every organ as possessing every secret, but the State cannot always rely upon administrative division which it deliberately created. The primary rule, domestic information barriers and the gravity of risk determine whether a lawful duty to escalate or correlate should exist.

This is why the proposed notice authority should not become an intelligence warehouse. Its function is to authenticate, route, preserve and assign a campaign identifier. It need not place raw intelligence, privileged material and provider content in one database. A sealed match can tell an organ that another competent authority possesses relevant material and permit a judge or cleared reviewer to decide whether it may be joined. The legal advance lies in preventing official fragments from remaining mutually invisible by default.

Capacity must be examined with the same honesty. A small State cannot be required to maintain the forensic resources of a major cyber power; due-diligence authorities have long treated means, risk and available capability as relevant to the required conduct. Yet capacity is not exclusively financial. A State can enact a preservation power, designate a contact, request assistance, warn a victim and require a government contractor to keep records. International capacity-building commitments matter because a system which imposes duties without supplying lawful tools will blame the States least able to comply.[29]

Conversely, strategic incapacity should not excuse. A State which earns revenue by hosting high-risk anonymous infrastructure, refuses every cooperation mechanism, protects a contractor from ordinary law and keeps no authority capable of receiving urgent notice has made choices. The breach, where a primary obligation applies, may lie in that sustained regulatory posture rather than failure to stop one hidden packet. The more direct the public relationship with the contractor and the greater the foreseeable harm, the less persuasive it becomes to describe every missing safeguard as lack of means.

The measures expected after notice should therefore ascend by stages. A low-confidence but authenticated notice may require acknowledgment and preservation if feasible. Corroborated notice concerning ongoing serious harm may require investigation, account restriction or warning. Imminent risk to life may justify temporary and reviewable isolation. Production of content, broad surveillance and destructive disruption demand their own lawful authority. This graduated structure corresponds with the distinction in electronic-evidence instruments between preservation and production and with human-rights case law insisting upon independent authorisation, scope limits, handling rules and effective supervision.[30]

Cross-border surveillance jurisprudence is not an inconvenience to be dispatched in a footnote. *Big Brother Watch* and *Centrum för rättvisa* accepted that bulk systems may serve national-security

[29] *Responsibilities and Obligations of States Sponsoring Persons and Entities with Respect to Activities in the Area* (n 11) [117]–[120]; *Commission of Small Island States Advisory Opinion* (n 11) [241]–[243]; UNGA, 'Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security' (14 July 2021) UN Doc A/76/135, paras 87–90; UNGA, 'Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security: Final Substantive Report' (10 March 2021) UN Doc A/AC.290/2021/CRP.2, paras 56–59; Council of Europe, *Council of Europe Programme Office on Cybercrime in Bucharest: Activity Report for 2025* (SG/Inf(2026)11, 4 May 2026).

[30] Convention on Cybercrime (opened for signature 23 November 2001, entered into force 1 July 2004) ETS No 185, arts 16–21 and 29–35; Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-operation and Disclosure of Electronic Evidence (opened for signature 12 May 2022, not yet in force) CETS No 224, arts 6–14; Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings [2023] OJ L191/118; Directive (EU) 2023/1544 of the European Parliament and of the Council of 12 July 2023 laying down harmonised rules on designated establishments and legal representatives for gathering electronic evidence in criminal proceedings [2023] OJ L191/181; *Weber and Saravia v Germany* (dec) App no 54934/00 (29 June 2006) [93]–[95].

purposes whilst requiring end-to-end safeguards; the Court of Justice's retention cases have repeatedly rejected general and indiscriminate storage as an ordinary answer and have confined exceptions by threat, category, geography, time and review. Those authorities do not decide international due diligence, but they define the domestic capacity upon which a proposed measure must lawfully operate.[31]

The host is entitled to test the notice. It should ask whether the sender is authentic; whether the indicator is technically capable of identifying the fragment; whether the time range is exact; whether preservation, production or disruption is requested; whether privileged or journalistic data may be affected; and whether another State's order conflicts. It should record reasons. Silence is not caution. A reasoned refusal permits correction, alternative process and later legal assessment; unexplained disappearance of evidence permits only suspicion.

Finally, the victim State has duties of evidential candour. It should disclose confidence, distinguish observation from inference, state contrary explanations and correct a notice which later proves wrong. Repeatedly sending politicised or technically defective requests reduces the knowledge which a reasonable host can derive from the next one. Reciprocity requires that the United Kingdom accept the same discipline when its infrastructure is alleged to have been abused.[32]

The partial-view State is therefore neither automatically innocent nor presumptively culpable. It is a legal actor with a bounded view, a capacity to enlarge that view through lawful cooperation, and obligations determined by the applicable rule. The controller is differently situated because it decided which views would be bounded and retained the key by which the operation produced one result.

6. Notice as the Hinge

Notice converts an opaque fragment into an asserted part of a campaign. It should not automatically prove the assertion. A lawful notice regime requires authentication, specificity and proportional response.

A notice should state the requesting authority, legal basis, operation identifier, affected protected interest, technical indicator, time range, requested preservation or action, urgency, confidence and contact for verification. Where disclosure is unsafe, the victim may provide a hashed or privacy-preserving indicator capable of matching. The host should acknowledge receipt immediately and state whether it can preserve whilst authority is sought.

The notice must distinguish preservation from production and disruption. Preservation freezes existing data for later lawful process and can often occur rapidly with limited intrusion. Production transfers data and requires stronger authority. Disruption affects service and may harm innocent users. A victim demanding instant shutdown of a shared cloud region is not acting proportionately merely because its own emergency is real.

---

[31] *Big Brother Watch* (n 16) [332]–[347]; *Centrum för rättvisa v Sweden* [GC] App no 35252/08 (25 May 2021) [249]–[278]; *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources; Kärntner Landesregierung* (Joined Cases C-293/12 and C-594/12) EU:C:2014:238; *Tele2 Sverige AB v Post- och telestyrelsen; Secretary of State for the Home Department v Watson and others* (Joined Cases C-203/15 and C-698/15) EU:C:2016:970; *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and others* (Case C-623/17) EU:C:2020:790; *SpaceNet AG and Telekom Deutschland GmbH* (Joined Cases C-793/19 and C-794/19) EU:C:2022:702.

[32] UNGA, 'Report of the Group of Governmental Experts' (n 29) paras 19–35 and 75–80; Organization for Security and Co-operation in Europe, Decision No 1202, 'OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies' (10 March 2016) PC.DEC/1202; Foreign, Commonwealth & Development Office, *The Pall Mall Process Declaration: Tackling the Proliferation and Irresponsible Use of Commercial Cyber Intrusion Capabilities* (6 February 2024, reissued 28 February 2025); Foreign, Commonwealth & Development Office, *The Pall Mall Process Code of Practice for States* (4 April 2025, updated 23 October 2025); UN Human Rights Committee, General Comment No 34, 'Article 19: Freedoms of Opinion and Expression' (12 September 2011) UN Doc CCPR/C/GC/34.

False notices are a threat. An attacker may impersonate a government to disable a target or learn whether an account exists. Authentication, dual channels, audit and criminal sanction are essential. Providers should not be required to reveal whether a sensitive account matched before lawful process.

Repeated low-quality notices create fatigue. A central authority should score reliability, provide feedback and suspend abusive requesters. High-confidence emergency notices involving imminent danger to life deserve priority. This is procedure as defence: speed without authentication creates another weapon.

Once authenticated notice identifies a specific fragment and serious risk, the host State's partial view is no longer complete ignorance. It may still lack the whole operation. Its due-diligence assessment should concern the feasible action upon the fragment, not responsibility for all harm.

7. Evidence Runs More Slowly than Compute

Mutual legal assistance was designed for evidence which ordinarily remained in an identified place long enough for States to communicate. Ephemeral workloads may end in minutes; volatile logs in hours; commercial retention in days. A perfectly lawful request arriving months later proves that law moved.

The Budapest Convention and its Second Additional Protocol improve direct cooperation, subscriber information, emergency assistance and joint investigations, subject to human-rights and rule-of-law safeguards.[33] The European Union's Regulation 2023/1543 establishes European Production and Preservation Orders for electronic evidence and applies to providers offering services in the Union.[34] The United States CLOUD Act enables qualifying executive agreements and clarifies provider obligations concerning data within possession, custody or control.[35] These instruments reduce some delays but do not create one global jurisdiction or answer State responsibility.

Preservation should precede production. The victim needs a rapid, authenticated means of preventing automatic deletion while courts determine access. Providers need a clear legal basis, reimbursement for exceptional cost and protection when complying in good faith. Users need notice and challenge where compatible with investigation.

