

# The Shadow Architecture of Sovereignty: Intelligence Services and the Governance of Cloud Diplomacy in International Law

Doctoral Researcher **Reza ABBASI**<sup>1</sup>

## **Abstract**

*The emergence of cloud computing as the structural substrate of contemporary statecraft has generated a new and insufficiently theorised domain of international relations: cloud diplomacy. This article argues that intelligence services occupy a peculiar yet constitutive role within this domain — functioning simultaneously as instruments of statecraft, threats to diplomatic confidence, and architects of the normative frameworks through which states negotiate digital sovereignty. Drawing on international law, intelligence studies, and theories of digital statecraft, the article develops an original tripartite analytical framework: intelligence services as (i) collectors of diplomatic advantage through cloud-based surveillance, (ii) disruptors of inter-state trust and the multilateral governance of data infrastructure, and (iii) normative entrepreneurs shaping the legal architecture that governs cross-border data flows. The article examines three critical junctures — the post-Snowden international order, the extraterritorial reach of the United States CLOUD Act (2018), and the Huawei 5G infrastructure contestation — as empirical anchors for the theoretical argument. It concludes that existing frameworks of international law are inadequate to address the structural power that intelligence services exercise in the cloud diplomacy arena, and proposes a set of de lege ferenda reforms oriented toward a principle of digital sovereign accountability.*

**Keywords:** cloud diplomacy, intelligence services, digital sovereignty, CLOUD Act, cyber espionage, international law.

**JEL Classification:** K33

**DOI:** <https://doi.org/10.62768/ADJURIS/2026/7/04>

## **Please cite this article as:**

Abbasi, Reza. “The Shadow Architecture of Sovereignty: Intelligence Services and the Governance of Cloud Diplomacy in International Law.” In *Comparative and International Law in an Era of Global Transformation: Sovereignty, Justice, Cooperation, and Emerging Technologies*, edited by Liliana Tymchenko and Paulina Guli Hoti, 63–78. ADJURIS – International Academic Publisher, 2026.

<https://doi.org/10.62768/ADJURIS/2026/7/04>

---

<sup>1</sup> Reza Abbasi - Faculty of Law and Political Science, University of Szeged, Hungary. ORCID: <https://orcid.org/0009-0005-0408-0452>. E-mail: rezaabbasi567@yahoo.com.

## 1. Introduction: The Intelligence Dimension of Cloud Diplomacy

The cloud is not neutral. Beneath the reassuring metaphor of weightlessness and universal access lies a physical and political infrastructure of extraordinary consequence: submarine cables traversing ocean floors, server farms concentrated in a handful of jurisdictions, routing protocols that make no concession to national borders, and intelligence services that have recognised in all of this a terrain of both opportunity and vulnerability. Cloud diplomacy — the conduct of diplomatic relations through, about, and in response to cloud-based digital infrastructure — has become one of the defining features of twenty-first century international relations, yet it remains under-theorised in the legal and political science literature.

This article addresses that gap. It begins from the proposition that intelligence services are not peripheral actors in cloud diplomacy but rather constitutive ones. The architecture of the cloud — its technical protocols, governance arrangements, and legal frameworks — has been shaped to a significant degree by the interests, capabilities, and normative interventions of state intelligence agencies.<sup>2</sup> This is not a marginal observation. It is the central claim: that any adequate theory of cloud diplomacy must account for the intelligence dimension, and that any adequate theory of intelligence law must account for the cloud.

The argument proceeds in six parts. The first section establishes the conceptual framework, defining cloud diplomacy and situating it within the broader literature on digital statecraft and cyber diplomacy. The second section examines intelligence services as actors of digital statecraft. The third section surveys the legal architecture governing intelligence operations in cloud environments. The fourth section develops the tripartite analytical framework — intelligence as collector, disruptor, and normative entrepreneur. The fifth section applies this framework to three empirical junctures. The sixth and concluding section draws implications for international law reform.

This article operates at the intersection of international law and political science, deploying doctrinal, theoretical, and case-analytical methods. It does not aim to produce a comprehensive survey of intelligence law or of cloud governance; rather, it aims to demonstrate their structural interdependence—a relationship that has been addressed only in fragments in the existing scholarship.<sup>3</sup>

---

<sup>2</sup> Richard J. Aldrich and John Kasuku, “Escaping from American Intelligence: Culture, Ethnocentrism and the Anglosphere,” *International Affairs* 88, no. 5 (2012): 1009–1028, <https://doi.org/10.1111/j.1468-2346.2012.01116.x>.

<sup>3</sup> Peter Gill and Mark Phythian, *Intelligence in an Insecure World*, 2nd ed. (Cambridge: Polity Press, 2012).

## 2. Conceptualising Cloud Diplomacy: Beyond the Digital Metaphor

The concept of cloud diplomacy is of recent coinage and its contours remain contested. In its narrowest usage, it refers to the diplomatic negotiations between states and between states and technology corporations concerning the governance, jurisdiction, and security of cloud computing infrastructure.<sup>4</sup> In a broader and theoretically more productive sense, however, cloud diplomacy encompasses the full range of diplomatic activities that are mediated, enabled, or constrained by cloud-based digital infrastructure: communications between foreign ministries, the storage of sensitive diplomatic cables, the conduct of intelligence liaison, and the exercise of soft power through data-dependent platforms.

This broader conception has significant analytical advantages. It captures the extent to which digital infrastructure has become constitutive of, rather than merely instrumental to, contemporary diplomacy. Nye's foundational account of soft power anticipated some aspects of this transformation, but could not have foreseen the degree to which information architecture would itself become a site of power contestation.<sup>5</sup> More recent scholarship on cyber diplomacy has begun to address this, emphasising the emergence of norms, institutions, and practices governing state behaviour in cyberspace.<sup>6</sup>

Cloud diplomacy, as conceptualised here, is irreducibly relational. It describes not merely what states do in the cloud, but how the cloud structures what states can do, know, and conceal from one another. This relational quality is what connects cloud diplomacy to intelligence services in a theoretically interesting way. Intelligence agencies are, in essence, institutional mechanisms for managing informational asymmetries between states.

The concept of digital sovereignty provides an important connecting thread. Digital sovereignty — broadly defined as the capacity of a state to exercise effective authority over data, digital infrastructure, and cyber activities within or associated with its territory — has emerged as a central preoccupation of international relations and international law.<sup>7</sup> Intelligence services are simultaneously the primary beneficiaries of weaker forms of digital sovereignty

---

<sup>4</sup> André Barrinha and Thomas Renard, "Cyber-diplomacy: The Making of an International Society in the Digital Age," *Global Affairs* 3, nos. 4–5 (2017): 353–364, <https://doi.org/10.1080/23340460.2017.1414924>.

<sup>5</sup> Joseph S. Nye Jr., *Soft Power: The Means to Success in World Politics* (New York: PublicAffairs, 2004).

<sup>6</sup> Barrinha and Renard, "Cyber-diplomacy," 354; Jovan Kurbalija, *An Introduction to Internet Governance*, 7th ed. (Geneva: DiploFoundation, 2016).

<sup>7</sup> Anu Bradford, *The Brussels Effect: How the European Union Rules the World* (Oxford: Oxford University Press, 2020), <https://doi.org/10.1093/oso/9780190088583.001.0001>; Mauro Santaniello, "Attributes of Digital Sovereignty: A Conceptual Framework," *Geopolitics* 31, no. 2 (2026): 788–809, <https://doi.org/10.1080/14650045.2025.2521548>.

in other states and the primary drivers of stronger forms of digital sovereignty in their own. This paradox is central to any understanding of the role of intelligence in cloud diplomacy.

Theoretically, cloud diplomacy invites engagement with constructivist accounts of norm formation, realist accounts of structural power, and critical accounts of surveillance capitalism.<sup>8</sup> The argument advanced here does not align exclusively with any single tradition; rather, it draws on each to illuminate different dimensions of a complex phenomenon. The realist insight that states pursue informational advantage is essential but insufficient. The constructivist insight that norms shape state behaviour even in the realm of intelligence is equally important. And the critical insight that commercial and state surveillance interests have converged in the cloud era is indispensable for understanding the structural context within which cloud diplomacy occurs.

### 3. Intelligence Services as Actors of Digital Statecraft

Intelligence services have always been instruments of statecraft. Their transformation into instruments of digital statecraft represents not a rupture but an acceleration — a quantitative shift in capability that has produced qualitative changes in the architecture of international relations.<sup>9</sup> The cloud era has endowed signals intelligence (SIGINT) agencies in particular with capabilities of extraordinary scope: the ability to intercept and process communications at scale, to map social networks with granularity, to access the stored records of billions of individuals and institutions, and to influence the technical standards and legal frameworks that govern all of the above.