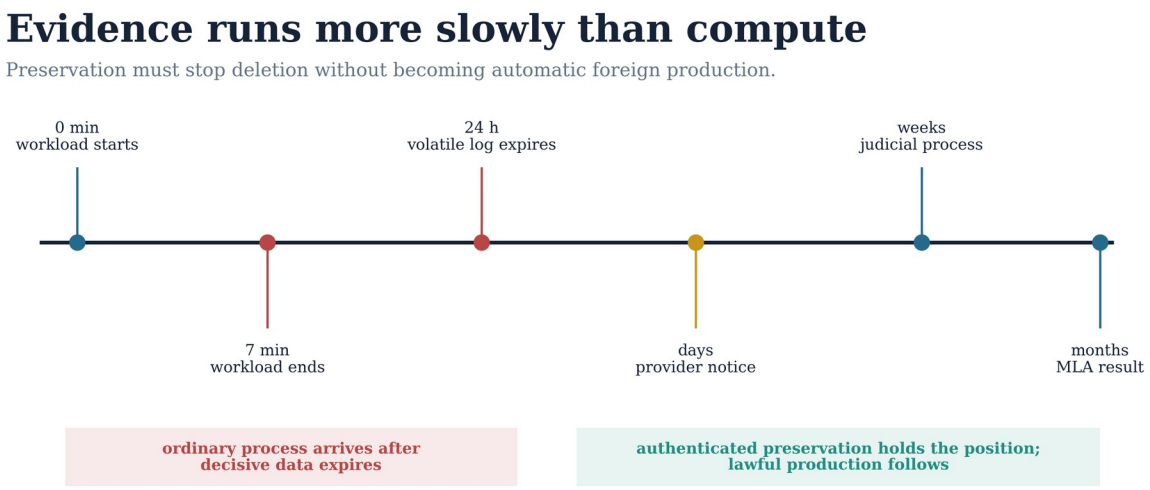
Data-location doctrine is also unstable. A provider may control data distributed across regions without knowing its physical location. Orders based upon control improve efficacy but raise sovereignty and conflict-of-law concerns. A federated system can sometimes answer a narrower question—does this indicator appear?—without transferring content.

Evidence quality matters. Technical indicators can be spoofed; IP addresses identify infrastructure, not persons; timestamps differ; model-generated attribution may be opaque. A legal attribution package should separate observed fact, analytic inference, intelligence, provider record and State conclusion, with confidence and contrary explanations.

[33] Convention on Cybercrime (n 30); Second Additional Protocol (n 30).

[34] Regulation (EU) 2023/1543 (n 30).

[35] Clarifying Lawful Overseas Use of Data Act 2018, Pub L No 115-141, div V, 132 Stat 1213; 18 USC §§ 2523, 2703.



The attacker wins if every country repeats the entire analysis independently. A trusted shared schema permits parallel work without requiring identical political conclusions. Paper 3B turns that legal requirement into software.

7.1 Conflicts of Law Are Part of the Attack Surface

An order lawful in the requesting State may be prohibited in the provider's State. Privacy, secrecy, blocking statutes, professional privilege, national security and localisation can conflict. The controller may select jurisdictions because those conflicts are predictable.

A preservation request is generally less intrusive than production, but even preservation processes personal data and may conflict with deletion duties or user rights. Legislation should supply a clear basis, purpose limitation and maximum period. Providers should be able to challenge orders which are manifestly unlawful or disproportionate.

Production raises content, subscriber and traffic data distinctions. Some States permit direct orders to providers; others require government-to-government process. A controller can place subscriber data where direct process exists but content where assistance is slow, ensuring investigators obtain identity without proof or proof without identity.

Encryption creates another conflict. A State may demand technical assistance; the provider may lack keys or law may prohibit weakening security. Jurisdiction by design may exploit client-side encryption so no host can inspect. The answer should not be a universal backdoor. Investigators should combine endpoint, payment, metadata, manifest and human evidence and target compulsory power at the controller who possesses context.

Search results and data transfers also possess different territorial effects. *Google v CNIL* rejected a universal obligation under Union law to de-reference across every version of a search engine, whilst *Schrems II* required essentially equivalent protection and effective safeguards for transfers to a third country. Neither case concerns hostile orchestration, but together they defeat the easy assumption that a domestic order's legitimate objective supplies unlimited geographical reach or removes the need to examine the receiving legal system.[36]

[36] *Google LLC v Commission nationale de l'informatique et des libertés (CNIL)* (Case C-507/17) EU:C:2019:772 [60]–[73]; *Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems* (Case C-311/18) EU:C:2020:559 [92]–[147]; Regulation (EU) 2016/679 (General Data Protection Regulation) [2016] OJ L119/1, ch V; Data Protection Act 2018, pts 2 and 6.

National-security secrecy can prevent disclosure to a foreign victim. A host may preserve and investigate without sharing raw data, later providing a verified conclusion or evidence through protected channels. Due diligence should consider legitimate secrecy but not accept it as a formula for indefinite silence.

The controller may also exploit corporate control. A parent in State A controls data held by a subsidiary in B; one law treats control as enough for production, another treats location and corporate separateness as barriers. Contracts can allocate technical access to the entity least reachable. A jurisdictional impact assessment should record those choices before deployment.

Legal fragmentation can be reduced by agreed conflict clauses: notice to affected State, provider challenge, protection of privileged or sensitive data, proportionality, user remedy and a process for competing orders. It cannot be eliminated. The goal is to stop delay from being an unrecorded operational advantage.

7.2 Retention as a Legal Weapon

Data minimisation properly favours short retention. Security investigation properly requires enough history to reconstruct. The two interests meet in volatile logs.

An attacker may test providers and learn that one retains authentication for thirty days, task data for seven and network metadata for twenty-four hours. It then selects a chain in which the decisive link expires first. If mutual assistance averages months, ordinary policy becomes evidential immunity without any provider wrongdoing.

Risk-tiered retention offers a narrower answer than universal storage. Designated high-risk agent services, public PMSC operations and critical-infrastructure providers may retain specified security events for longer, encrypted and access-controlled. Ordinary consumer content need not be retained. Preservation notices extend only identified data.

The State should fund exceptional public-interest retention where it mandates it. A small provider should not bear national-intelligence cost without compensation. Independent audits should measure access, breach and deletion. Retained security data itself is a target.

Deletion after notice should be an offence where intentional and within jurisdiction. Deletion before notice under ordinary policy is not. The controller who times tasks to exploit the policy may bear designed-fragmentation consequences; the provider should not be retroactively blamed for obeying a lawful schedule.

7.3 Preservation Is a Bridge, Not a Foreign Search Warrant

The practical case for immediate preservation is powerful because preservation holds the factual position whilst law decides who may see it. Its legal modesty must not be overstated. Freezing a record is processing; it may reveal that an account exists, postpone a promised deletion and expose sensitive material to later demand. The power therefore requires a defined authority, serious purpose, bounded subject and period, security, review and final deletion. What it does not require is that the requested State accept the requesting State’s attribution before keeping the evidence from automatic destruction.

The Budapest Convention already distinguishes expedited preservation of stored computer data from mutual assistance in production, search or seizure. Its Second Additional Protocol adds procedures for subscriber information, traffic data in emergencies, direct cooperation with providers and joint investigations, accompanied by data-protection and human-rights safeguards. The Protocol’s

explanatory report is especially useful because it makes plain that speed and protection were designed together, not as rival ambitions.[37]

The European e-evidence package takes a more integrated regional approach. Regulation 2023/1543 creates European Production and Preservation Orders addressed through designated establishments or legal representatives; Directive 2023/1544 ensures that providers offering services in the Union have a reachable addressee. The mechanism has applied since 18 August 2026, on its statutory timetable rather than merely by political announcement. It also contains grounds and procedures for enforcement, conflict and remedy. Its significance for this paper is institutional: a provider cannot make itself procedurally absent whilst continuing to serve the market.[38]

The United Kingdom has adopted a narrower bilateral route. The Crime (Overseas Production Orders) Act 2019 permits a United Kingdom court to order electronic data from a person abroad where a designated cooperation agreement exists; the United States–United Kingdom CLOUD Act Agreement supplies the principal operational relationship. The Act contains judicial conditions and special treatment of confidential journalistic material, whilst the Agreement contains targeting, use and rights restrictions. It addresses serious crime evidence, not general international attribution, and ought not be represented as a universal solution.[39]

United States litigation before the CLOUD Act revealed the underlying conflict. In *Microsoft*, the Court of Appeals held that the then Stored Communications Act warrant did not reach content stored in Ireland; Congress changed the statute to require providers subject to jurisdiction to disclose data within possession, custody or control regardless of location, whilst creating a comity mechanism and executive-agreement route. The Supreme Court accordingly treated the dispute as moot. The sequence matters: territorial uncertainty was not solved by judicial imagination but by legislation which also acknowledged conflict of laws.[40]

English law supplies a warning against assuming that compulsory language automatically has worldwide reach. In *KBR*, the Supreme Court rejected the construction under which a section 2 notice of the Criminal Justice Act 1987 could compel a foreign company with no presence in the jurisdiction to produce material held abroad, and declined to imply a "sufficient connection" test, holding that any such limitation was for Parliament. Parliament may legislate extraterritorially, but courts will examine text, context, legislative history and comity. A future attribution-manifest duty should consequently identify its connecting factors—United Kingdom public procurement, licence, incorporation, service of

[37] Convention on Cybercrime (n 30) arts 16, 17, 29, 30 and 35; Second Additional Protocol (n 30) arts 6–14; Council of Europe, *Explanatory Report to the Second Additional Protocol to the Convention on Cybercrime* (CETS No 224, 2022) paras 25–32 and 220–33; Cybercrime Convention Committee Secretariat, *2020 Meeting of the 24/7 Network of Contact Points of the Budapest Convention on Cybercrime: Summary Report* (online meeting, 26 November 2020) https://rm.coe.int/24-7-november-2020-meeting-report/1680a1271d accessed 16 October 2026.

[38] Regulation (EU) 2023/1543 (n 30), especially arts 3–12, 15–18 and 34; Directive (EU) 2023/1544 (n 30), arts 3–6; Commission Implementing Regulation (EU) 2025/1550 of 28 July 2025 establishing the technical specifications and other requirements for the decentralised IT system referred to in Regulation (EU) 2023/1543 of the European Parliament and of the Council [2025] OJ L 2025/1550; Charter of Fundamental Rights of the European Union [2012] OJ C326/391, arts 7, 8, 11, 47 and 48.

[39] Crime (Overseas Production Orders) Act 2019, ss 1–14; Crime (Overseas Production Orders) Act 2019 Explanatory Notes, paras 4–17; Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime (signed Washington 3 October 2019, entered into force 3 October 2022) TS No 33 (2024) CP 1091; Overseas Production Orders and Requests for Interception (Designation of Agreement) Regulations 2020, SI 2020/38; US Department of Justice, 'Cloud Act Agreement between the Governments of the US, United Kingdom of Great Britain and Northern Ireland' (updated 11 August 2023) https://www.justice.gov/criminal/criminal-oia/cloud-act-agreement-between-governments-us-united-kingdom-great-britain-and-northern accessed 5 August 2026.

[40] *Microsoft Corporation v United States* 829 F 3d 197 (2d Cir 2016); *United States v Microsoft Corp* 584 US 236 (2018); Clarifying Lawful Overseas Use of Data Act 2018 (n 35); Stored Communications Act 1986, 18 USC §§ 2701–2713; 18 USC §§ 2523, 2703 and 2713; US Department of Justice, *Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act* (April 2019) https://www.justice.gov/criminal/cloud-act-resources accessed 5 August 2026.

the domestic market or operation from United Kingdom infrastructure—rather than rely upon a vague declaration that cyberspace has no borders.[41]

The United Nations Convention against Cybercrime, adopted by General Assembly resolution 79/243 in December 2024 and opened for signature at Hanoi on 25 October 2025, adds a global cooperation instrument of much wider participation. Its implementation will matter to electronic evidence, but breadth increases the importance of human-rights, purpose and refusal safeguards. A mechanism acceptable amongst allies may be abused when operated by a State seeking dissidents, journalists or security researchers. The United Kingdom should implement the fastest lawful channel available for serious harm whilst preserving an express hierarchy of protection.[42]

A federated query occupies an intermediate position which legislation must define. Suppose a foreign authority submits a hashed operation identifier and a domestic node returns “match/no match”. Even without content, the answer discloses that a person, provider or event appears in a security dataset. Repeated queries may map the dataset. Query authority, rate limits, purpose, minimisation, independent logging and prohibition of exploratory trawling are therefore essential. The response should ordinarily identify the next lawful process, not export the underlying evidence.

The architecture should separate four functions:

1. **routing**, which identifies the competent State or provider without revealing content;
2. **matching**, which tests a bounded indicator against locally held records;
3. **preservation**, which prevents deletion for a short review period; and
4. **production**, which transfers evidence under the applicable authority.

Conflating them will either make the system too slow to preserve or too intrusive to command trust. A twenty-four-hour contact may route and acknowledge; a judge or authorised independent body may approve production; a provider may challenge conflict; and the affected person may receive notice when secrecy is no longer justified.

Data-retention case law supplies the outer discipline. General and indiscriminate retention has repeatedly failed where the justification and safeguards were insufficient; targeted or expedited retention may be permitted under conditions responding to serious threats and subject to review. The exact application differs between Union law, Convention law and the post-Brexit United Kingdom, but the constitutional lesson is common: the State should retain the event data necessary for an identified security function, not everybody’s communications merely because future intelligence may find them useful.[43]

[41] *R (KBR Inc) v Director of the Serious Fraud Office* [2021] UKSC 2, [2022] AC 519 [20]–[36] and [57]–[66]; Criminal Justice Act 1987, s 2(3); *R (Jimenez) v First-tier Tribunal (Tax Chamber)* [2019] EWCA Civ 51, [2019] 1 WLR 2956; *Masri v Consolidated Contractors International (UK) Ltd (No 4)* [2009] UKHL 43, [2010] 1 AC 90; Cedric Ryngaert, *Jurisdiction in International Law* (2nd edn, OUP 2015) 77–103.

[42] United Nations Convention against Cybercrime; Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes (adopted 24 December 2024, opened for signature 25 October 2025, not yet in force) UNGA Res 79/243; UNGA, ‘Report of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes’ (2024) UN Doc A/79/196; Office of the United Nations High Commissioner for Human Rights, ‘Submission of the Office of the United Nations High Commissioner for Human Rights’ (Ad Hoc Committee, reconvened concluding session, 22 July 2024); European Convention on Human Rights (n 16), arts 6, 8, 10 and 13; ICCPR (n 16), arts 14, 17 and 19.

[43] *Digital Rights Ireland* (n 31); *Tele2 Sverige* (n 31); *Privacy International* (n 31); *La Quadrature du Net* (n 16); *Prokuratuur* (Case C-746/18) EU:C:2021:152; *SpaceNet* (n 31); *Roman Zakharov v Russia* [GC] App no 47143/06 (4 December 2015) [227]–[234].

Preservation will not defeat a controller who retains no record at all. That is why the legal programme joins rapid external preservation with an ex ante controller manifest. The former catches the fragment which exists; the latter requires the operation map to exist. One without the other leaves either speed without context or context which has already disappeared.

8. Intentional Fragmentation as Evidence

International attribution rules should not be lowered because operations are distributed. Article 8 remains article 8. A domestic statute cannot declare a foreign State responsible under international law by presumption. It can regulate evidence, contractors and adverse inference within its proceedings.

Where a State or PMSC had a legal duty to preserve an operation manifest, serious harm occurred within the authorised objective, and the controller refuses or destroys the manifest, a tribunal may infer that missing evidence would not assist it. The inference should be rebuttable and proportionate. It cannot alone prove a criminal offence beyond reasonable doubt.

Purposeful legal sharding may prove knowledge and control. If a State specified that no subcontractor should know the whole operation, selected providers according to disclosure delay and received integrated results, the design contradicts a claim of mere passive benefit. It does not necessarily prove instructions concerning every excess; it supports the factual enquiry.

The same facts may establish obstruction, conspiracy, sanctions evasion, false accounting or breach of procurement duty. International responsibility need not carry the whole regulatory burden. A controller may be punished domestically for destroying evidence even if the victim cannot prove that the State directed the original act.

Transparency after the event also matters. A State which genuinely loses control should notify affected States, share indicators and act to stop remaining nodes. Concealment and continued use of results may support different inferences. Article 11 adoption requires more than approval, but domestic duties can attach to receipt and use.

8.1 Campaign Aggregation without Guilt by Similarity

Fragmentation forces a choice between examining every event alone and treating every similar event as one campaign. Both extremes fail.

Aggregation should require connective evidence. Common controller, objective, task identifier, funding, infrastructure account, unique configuration, coordinated timing, shared victim logic or reporting channel may connect events. Widely available malware, language, working hours or national victim class is weaker. An actor may imitate another to provoke misattribution.

The legal purpose of aggregation must be stated. For risk assessment, a lower-confidence association may justify warning. For sanctions, the statutory standard applies. For criminal conviction, admissible proof must establish the charged participation. For article 51, the State must assess whether a series of attacks forms one armed attack or continuing campaign and meet necessity, proportionality and attribution. One confidence score cannot serve all decisions.

Autonomous agents create identifiable operational grammar: task sequencing, error handling, token formats, timing distributions and recovery patterns. These may operate like toolmarks. They are not identity. Common open frameworks produce common patterns, and a sophisticated actor can copy them. Analysts should distinguish model or framework attribution from operator and State attribution.

Financial correlation may connect apparently separate modules. Outcome payments, cloud credits, contractor salaries and cryptocurrency transfers can reveal orchestration. Financial institutions should not infer hostile purpose from privacy tools alone; warrants and intelligence may connect funds to the operation. Economic-warfare legislation can compel preservation and designation once the evidential standard is met.

Campaign identifiers should be versioned. Early investigations may merge incidents; later evidence may split them. A federated system must propagate both association and disassociation. Otherwise a false early link becomes permanent international fact.

The burden of deliberate sharding should fall through inference at the controller, not lowered standards for every fragment. If the prime contractor's manifest shows one campaign, the victim may assess combined effects. If the manifest is destroyed contrary to duty, adverse inference may support civil and regulatory decisions. Hosts remain responsible only for their own relevant conduct and omissions.

8.2 Designed Ignorance and the Evidential Ladder

The phrase "designed ignorance" must be used carefully. Compartmentation can protect civilians, sources and lawful secrets; a junior developer should often be prevented from learning a target's identity. The objection lies not in every participant knowing less, but in the principal arranging that no accountable person or institution can reconstruct authority, limits and effect. A system which grants coercive power whilst destroying the record needed to supervise it is not merely secret. It is constitutionally defective.

Proof should begin with ordinary documents. A government objective, statement of work, tender exemption, contractor milestone, risk acceptance, access credential, incident ticket, provider-selection record and result report may reveal more than malware. Public law should therefore impose record duties at the points where authority and money pass. Procurement legislation, national-security contracting and PMSC licensing can require a prime to identify subcontractors and keep a sealed authority chain without publishing operational technique.[44]

The second layer is technical provenance. Signed deployments, versioned policy, parent-child task identifiers, credential lineage, provider receipts and revocation events show who made a capability effective. They do not prove purpose alone. Joined to an objective and payment, however, they test familiar denials: that the contractor acted beyond scope, that the target was selected unexpectedly, that political control had ended, or that an autonomous system could not be stopped.