The signals intelligence agencies that emerged from the Second World War — most notably the National Security Agency (NSA) of the United States, the Government Communications Headquarters (GCHQ) of the United Kingdom, and their partners in the Five Eyes alliance — were designed to exploit analogue communications infrastructure. Their adaptation to the digital environment required sustained institutional investment, legal innovation, and the cultivation of relationships with the private technology sector.<sup>10</sup>

Three dimensions of this transformation are particularly relevant to cloud diplomacy. The first is the shift from targeted to bulk intelligence collection. Pre-

---

<sup>8</sup> Martha Finnemore and Kathryn Sikkink, “International Norm Dynamics and Political Change,” *International Organization* 52, no. 4 (1998): 887–917, <https://doi.org/10.1162/002081898550789>; Kenneth N. Waltz, *Theory of International Politics* (Reading, MA: Addison-Wesley, 1979); Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (New York: PublicAffairs, 2019).

<sup>9</sup> Loch K. Johnson, *National Security Intelligence: Secret Operations in Defense of the Democracies* (Cambridge: Polity Press, 2012); David Omand, *Securing the State* (London: Hurst, 2010).

<sup>10</sup> Gordon Corera, *Intercept: The Secret History of Computers and Spies* (London: Weidenfeld & Nicolson, 2015); Thomas Rid, *Active Measures: The Secret History of Disinformation and Political Warfare* (New York: Farrar, Straus and Giroux, 2020).

digital SIGINT operations were constrained by limited processing capacity. Digital infrastructure has enabled collection at a scale that effectively renders the distinction between targeted and bulk surveillance analytically unstable.<sup>11</sup> This has profound implications for diplomatic communications, which are now systematically exposed to interception by technologically advanced intelligence services.

The second is the internationalisation of intelligence collection through the exploitation of data flows that traverse multiple jurisdictions. Cloud service providers, by the nature of their business model, store and process data in jurisdictions other than those in which it was generated. This creates what Daskal terms 'data in transit' vulnerability: the possibility that data generated in State A, stored in State B, and transiting through State C may be subject to intelligence collection by the authorities of any of those states.<sup>12</sup>

The third is the emergence of intelligence services as participants in, and shapers of, the governance frameworks for digital infrastructure. Through their participation in standards bodies, their influence over domestic legislation with extraterritorial effect, and their engagement with technology corporations, intelligence agencies have become significant actors in the governance of the global digital environment.<sup>13</sup>

#### **4. The Legal Architecture Governing Intelligence in Cloud Environments**

The legal architecture governing intelligence operations in cloud environments is characterised by fragmentation, indeterminacy, and profound asymmetry between domestic authorisation and international constraint. At the domestic level, intelligence agencies in advanced democracies operate under increasingly elaborated statutory frameworks that authorise bulk data collection and the compelled disclosure of cloud-stored data. At the international level, the relevant normative framework remains embryonic and contested.

The Tallinn Manual process, culminating in the publication of Tallinn Manual 2.0 in 2017, represents the most systematic attempt to apply existing international law to cyber operations.<sup>14</sup> The Manual's analysis proceeds from the foundational principle of sovereignty, applying it through the concept of territorial integrity. Rule 4 provides that a State must not conduct cyber operations that violate the sovereignty of another State. Rule 14 addresses internationally

---

<sup>11</sup> Ronald J. Deibert, *Black Code: Inside the Battle for Cyberspace* (Toronto: McClelland & Stewart, 2013), 112–130; Zuboff, *The Age of Surveillance Capitalism*, 88–95.

<sup>12</sup> Jennifer Daskal, "The Un-Territoriality of Data," *Yale Law Journal* 125, no. 2 (2015): 326–398, <https://yalelawjournal.org/article/the-un-territoriality-of-data>.

<sup>13</sup> Omand, *Securing the State*, 220–235.

<sup>14</sup> Michael N. Schmitt, ed., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2nd ed. (Cambridge: Cambridge University Press, 2017), <https://doi.org/10.1017/9781316822524>.

wrongful cyber acts, while Rules 15–18 address attribution and related questions of State responsibility.

These principles leave critical questions unresolved when applied to intelligence collection in the cloud. The first is attribution: given the technical difficulty of definitively attributing cyber operations to state actors, the law of state responsibility faces a serious implementation deficit. The International Law Commission's Articles on State Responsibility (2001) require attribution to a state organ (Art. 4) or to a person or entity exercising governmental authority (Art. 5); the opacity of intelligence operations, combined with the technical sophistication of false-flag operations, makes attribution inherently contestable.<sup>15</sup> The Manual addresses attribution of cyber operations by non-State actors in Rule 17, including conduct carried out pursuant to a State's instructions or under its direction or control, as well as conduct subsequently acknowledged and adopted by the State.<sup>16</sup>

The second unresolved question is the legality of intelligence collection *per se*. The Tallinn Manual experts were divided on whether peacetime intelligence collection that does not rise to the level of a wrongful act constitutes a violation of international law. This doctrinal uncertainty is diplomatically corrosive: the absence of a clear prohibition on cloud-based intelligence collection undermines the foundations of inter-state trust on which diplomacy depends.