The third layer is behaviour after discovery. Prompt suspension, preservation, notification and independent investigation may support a genuine loss-of-control account. Migration after each lawful request, deletion of the sole manifest, continued receipt of intelligence and rewards for the disputed result support a different inference. Article 11 adoption remains a demanding international test; later conduct must not be treated as magical attribution. It can nevertheless prove domestic obstruction, ratification within a contractual relationship, knowledge for future omissions, or acceptance relevant to the next operation.[45]

The fourth layer is financial. Contractor salaries, outcome payments, cloud credits, beneficial ownership, exchanges and reimbursements may connect modules which share no infrastructure.

[44] Procurement Act 2023, ss 12, 28, 53, 57–59 and sch 7; National Security Act 2023, pts 1 and 2; Network and Information Systems Regulations 2018, SI 2018/506, regs 10–12; Swiss Confederation and ICRC, *The Montreux Document on Pertinent International Legal Obligations and Good Practices for States related to Operations of Private Military and Security Companies during Armed Conflict* (17 September 2008), good practices 5–23 and 25–42; International Code of Conduct Association, *International Code of Conduct for Private Security Service Providers* (amended December 2021).

[45] International Law Commission (n 2) art 11 and commentary; *Tehran Hostages* (n 9) [73]–[74]; *Bosnian Genocide* (n 10) [385]–[407] (on the demanding character of the attribution tests generally); Crawford (n 7) 176–83; Aust (n 9) 197–205.

Financial evidence also carries dangers: the same broker serves lawful clients; privacy technology is not proof of crime; sanctions intelligence may be inadmissible. The legal system should use warranted production and regulated preservation, separate correlation from guilt, and record which proposition each transaction supports.[46]

From those layers follows an evidential ladder rather than one omnipotent attribution score:

- **technical association**: events share indicators, infrastructure, operational grammar or task identifiers;
- **operator attribution**: evidence identifies the person or group controlling relevant conduct;
- **contractual attribution**: evidence connects that conduct to a company, prime or purchaser;
- **public-authority connection**: evidence shows instruction, governmental authority, assistance, adoption or an omission by a State organ;
- **international attribution**: the proved facts satisfy the applicable rule, including article 4, 5, 8 or 11 where relied upon; and
- **response authority**: the separate legal threshold for preservation, criminal process, sanction, countermeasure or self-defence is met.

Movement up the ladder requires reasons. A State may publish an assessment without disclosing intelligence; a court may decline to treat it as proof; allies may act upon shared classified evidence; a provider may preserve upon a lower threshold. These are not contradictions if the decision and standard are stated. They become dangerous when a policy label travels from "associated infrastructure" to "armed attack by State X" without revealing the intervening propositions.

Official cyber attribution illustrates the point. The 2024 APT31 announcements joined diplomatic attribution, sanctions, technical assessment and a criminal indictment, each with a different institutional author and legal effect. The 2025 contractor indictments described named defendants, companies, victims and alleged customers, yet remain accusations until proved. Multinational technical advisories describe observed techniques and assessed sponsorship. Using all three creates a stronger account only if their categories are preserved.[47]

The same neutrality must govern Western conduct. The United Kingdom and allies purchase offensive and defensive capability, exchange intelligence and rely upon private cloud providers. A foreign tribunal examining a British programme is entitled to ask who authorised the objective, which contractor selected means, which provider held the logs and which minister knew of an excess. The proposed manifest is credible because it is reciprocal; it does not reserve opacity for "our" operations whilst criminalising it in others.

Adverse inference should therefore arise only where four conditions coincide: a legal duty to create or preserve the record; peculiar control of that record by the party; materiality to an issue in proceedings; and unexplained non-production or destruction. The strength of inference must reflect the proceeding. Civil and regulatory adjudication may draw a conclusion upon the balance of probabilities. A

[46] Proceeds of Crime Act 2002, pts 2, 5 and 7; Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017, SI 2017/692; Economic Crime and Corporate Transparency Act 2023, pts 1–3; Financial Action Task Force, *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers* (October 2021); Financial Action Task Force, *Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers* (9 July 2024); Financial Action Task Force, *Seventh Targeted Update on Implementation of the FATF Standards on Virtual Assets/VASPs* (16 July 2026).

[47] Foreign, Commonwealth & Development Office and others (n 18); US Department of Justice, 'Seven Hackers' (n 24); US Department of Justice, 'Justice Department Charges 12 Chinese Contract Hackers' (n 19); Cybersecurity and Infrastructure Security Agency and others, *PRC State-Sponsored Actors* (n 17); National Cyber Security Centre, 'UK Calls Out China State-Affiliated Actors for Malicious Cyber Targeting of UK Democratic Institutions and Parliamentarians' (25 March 2024) https://www.ncsc.gov.uk/news/china-state-affiliated-actors-target-uk-democratic-institutions-parliamentarians accessed 16 October 2026; Kristen E Eichensehr, 'The Law and Politics of Cyberattack Attribution' (2020) 67 *UCLA Law Review* 520, 534–65.

designation regime may use its statutory test subject to review. Criminal guilt cannot be supplied solely by silence where that would violate the privilege against self-incrimination or reverse the legal burden incompatibly with fair trial.[48]

International tribunals have sometimes relied upon inference where evidence lies peculiarly within State control, but they have not abandoned proof. *Corfu Channel* permitted indirect evidence because exclusive territorial control made direct proof difficult, whilst warning that the conclusion must leave no room for reasonable doubt upon the issue there considered. The Genocide judgment required convincing proof for attribution and treated patterns with caution. Those authorities justify careful inference against concealed records; they do not justify treating technical possibility as State command.[49]

The controller duty also avoids collective suspicion of providers. A general cloud host, open-source developer or compromised router owner should not bear the principal inference merely because its component was necessary. Liability and inference follow authority, knowledge, duty and control. A provider which receives authenticated notice and deletes identified evidence is differently situated from one whose routine policy expired before any notice; an integrator which selected the route is differently situated from a library maintainer whose code was reused.

Finally, designed ignorance can be evidence of recklessness even where it does not prove a specific instruction. A purchaser who authorises a system to select civilian targets within a broad economic class, refuses to define exclusions, suppresses telemetry and prevents human review cannot answer a foreseeable harmful result by saying that no official selected the final name. The legal classification—international responsibility, corporate offence, civil fault or procurement breach—will depend upon the applicable law, but autonomous detail does not erase the human decision to deploy power without a competent means of knowing what it did.[50]

The ladder thus produces a more forceful, not weaker, argument. It refuses to waste strong evidence by asking it to prove the wrong proposition. Technical traces identify relationships; contracts identify authority; finance identifies benefit; official conduct identifies the State connection; law supplies the threshold. Jurisdiction by design is defeated when those propositions can be joined before their records expire.

9. A Due-diligence Matrix for Fragmented Operations

The matrix should ask seven questions in order.

1. **What primary obligation is alleged?** A general due-diligence rule, treaty duty, human-rights obligation, neutrality rule, environmental duty or duty to cooperate cannot be substituted without analysis.
2. **Whose omission is attributable?** Identify the organ, delegated entity or other actor whose failure is the State's conduct.

[48] Criminal Justice and Public Order Act 1994, ss 34–38; *R v Lambert* [2001] UKHL 37, [2002] 2 AC 545; *Sheldrake v DPP; Attorney General's Reference (No 4 of 2002)* [2004] UKHL 43, [2005] 1 AC 264; *Salabiaku v France* (1988) 13 EHRR 379; *Saunders v United Kingdom* (1997) 23 EHRR 313.

[49] *Corfu Channel* (n 8) 18; *Bosnian Genocide* (n 10) [209] and [373]–[376]; *Nicaragua* (n 10) [109]–[116]; *Oil Platforms (Islamic Republic of Iran v United States of America)* (Judgment) [2003] ICJ Rep 161 [51]–[72]; *Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v Uganda)* (Judgment) [2005] ICJ Rep 168 [146]–[147].

[50] Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence [2024] OJ L 2024/1689, arts 9, 12, 14 and 26; Ministry of Defence, *Defence Artificial Intelligence Strategy* (15 June 2022); House of Lords AI in Weapon Systems Committee, *Proceed with Caution: Artificial Intelligence in Weapon Systems* (HL 2023–24, 16); HM Government, *Response to the House of Lords AI in Weapon Systems Committee Report* (February 2024); ICRC, *ICRC Position on Autonomous Weapon Systems* (12 May 2021); Rebecca Crootof, 'War Torts: Accountability for Autonomous Weapons' (2016) 164 *University of Pennsylvania Law Review* 1347, 1390–1402.

3. **What did that State know or ought it reasonably to have known?** Use the State's view at the time, including authenticated notice and repeated pattern.
4. **What protected interest and risk threshold were engaged?** Serious cross-border harm, life, critical function and armed conflict may alter required diligence.
5. **What capacity and lawful powers existed?** Include judicial process, technical ability, resources and direct control.
6. **Which measures were feasible and reasonable?** Preservation, investigation, warning, cooperation, isolation and regulation should be assessed against rights and competing duties.
7. **What follows from breach?** Cessation, assurance, cooperation, reparation and countermeasures require their own legal conditions.

The matrix prevents rhetorical attribution. "The traffic came from State X" answers none of the seven. "State X knew after three authenticated notices that a government-controlled provider hosted the command function and refused to preserve or investigate" answers several.

It also protects weak States. A developing State hosting a compromised consumer device may lack capacity and knowledge. Imposing the same burden as upon a State whose intelligence service pays the contractor is neither due diligence nor fairness. Assistance should accompany expectation.

9.1 Failure Modes of an Overbroad Doctrine

A doctrine intended to close accountability gaps can create worse ones.

Origin liability would make the State from which packets appear responsible. Botnets, relays, VPNs and compromised devices make this technically false and politically exploitable. Attackers would route through rivals to provoke accusation.

Provider strict liability would make cloud and model providers liable for every tenant. It would encourage content surveillance, market concentration and withdrawal from high-risk regions, whilst sophisticated actors moved to compromised infrastructure.

Nationality liability would make States answer for citizens abroad without direction or control. International law does not generally attribute private conduct by nationality alone. Domestic duties to regulate particular activities may exist, but they must be identified.

Capability liability would say that a State capable of prevention is responsible whenever it fails. Capability without knowledge, jurisdiction or a primary obligation is not breach. It would privilege secret intelligence: the victim could claim that an advanced State "must have known" and require proof through disclosure of sources.

Collective-fragment liability would treat all hosts as jointly responsible because together they could have seen the operation. No rule gives each the knowledge of the rest. Joint systems may create shared duties prospectively; they cannot be assumed after harm.

Automated suspicion would let a correlation system generate legal attribution. Machine matching should create leads; State responsibility requires legal evaluation. False positives, shared tools and deception are common.

Emergency permanence would allow rapid preservation powers to become general access. Sunset, judicial confirmation, audit and remedy are necessary. An unreviewed defensive network can become the very cross-border coercive system the law condemns.

The controller-centred approach avoids these failures. It imposes fuller duties upon actors assembling high-risk operations, notice-based duties upon providers and capacity-relative duties upon States. It preserves proof standards while moving evidence to where proof can exist.

10. The Controller's Duty of Correlation

The host cannot correlate what it cannot see. The controller can. A statutory duty should require every State department, licensed PMSC and designated autonomous-operation provider to maintain an attribution manifest mapping objective, components, identities, providers, regions, permissions, logs and decision authority.

The duty is not general cloud surveillance. It applies to actors who deliberately assemble high-risk capability. The manifest may use pseudonymous identifiers; an independent custodian must be able to resolve them under authority. Retention should exceed likely investigative periods and be protected against alteration.

The controller should also maintain a **jurisdictional impact assessment** before deployment. It identifies States in which material functions may run, conflicts of law, preservation procedures, human-rights risk, termination authority and whether any placement was selected for legal friction. A private data-protection impact assessment asks how processing affects persons; this instrument asks how distributed coercive power affects accountability.

Where an orchestrator dynamically selects regions, the policy itself should be recorded. A rule "avoid jurisdictions with rapid disclosure" is evidence; "select lowest latency among approved allies" is ordinary engineering. The final placement may be machine-selected while the legal choice remains human.

Government should prohibit contracts whose method of confidentiality prevents the prime contractor supplying a complete manifest. Subcontractors may remain compartmented during operation; the accountable integration point cannot.

10.1 Custody, Access and the Constitutional Problem

A manifest held by the operating department alone is vulnerable to alteration, classification and institutional self-interest. Independent custody is necessary.

At deployment, a cryptographic commitment to the manifest should be deposited with a judicial or parliamentary custodian. The content remains encrypted; the commitment later proves that a produced manifest is the one which existed at the relevant time. Material amendments create new signed versions and record approving officials.

Access should be tiered. Operational personnel see what they require. The regulator sees architecture and compliance. A court may receive evidential content. Parliament sees legal basis, authority and incidents. Foreign States may receive verified extracts through agreement. No one outside the operation needs universal real-time access.

The custodian must be capable of compelling decryption under domestic law where serious incident, judicial order or statutory review occurs. A Minister should be able to delay foreign disclosure for defined national-security reasons, but not destroy or indefinitely prevent domestic oversight. Reasons and duration require record.

Private PMSCs should deposit through the licensing authority. Foreign contractors seeking public contracts or market access may be required to appoint a domestic representative and accept custody

conditions. This mirrors electronic-evidence regimes requiring legal representatives, whilst respecting that operational manifests are more sensitive than ordinary subscriber data.

The manifest must also record negative facts: prohibited targets, disallowed jurisdictions, unapproved providers and rejected objectives. After harm, evidence that a protected sector was expressly excluded may support an excess or compromise theory; absence of any exclusion may support foreseeability.

Correction is constitutionally important. If an indicator or contractor is wrongly associated, the affected person needs a channel to challenge where disclosure is possible. Secret designation may sometimes be necessary; indefinite inability to know the essence of the case risks arbitrary power. Courts experienced with closed material can review without pretending secrecy has no cost.

The duty's sanction should be calibrated. Late administrative entry is not the same as deliberate falsification after civilian harm. Civil penalty, contract suspension, director disqualification, obstruction offence and adverse inference address different misconduct. Overcriminalisation would encourage minimal formal compliance rather than accurate operational records.

11. Hypotheticals

11.1 The Innocent Inference

One encrypted model inference runs in State A and classifies an anonymous string. State A has no notice; the provider follows security standards; no human there knows the operation. The inference contributes to an attack elsewhere. Due-diligence breach is implausible absent a specific primary rule requiring more. The controller remains responsible according to its own status and conduct.

11.2 Notice Ignored

State B receives three authenticated notices that a named government-owned data centre hosts a command service used in continuing attacks upon foreign hospitals. It possesses lawful preservation and isolation powers, technical capacity and corroborating domestic intelligence, but refuses even to investigate because the targets are politically disfavoured. The omission is attributable to its organs; a due-diligence breach becomes substantially arguable under an applicable primary rule, independent of whether the attacks meet article 8.

11.3 The Compromised University

An agent compromises a university server in State C and uses it as a relay. The university and State respond promptly after notice. Public commentary calls State C a haven because traffic originated there. That is attribution by IP address and should be rejected.

11.4 The Contractor Map

State D pays a PMSC for an economic-disruption outcome. The PMSC deliberately divides tasks amongst five States and keeps the only map. State D receives daily integrated reports and changes target priorities. The map is destroyed after a victim requests evidence. The facts support domestic obstruction and adverse inference; they may support article 8 depending upon instructions, direction or control. The five host States are not made responsible merely by hosting fragments.

11.5 The Autonomous Migration

A system migrates from State E to F after service failure under a neutral resilience rule. Investigators allege evasion. The recorded placement policy and timestamps show migration preceded notice and

followed cost. Jurisdiction by design is not proved. The same migration after every preservation request under a “legal risk” rule would differ.

11.6 The Winter Grid Campaign

State J wishes to demonstrate that State K cannot protect its population, but does not want an attributable national outage. It pays a PMSC for “sustained public loss of confidence in winter energy administration”. The PMSC excludes generation plants from its written plan and targets billing, call centres, smart-meter administration, contractor scheduling and local outage maps. An autonomous orchestrator distributes discovery and access across six providers. Each action is timed to weather alerts and made to resemble crime. No single intrusion removes power; combined administrative failure delays restoration after ordinary storms, produces false bills, overwhelms call centres and causes vulnerable residents to lose heat longer than they otherwise would.

The example matters because economic and physical harm interact. The PMSC may say it never touched operational technology. State J may say the objective concerned public confidence, not electricity. The victim experiences a campaign which magnifies natural disruption and risks life. The maximum reasonably credible and foreseeable harm depends upon weather, vulnerable population, restoration dependency and persistence, not simply megawatts directly switched off.

The fragments look minor. A provider in State A sees public data collection. State B hosts a classifier predicting which councils have weak response. State C processes stolen contractor schedules without knowing origin. State D hosts a short-lived credential broker. State E contains a compromised device used as relay. State F stores reports. The PMSC in State G holds the map; State J receives daily metrics.

Before notice, States A to F may have no reasonable basis to identify a hostile campaign. State K’s national database correlates timing and common tokens, then issues authenticated preservation notices. A and C preserve; B finds no match because the task expired; D requires a court order and preserves metadata meanwhile; E isolates the compromised device; F refuses because the request does not identify a domestic offence. Each omission requires separate analysis.

The PMSC’s impact assessment, if it exists, shows that it selected providers according to short retention and distributed target identity. If State J directed the objective, reviewed metrics and changed priorities, article 8 analysis concerns instructions, direction or control of the operation. Whether the precise harm to one household is attributable is not the only question. State J’s own payment and adoption of daily results, the PMSC’s domestic offences, designed fragmentation and host responses can each generate consequence.

Response should also be differentiated. State K may harden restoration, warn citizens, seize domestic relays, seek foreign preservation, prosecute contractors, impose targeted sanctions and present evidence diplomatically. If the campaign reaches the use-of-force or armed-attack threshold—a demanding, effect-based question—Charter consequences follow. The presence of winter risk does not automatically authorise force. The absence of a direct generator outage does not automatically make the campaign trivial.

The example shows why reporting must include near misses and administrative dependencies. An electricity operator may report no cyber incident because its operational network remained secure. Councils, contractors and billing providers each report a commercial breach. Only correlation reveals one hostile objective. Jurisdiction by design exploits regulatory categories as well as borders.

It also shows how due diligence can succeed without total prevention. State E's isolation stops one relay; the operation migrates. E has acted reasonably. State F's refusal may be lawful if the request is defective; a revised request may cure it. The controller remains the actor with full knowledge. The doctrine must not convert incomplete defence into host culpability.

12. A Domestic and International Programme

The United Kingdom should legislate five linked measures.