The CLOUD Act (Clarifying Lawful Overseas Use of Data Act, 2018) represents a particularly significant development at this intersection. The Act permits US law enforcement and intelligence agencies to compel US-based cloud providers to produce data stored abroad, while establishing a framework for bilateral executive agreements with foreign governments. It has been criticised by European data protection authorities as incompatible with the GDPR, and by legal scholars as asserting extraterritorial jurisdiction without a clear basis in customary international law.<sup>17</sup>

The GDPR, for its part, represents the European Union's assertion of regulatory sovereignty over data processed in connection with EU residents. Its extraterritorial reach creates a direct normative conflict with the CLOUD Act. This conflict was extensively litigated in the Schrems II decision of the Court of Justice of the European Union (Data Protection Commissioner v. Facebook

---

<sup>15</sup> International Law Commission, "Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries," *Yearbook of the International Law Commission* 2, pt. 2 (2001): 26–143, UN Doc. A/56/10.

<sup>16</sup> Schmitt, *Tallinn Manual 2.0*, 94–97 (Rule 17 and commentary).

<sup>17</sup> Clarifying Lawful Overseas Use of Data Act (CLOUD Act), Pub. L. No. 115-141, div. V, 132 Stat. 348 (2018), 18 U.S.C. § 2713; European Data Protection Board and European Data Protection Supervisor, "EDPB-EDPS Joint Response to the LIBE Committee on the Impact of the US CLOUD Act on the European Legal Framework for Personal Data Protection," July 10, 2019, [https://www.edps.europa.eu/data-protection/our-work/publications/opinions/edpb-edps-joint-response-us-cloud-act\\_en](https://www.edps.europa.eu/data-protection/our-work/publications/opinions/edpb-edps-joint-response-us-cloud-act_en).

Ireland Limited and Maximillian Schrems, Case C-311/18, 2020), which invalidated the EU-US Privacy Shield framework on the grounds that US intelligence surveillance laws failed to provide adequate protection for EU data subjects.<sup>18</sup>

The Budapest Convention on Cybercrime (2001) provides a further node in the legal architecture, establishing provisions for the expedited preservation and disclosure of electronic evidence across borders.<sup>19</sup> While primarily oriented toward criminal rather than intelligence matters, its mechanisms have been invoked in intelligence-adjacent contexts, and the development of its Second Additional Protocol (finalised in 2021) has deepened the cross-border data access framework while leaving unresolved the fundamental tension between intelligence collection and data protection norms.

### **5. Intelligence as Collector, Disruptor, and Normative Entrepreneur: A Tripartite Analytical Framework**

The article now develops its principal theoretical contribution: a tripartite analytical framework for understanding the role of intelligence services in cloud diplomacy. The three roles — intelligence as collector, as disruptor, and as normative entrepreneur — are analytically distinct but empirically interrelated. Together, they constitute what the article terms the 'shadow architecture of sovereignty': the set of intelligence-driven practices and frameworks that structure the cloud environment in ways that are largely invisible to the public but profoundly consequential for international relations.

The first role, intelligence as collector, is the most familiar. Intelligence services collect information about foreign states, non-state actors, and transnational threats through the exploitation of cloud-based communications and data infrastructure. The shift from targeted collection to ambient collection — the systematic harvesting of cloud-stored data for retrospective analysis — represents a fundamental change in the relationship between intelligence and diplomacy. Ambassadors, foreign ministers, and heads of state now conduct significant portions of their diplomatic activities through cloud-based platforms whose security cannot be guaranteed.

The implications for international law are significant. The principle of the inviolability of diplomatic communications, enshrined in Article 27 of the Vienna Convention on Diplomatic Relations (1961), was designed for an era in which the principal threat to diplomatic confidentiality was the physical interception of dispatches. Its application to cloud-based diplomatic communications is contested: while the principle of inviolability clearly extends

---

<sup>18</sup> Court of Justice of the European Union, *Data Protection Commissioner v. Facebook Ireland Ltd and Maximillian Schrems (Schrems II)*, Case C-311/18, ECLI:EU:C:2020:559, July 16, 2020.