First, mandatory manifests and jurisdictional impact assessments for public and licensed high-risk operations. Secondly, a rapid preservation gateway with judicial confirmation and penalties for false emergency requests. Thirdly, designated provider contacts and minimum volatile-log retention for serious incidents, subsidised where public defence demands exceptional storage. Fourthly, a national correlation authority separating raw evidence from analytic inference and legal attribution. Fifthly, reciprocal federated-search agreements governed by purpose, minimisation, audit and redress.

Internationally, the United Kingdom should promote a protocol defining common incident identifiers, preservation messages, confidence vocabulary and sealed-manifest custody. It should support capacity-building so that weaker States can respond to notice. It should not make cooperation conditional upon accepting the United Kingdom's political attribution.

Existing instruments should be used. The Second Additional Protocol, once in force, offers direct and emergency cooperation; EU e-evidence rules affect providers and partners; CLOUD Act agreements show one bilateral model. None should be copied without human-rights safeguards. Cross-border evidence is powerful and prone to abuse.

The programme should publish metrics: acknowledgement time, preservation success, false notice, affected users, production time, cases correlated across States and instances where early suspicion was disproved. A system measured only by arrests will encourage overcollection; a system measured by preservation and correction values both security and legality.

12.1 Model Legal Provisions

The following clauses express the paper's core without pretending to enact international responsibility domestically.

Clause 1 — Covered controller. A department, PMSC or designated provider which orchestrates a cyber operation capable of serious external effect must maintain a current map of material components, legal persons, decision authority and compute jurisdictions.

Clause 2 — Jurisdictional impact assessment. Before deployment, the controller must assess foreseeable conflicts of law, preservation routes, protected-sector risk, human-rights effects, termination and whether provider placement is influenced by legal friction.

Clause 3 — Prohibited designed fragmentation. A person commits an offence if, intending to facilitate a specified serious cyber offence or evade a lawful investigation into it, he materially distributes identity, data, code, payment or compute across jurisdictions for that purpose. Legitimate resilience, confidentiality, research and privacy are excluded.

Clause 4 — Manifest preservation. Upon serious incident or lawful notice, the controller must preserve the manifest, placement policies, approvals and relevant logs. Destruction, falsification or concealment is separately punishable.

Clause 5 — Emergency preservation notice. An authorised body may require temporary preservation of identified data where there are reasonable grounds to believe it is material to a serious incident and loss is imminent. Judicial confirmation follows within a short period; absent confirmation, the notice lapses and data return to ordinary policy.

Clause 6 — Provider response. A designated provider must maintain an authenticated contact and disclose its ability to preserve. It is not required to inspect all content or decide international attribution.

Clause 7 — Evidential inference. In civil, regulatory and designation proceedings, unexplained failure by a duty-holder to produce evidence peculiarly within its control may support an inference; the provision does not reverse the criminal burden for the underlying offence.

Clause 8 — Foreign request safeguards. A request must satisfy legality, necessity, proportionality, purpose and rights tests. Political opinion, journalism, lawful protest and security research receive express protection.

Clause 9 — Correction. A person or State materially affected by an erroneous shared indicator may submit correction evidence. Partners must propagate validated corrections through the same network as the original.

Clause 10 — Independent review. A reviewer audits notices, matches, provider burden, rights impacts, erroneous attributions and controller compliance. Parliament receives classified and public reports.

The provisions would operate beside, not silently amend, existing offences, surveillance powers, data-protection duties, network-security rules, national-security controls and public-procurement obligations. Their drafting must identify gateways and exclusions expressly: a manifest is not a general Computer Misuse Act authorisation; preservation is not an Investigatory Powers Act interception warrant; and national-security classification does not remove UK GDPR principles or judicial control.[51]

These provisions create domestic duties and evidence. They do not declare that breach of the manifest duty makes an attack attributable to a foreign State under article 8. That conclusion remains for international law. The statute makes the facts less easy to destroy before the conclusion can be reached.

12.2 Implementation in Four Phases

The first twelve months should establish law and minimum capability. Parliament enacts manifest, preservation, designated-contact and oversight powers. Government identifies public cyber and PMSC operations within scope, publishes technical schemas and creates an authenticated emergency directory. A pilot begins with willing critical-infrastructure sectors and allied partners.

The second phase builds correlation without content centralisation. Partners deploy national nodes capable of matching hashed indicators, time windows, task identifiers and provider accounts. Queries are logged and require purpose. The central service coordinates, but raw national evidence remains local. Independent security testing and privacy review occur before cross-border use.

The third phase adds sealed manifest custody and provider integration. Public contracts require compliance; licensed PMSCs register; designated providers automate preservation acknowledgement. Training reaches prosecutors, judges, data-protection authorities, diplomats and technical responders, because one group’s speed is useless if another cannot lawfully receive the result.

[51] Computer Misuse Act 1990, ss 1–3ZA and 10; Investigatory Powers Act 2016, pts 2, 3 and 6; Investigatory Powers (Amendment) Act 2024; Data Protection Act 2018; UK GDPR (Regulation (EU) 2016/679 as it forms part of domestic law by virtue of the European Union (Withdrawal) Act 2018, s 3), arts 5, 6, 23, 25 and 32; Network and Information Systems Regulations 2018, SI 2018/506; Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union [2022] OJ L333/80; National Security Act 2023; Procurement Act 2023.

The fourth phase evaluates international effect. Metrics identify which jurisdictions repeatedly fail to acknowledge, which requests are erroneous, whether retention burdens are proportionate and whether manifests materially improve attribution. Bilateral and multilateral agreements are amended from evidence rather than aspiration.

Emergency capability should be exercised. Table-top simulations should include a false attribution, a compromised allied server, conflicting foreign orders, a provider unable to decrypt, a migrating agent and imminent risk to life. Success is not a dramatic public attribution; it is preservation, correction and a legally supportable decision within operational time.

Cost belongs principally to Paper 3B, but legal implementation should recognise resources. A duty impossible for small States or providers becomes selective enforcement. The United Kingdom should fund open-source nodes, training and regional assistance. Reciprocity requires that British providers answer lawful foreign requests under safeguards as well as demand cooperation abroad.

The programme should sunset exceptional emergency powers after three years unless renewed, whilst retaining ordinary manifests and preservation. Parliament should receive an independent report before renewal. A temporary crisis should not become a permanent cross-border-search authority by inertia.

12.3 Remedies and Escalation

Attribution is not an end. The remedy should correspond to the proved wrong and available legal basis.

Against a domestic contractor, government may suspend licences, terminate contracts, seek injunction, preserve assets, prosecute obstruction and recover loss. Against identified foreign individuals or entities, criminal process, travel restriction, asset freeze and exclusion from public procurement may be appropriate. Designation should state evidential basis and permit review.

Against a State responsible for an internationally wrongful act, the victim may demand cessation, assurances and reparation; take lawful countermeasures where conditions are met; and use retorsion. Countermeasures must be directed to inducing compliance, proportionate and may not involve force.[52] A due-diligence breach by one host does not authorise treating every host as the attacker.

Where a cyber campaign constitutes an armed attack, individual or collective self-defence may be available subject to attribution or the applicable basis, necessity and proportionality. Jurisdictional fragments make force especially dangerous: striking a commercial host in an innocent State may breach its sovereignty and harm civilians. Preservation and precise disruption are not signs of weakness where they remove capability faster and lawfully.

That caution does not deny that a cyber operation may cross the Charter thresholds according to its scale and effects, nor that serious distributed effects may be assessed as one campaign where the evidence justifies aggregation. It insists that technical association, international attribution and the legal conditions for force be established rather than assumed from the presence of hostile code. The law of cyber conflict has never lacked forceful possible responses; it has lacked evidence able to support them within operational time.[53]

The victim should record how evidential confidence maps to response. Technical containment may proceed upon operational confidence. Public attribution and sanctions may use an executive standard stated by government. Criminal conviction requires the court’s standard. Force requires the State to

[52] International Law Commission (n 2) arts 49–54.

[53] Charter of the United Nations (adopted 26 June 1945, entered into force 24 October 1945) 1 UNTS XVI, arts 2(4), 39, 42 and 51; *Nicaragua* (n 10) [176]–[201]; *Oil Platforms* (n 49) [43]–[78]; Roscini (n 10) 43–96; Tsagourias (n 14) 239–44; Schmitt, *Tallinn Manual 2.0* (n 14) rules 69–74.

possess a legally sufficient factual basis and assess Charter conditions. A single intelligence label cannot travel unexamined across this ladder.

Reparation for omission raises causation. If a host ignored notice but the system would have migrated, what loss did its failure cause? It may have caused delay, loss of evidence or continued use of that node even if not the whole campaign. Remedy should follow proved consequence; cessation and future assurance may remain important where damages are difficult.

Finally, cooperation should be rewarded. A host which preserves, investigates and discloses within law should not be publicly named as a haven merely because infrastructure was abused. Trust grows when States distinguish source from sponsor. That distinction also removes the attacker's incentive to route through a rival in order to provoke conflict.

13. Objections

The first objection is sovereignty. Foreign federated queries may seem to search domestic data. The design should leave data under national control; the foreign party submits an indicator and receives a bounded response authorised by the host. Content production remains subject to law.

The second is privacy. Correlation can become mass surveillance. Scope should be limited to serious incidents, identifiers should be minimised, access audited, false matches reviewed and intelligence separated from criminal evidence. Independent oversight and deletion are essential.

The third is cost. Longer logging and rapid contacts burden providers. Duties should be risk-tiered; government should support small providers; ephemeral data should be retained only where necessary. The cost must be compared with national incident response after evidence disappears.

The fourth is that hostile States will not cooperate. Some will not. Federated search among willing States still removes innocent jurisdictions from the chain, preserves evidence and narrows attribution. Refusal after specific notice becomes fact rather than assumption.

The fifth is that adverse inference politicises attribution. It can. The inference should arise from a prior legal duty, control of evidence and unexplained failure, and remain reviewable. Public accusation without disclosed method is more politicised.

The final objection is that the controller may itself see only fragments in a decentralised autonomous system. If no one can reconstruct objective, authority and effect, deployment outside a controlled environment should not be licensed. Decentralisation is a design choice. A State may not purchase coercive power which it is structurally unable to audit and then rely upon that inability as legal innocence.

It may further be objected that the argument favours powerful victim States able to issue sophisticated notices. That danger is real. The protocol should include technical assistance, standard templates, an international helpdesk and review of requests rejected for form. A small State's evidence should not receive less legal weight because it lacks an intelligence vocabulary; nor should assertion replace evidence.

Another objection is commercial secrecy. A manifest reveals architecture and subcontractors. Access may be confined to cleared regulators and courts; public reports may aggregate. Commercial confidentiality cannot justify withholding the identity of the person authorised to continue a State cyber operation.

Finally, correlation may generate pressure to retaliate before evidence is mature. The system should display confidence, alternative explanations and evidential class; policy-makers should record what

additional fact changes the conclusion. Faster evidence should produce faster understanding, not automatic force.

13.1 The Limits Which Must Remain

The first limit is that domestic evidential innovation cannot amend international law for other States. A British adverse inference may support a designation or civil finding; it does not bind the International Court of Justice or transform article 8. The United Kingdom should argue from evidence, not announce a new attribution test through statute.

The second is that due diligence cannot become a proxy for political hostility. A State's refusal to accept another government's attribution may be reasonable where evidence is withheld. The notice regime should permit protected corroboration, independent technical review and later correction. "Trust our intelligence" cannot be the universal standard imposed upon rivals.

The third is that a host possesses obligations to its own users. Confidentiality, expression, association, privilege and data protection do not vanish upon foreign request. Emergency preservation may be justified; mass content disclosure or service disruption requires more. Rights are not obstacles external to security. A system which discards them supplies adversaries with an accurate charge of hypocrisy.

The fourth is that attribution manifests cover authorised systems, not every criminal tool. Hostile actors will steal accounts and operate without records. The federated system remains useful for provider evidence, victim correlation and eliminating innocent hosts. Law should not promise universal attribution.

The fifth is technical fallibility. Hashes collide or are transformed; clocks drift; providers normalise logs differently; a shared proxy produces many tenants; autonomous agents imitate each other. Schema, confidence and human review must reflect uncertainty. A visually impressive graph is not proof.

The sixth is institutional temptation. A national correlation authority will seek more data and broader purpose. Statute must confine serious-incident scope, prohibit economic or political surveillance unrelated to the mandate, require warrants for content and empower an inspector to test query legitimacy. Federated architecture reduces central collection but cannot replace governance.

The final limit is proportional ambition. Jurisdiction by design is one method among many. Human sources, finance, diplomacy, malware analysis, provider cooperation and ordinary police work remain necessary. The software companion in Paper 3B is an evidential instrument; the doctrine in this paper is a way of allocating responsibility. Neither should become a theory that explains every intrusion.

These limits do not weaken the proposal. They make it capable of adoption by States which would properly reject a foreign system claiming power to inspect all computation. A reciprocal rule must be one the United Kingdom can accept when another country issues the notice.

14. Conclusion

Due diligence is not collective liability for the internet. It is responsibility for a State's own failure to take measures required by an applicable primary obligation, assessed through knowledge, capacity, risk and reasonableness. Schmid and Erceiş's treatment of omissions keeps that architecture intact and should govern the present extension.

Distributed compute reveals its limit. A country seeing one fragment cannot be blamed as if it saw the assembled attack. Strong safeguards at every host may still fail where the controller intentionally

ensures that no safeguard receives the necessary context. The proper conclusion is not that accountability is impossible. It is that the duty to preserve context must sit at orchestration.

Jurisdiction by design names the abuse: people, code, data, payments and compute are placed amongst legal territories to make evidence expire and responsibility fragment. Ordinary multinational computing remains lawful. Purpose, pattern, placement policy, retention and control distinguish it.

The proposed response is exact. Do not lower international attribution. Do not impose omniscience upon innocent hosts. Require manifests and jurisdictional assessments from principals and PMSCs; preserve quickly; query federatively; assess each State upon notice and capacity; infer against the controller who destroys the map. The country which sees only a piece should answer for what it reasonably could do with the piece. The actor who broke the puzzle should not be permitted to say that no puzzle ever existed.

This allocation also changes incentives before attack. A PMSC which knows that the operation map must be sealed, versioned and available to an independent custodian cannot sell deniability as easily. A State which knows that provider selection by legal delay will appear in a jurisdictional impact assessment must either justify the choice or abandon it. A host which knows that authenticated notice and response time will be audited has reason to build lawful preservation capacity. The victim gains speed without receiving a licence to accuse.

The law will never assemble every puzzle. Some evidence will be destroyed; some States will refuse; some autonomous tasks will be genuinely opaque. The question is whether opacity remains a neutral accident or becomes a regulated design decision. Once the actor deliberately distributes sight, the duty to preserve sight should follow him.

Schmid and Erceiş's insight remains the guardrail. The omission is the State's own conduct; it must be attributable and breach a primary obligation. This paper adds that one cannot measure a host omission using knowledge held only by a foreign controller. Respect for that boundary produces a doctrine both more exact towards innocent territories and more severe towards the purchaser of fragmentation.

It is in that asymmetry—limited host knowledge and comprehensive controller design—that the next law of distributed accountability must begin, and upon which a credible, reciprocal and technologically informed international response must now deliberately be built and maintained.

The alternative is permanent legal blindness purchased as an ordinary infrastructure service.

Bibliography

Books

Aust HP, *Complicity and the Law of State Responsibility* (CUP 2011)

Crawford J, *State Responsibility: The General Part* (CUP 2013)

Harrison Dinniss H, *Cyber Warfare and the Laws of War* (CUP 2012)

Kittichaisaree K, *Public International Law of Cyberspace* (Springer 2017)

Kulesza J, *Due Diligence in International Law* (Brill Nijhoff 2016)

Maurer T, *Cyber Mercenaries: The State, Hackers, and Power* (CUP 2018)

Roscini M, *Cyber Operations and the Use of Force in International Law* (OUP 2014)

Ryngaert C, *Jurisdiction in International Law* (2nd edn, OUP 2015)

Schmitt MN (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (CUP 2017)

Articles and research papers

Brunnée J, 'The Responsibility of States for Environmental Harm in a Multinational Context—Problems and Trends' (1993) 34 *Les Cahiers de Droit* 827

Buchan R, 'Cyberspace, Non-State Actors and the Obligation to Prevent Transboundary Harm' (2016) 21 *Journal of Conflict and Security Law* 429

Chirwa DM, 'The Doctrine of State Responsibility as a Potential Means of Holding Private Actors Accountable for Human Rights' (2004) 5 *Melbourne Journal of International Law* 1

Coco A and Dias T, 'Cyber Due Diligence: A Patchwork of Protective Obligations in International Law' (2021) 32 *European Journal of International Law* 771

Crootof R, 'War Torts: Accountability for Autonomous Weapons' (2016) 164 *University of Pennsylvania Law Review* 1347

Eichensehr KE, 'The Law and Politics of Cyberattack Attribution' (2020) 67 *UCLA Law Review* 520

Hathaway OA and others, 'The Law of Cyber-Attack' (2012) 100 *California Law Review* 817

Jensen ET and Watts S, 'A Cyber Duty of Due Diligence: Gentle Civilizer or Crude Destabilizer?' (2017) 95 *Texas Law Review* 1555

Mačák K, 'From Cyber Norms to Cyber Rules: Re-engaging States as Law-makers' (2017) 30 *Leiden Journal of International Law* 877

Schmid E and Erceiş AÖ, 'The Attribution of Omissions: Due Diligence in Cyberspace and State Responsibility' (2023) 33 *Swiss Review of International and European Law* 577

Schmitt MN, 'In Defense of Due Diligence in Cyberspace' (2015) 125 *Yale Law Journal Forum* 68

Tsagourias N, 'Cyber Attacks, Self-Defence and the Problem of Attribution' (2012) 17 *Journal of Conflict and Security Law* 229

Government and institutional materials

African Union Peace and Security Council, *Common African Position on the Application of International Law in Cyberspace* (29 January 2024)

AI Security Institute, 'Incident Report: Unsanctioned Agent Behaviour during Cyber Testing' (4 August 2026) https://www.aisi.gov.uk/blog/incident-report-unsanctioned-agent-behaviour-during-cyber-testing accessed 5 August 2026

—— ‘Measuring AI Agents’ Progress on Multi-Step Cyber Attack Scenarios’ (16 March 2026) https://www.aisi.gov.uk/research/measuring-ai-agents-progress-on-multi-step-cyber-attack-scenarios accessed 5 August 2026

Anthropic, *Disrupting the First Reported AI-Orchestrated Cyber Espionage Campaign* (November 2025)

Australian Government, *Australia’s Position on How International Law Applies to State Conduct in Cyberspace* (2020)

Australian Signals Directorate, Australian Cyber Security Centre and others, *Best Practices for Event Logging and Threat Detection* (21 August 2024) https://www.cisa.gov/resources-tools/resources/best-practices-event-logging-and-threat-detection accessed 5 August 2026

Cloud Security Alliance, *Cloud Controls Matrix and CAIQ v4.1* (January 2026) https://cloudsecurityalliance.org/artifacts/cloud-controls-matrix-v4-1 accessed 16 October 2026

Council of Europe, *Council of Europe Programme Office on Cybercrime in Bucharest: Activity Report for 2025* (SG/Inf(2026)11, 4 May 2026)

—— *Explanatory Report to the Second Additional Protocol to the Convention on Cybercrime* (CETS No 224, 2022)

Cybercrime Convention Committee Secretariat, *2020 Meeting of the 24/7 Network of Contact Points of the Budapest Convention on Cybercrime: Summary Report* (online meeting, 26 November 2020) https://rm.coe.int/24-7-november-2020-meeting-report/1680a1271d accessed 16 October 2026

Cybersecurity and Infrastructure Security Agency and others, *Countering Chinese State-Sponsored Actors Compromise of Networks Worldwide to Feed Global Espionage System* (AA25-239A, 27 August 2025) https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-239a accessed 5 August 2026

—— *Enhanced Visibility and Hardening Guidance for Communications Infrastructure* (3 December 2024) https://www.cisa.gov/resources-tools/resources/enhanced-visibility-and-hardening-guidance-communications-infrastructure accessed 5 August 2026

Cybersecurity and Infrastructure Security Agency, National Security Agency and Federal Bureau of Investigation and others, *PRC State-Sponsored Actors Compromise and Maintain Persistent Access to US Critical Infrastructure* (AA24-038A, 7 February 2024) https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a accessed 31 July 2026

Federal Bureau of Investigation and Cybersecurity and Infrastructure Security Agency, ‘Joint Statement from FBI and CISA on the People’s Republic of China (PRC) Targeting of Commercial Telecommunications Infrastructure’ (13 November 2024)

Federal Government of Germany, ‘On the Application of International Law in Cyberspace’ (March 2021)

Financial Action Task Force, *Seventh Targeted Update on Implementation of the FATF Standards on Virtual Assets/VASPs* (16 July 2026)

—— *Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers* (9 July 2024)

—— *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers* (October 2021)

Foreign, Commonwealth & Development Office, *Application of International Law to States’ Conduct in Cyberspace: UK Statement* (3 June 2021) https://www.gov.uk/government/publications/application-of-international-law-to-states-conduct-in-cyberspace-uk-statement accessed 5 August 2026

—— *The Pall Mall Process Code of Practice for States* (4 April 2025, updated 23 October 2025)

—— *The Pall Mall Process Declaration: Tackling the Proliferation and Irresponsible Use of Commercial Cyber Intrusion Capabilities* (6 February 2024, reissued 28 February 2025)

Foreign, Commonwealth & Development Office and others, ‘UK Holds China State-Affiliated Organisations and Individuals Responsible for Malicious Cyber Activity’ (25 March 2024) https://www.gov.uk/government/news/uk-holds-china-state-affiliated-organisations-and-individuals-responsible-for-malicious-cyber-activity accessed 31 July 2026

France, Ministry of the Armies, *International Law Applied to Operations in Cyberspace* (9 September 2019)

Google Threat Intelligence Group, 'Read Our New Report on AI-powered Threats and Our Latest Defenses' (11 May 2026) https://blog.google/innovation-and-ai/infrastructure-and-cloud/google-cloud/google-threat-intelligence-group-report/ accessed 5 August 2026

Government of Canada, *International Law Applicable in Cyberspace* (22 April 2022)

Government of the Netherlands, 'Letter to the Parliament on the International Legal Order in Cyberspace' (5 July 2019)

Herman M and others, *NIST Cloud Computing Forensic Reference Architecture* (NIST SP 800-201, July 2024)

—— *NIST Cloud Computing Forensic Science Challenges* (NISTIR 8006, August 2020)

HM Government, *Response to the House of Lords AI in Weapon Systems Committee Report* (February 2024)

House of Lords AI in Weapon Systems Committee, *Proceed with Caution: Artificial Intelligence in Weapon Systems* (HL 2023–24, 16)

ICRC, *ICRC Position on Autonomous Weapon Systems* (12 May 2021)

International Code of Conduct Association, *International Code of Conduct for Private Security Service Providers* (amended December 2021)

International Law Commission, *Report of the International Law Commission: Seventy-fifth Session* (2024) UN Doc A/79/10

—— *Report of the International Law Commission: Seventy-sixth Session* (2025) UN Doc A/80/10

—— *Report of the International Law Commission: Seventy-seventh Session* (2026) UN Doc A/81/10

Kent K and others, *Guide to Integrating Forensic Techniques into Incident Response* (NIST SP 800-86, August 2006)

Kent K and Souppaya M, *Guide to Computer Security Log Management* (NIST SP 800-92, September 2006)

Liu F and others, *NIST Cloud Computing Reference Architecture* (NIST SP 500-292, September 2011)

Ministry of Defence, *Defence Artificial Intelligence Strategy* (15 June 2022)

National Cyber Security Centre, 'Logging Made Easy with CISA' https://www.ncsc.gov.uk/information/logging-made-easy accessed 5 August 2026

—— *The Near-term Impact of AI on the Cyber Threat* (24 January 2024) https://www.ncsc.gov.uk/report/impact-of-ai-on-cyber-threat accessed 5 August 2026

—— 'UK Calls Out China State-Affiliated Actors for Malicious Cyber Targeting of UK Democratic Institutions and Parliamentarians' (25 March 2024) https://www.ncsc.gov.uk/news/china-state-affiliated-actors-target-uk-democratic-institutions-parliamentarians accessed 16 October 2026

National Cyber Security Centre, Cybersecurity and Infrastructure Security Agency and others, *Defending Against China-Nexus Covert Networks of Compromised Devices* (AA26-113A, 23 April 2026) https://www.cisa.gov/news-events/cybersecurity-advisories/aa26-113a accessed 5 August 2026

National Institute of Standards and Technology, *Secure Software Development Framework (SSDF) Version 1.1* (NIST SP 800-218, February 2022)

—— *Secure Software Development Practices for Generative AI and Dual-Use Foundation Models* (NIST SP 800-218A, July 2024)

National Telecommunications and Information Administration, *The Minimum Elements for a Software Bill of Materials* (12 July 2021)

Nelson A and others, *Incident Response Recommendations and Considerations for Cybersecurity Risk Management* (NIST SP 800-61 rev 3, April 2025)

New Zealand Ministry of Foreign Affairs and Trade, *The Application of International Law to State Activity in Cyberspace* (1 December 2020, updated 17 June 2025)

Office of the United Nations High Commissioner for Human Rights, 'Submission of the Office of the United Nations High Commissioner for Human Rights' (Ad Hoc Committee, reconvened concluding session, 22 July 2024)

Organization for Security and Co-operation in Europe, Decision No 1202, 'OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies' (10 March 2016) PC.DEC/1202

SLSA, 'Supply-chain Levels for Software Artifacts Specification v1.2' (24 November 2025) https://slsa.dev/spec/v1.2/ accessed 17 October 2026

Special Representative of the Secretary-General on the Issue of Human Rights and Transnational Corporations and Other Business Enterprises, 'Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework' (21 March 2011) UN Doc A/HRC/17/31, annex

Swiss Confederation and ICRC, *The Montreux Document on Pertinent International Legal Obligations and Good Practices for States related to Operations of Private Military and Security Companies during Armed Conflict* (17 September 2008)

UN Human Rights Committee, General Comment No 34, 'Article 19: Freedoms of Opinion and Expression' (12 September 2011) UN Doc CCPR/C/GC/34

UNGA, 'Official Compendium of Voluntary National Contributions on the Subject of How International Law Applies to the Use of Information and Communications Technologies by States' (13 July 2021) UN Doc A/76/136

—— 'Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security: Final Substantive Report' (10 March 2021) UN Doc A/AC.290/2021/CRP.2

—— 'Report of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes' (2024) UN Doc A/79/196

—— 'Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security' (14 July 2021) UN Doc A/76/135

US Department of Justice, 'Cloud Act Agreement between the Governments of the US, United Kingdom of Great Britain and Northern Ireland' (updated 11 August 2023) https://www.justice.gov/criminal/criminal-oia/cloud-act-agreement-between-governments-us-united-kingdom-great-britain-and-northern accessed 5 August 2026

—— 'Justice Department Charges 12 Chinese Contract Hackers and Law Enforcement Officers in Global Computer Intrusion Campaigns' (5 March 2025) https://www.justice.gov/opa/pr/justice-department-charges-12-chinese-contract-hackers-and-law-enforcement-officers-global accessed 31 July 2026

—— *Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act* (April 2019)

—— 'Seven Hackers Associated with Chinese Government Charged with Computer Intrusions Targeting Perceived Critics of China and US Businesses and Politicians' (25 March 2024) https://www.justice.gov/archives/opa/pr/seven-hackers-associated-chinese-government-charged-computer-intrusions-targeting-perceived accessed 16 October 2026

—— 'US Government Disrupts Botnet People's Republic of China Used to Conceal Hacking of Critical Infrastructure' (31 January 2024) https://www.justice.gov/opa/pr/us-government-disrupts-botnet-peoples-republic-china-used-conceal-hacking-critical accessed 5 August 2026