<sup>19</sup> Council of Europe, *Convention on Cybercrime (Budapest Convention)*, ETS No. 185 (Budapest, November 23, 2001).

to the content of diplomatic communications, its extension to the metadata generated by cloud-based communications is doctrinally unsettled.<sup>20</sup>

The second role, intelligence as disruptor, is less frequently theorised but equally consequential. Intelligence services disrupt cloud diplomacy not only through active operations—the insertion of malware into diplomatic systems, the manipulation of cloud-based communications, the conduct of influence operations — but through the mere awareness that such operations are possible. The chilling effect of intelligence surveillance on diplomatic communication is structurally analogous to the chilling effect of surveillance on free expression identified in the critical literature.<sup>21</sup>

The disruptive role of intelligence services in cloud diplomacy has been most starkly illustrated by the revelations of Edward Snowden in 2013. The exposure of the NSA's PRISM programme produced a diplomatic crisis that affected US relations with European allies, Latin American partners, and developing nations.<sup>22</sup> The diplomatic damage was not principally a function of the specific intelligence collection revealed; it was a function of the demonstration that the foundational infrastructure of cloud diplomacy — the servers, protocols, and legal frameworks of US-based cloud providers — was systematically accessible to US intelligence.

The third role, intelligence as normative entrepreneur, is the most theoretically novel. Finnemore and Sikkink's account of norm entrepreneurship describes the process by which actors with strong organisational platforms promote new norms in international society.<sup>23</sup> Intelligence services have increasingly assumed this role in the governance of digital infrastructure. Through their influence over domestic legislation, their participation in technical standards bodies, and their conduct of intelligence liaison relationships, intelligence agencies have become significant architects of the normative frameworks that govern the cloud.

The intelligence community's role in shaping the CLOUD Act is illustrative. While the Act was formally drafted in response to a Supreme Court case concerning the production of data stored in Ireland, its substantive provisions reflect the longstanding interests and preferences of the intelligence community in establishing a legally coherent regime for cross-border data access that preserves US intelligence advantage while offering sufficient reciprocity to secure allied cooperation.

---

<sup>20</sup> Hans Born and Ian Leigh, *Making Intelligence Accountable: Legal Standards and Best Practice for Oversight of Intelligence Agencies* (Oslo: Publishing House of the Parliament of Norway, 2005), 77–85.

<sup>21</sup> Zuboff, *The Age of Surveillance Capitalism*, 300–315; Deibert, *Black Code*, 145–160.

<sup>22</sup> David P. Fidler, ed., *The Snowden Reader* (Bloomington: Indiana University Press, 2015), 52–69, 96–100, <https://doi.org/10.2307/j.ctt16gh840>; Privacy and Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* (Washington, DC, July 2, 2014), <https://www.pclob.gov/Oversight>.

<sup>23</sup> Finnemore and Sikkink, “International Norm Dynamics,” 897–905.

Similarly, the intelligence community's influence over technical standards represents a form of normative entrepreneurship that operates below the threshold of formal diplomacy but with consequences for the entire global digital environment. The revelation that the NSA had backdoored the Dual\_EC\_DRBG encryption standard illustrates the depth of intelligence community engagement with the technical foundations of cloud security.<sup>24</sup>

## **6. Empirical Anchors: Three Junctures in Intelligence-Cloud Diplomacy**

### **6.1. The PRISM Revelations and the Post-Snowden Diplomatic Order**

The exposure of the NSA's PRISM programme in June 2013 constitutes a watershed moment in the history of cloud diplomacy. The programme, which compelled disclosure from nine major US cloud providers under the authority of Section 702 of the Foreign Intelligence Surveillance Act, enabled the NSA to access the emails, documents, photographs, and communications of foreign nationals stored on US servers.

Three aspects of the post-Snowden diplomatic landscape are particularly instructive. First, the revelations exposed the structural vulnerability of cloud-based diplomacy to intelligence collection. States that had relied on US cloud services for diplomatic communications were forced to recognise that those communications were, in principle, accessible to US intelligence.

Second, the Snowden revelations produced a significant normative response at the international level. The United Nations General Assembly adopted Resolution 68/167 in December 2013, affirming the applicability of international human rights law to digital communications.<sup>25</sup> While non-binding, the resolution represented a significant moment in the development of the *lex digitalis*.

Third, the post-Snowden period witnessed significant diplomatic investment in reducing dependence on US-centred digital infrastructure. Brazil pursued new data-sovereignty measures after the disclosures, while later European digital-sovereignty initiatives included Gaia-X. Germany's De-Mail initiative, however, predates the Snowden disclosures and cannot be treated as a post-Snowden response.<sup>26</sup>

---

<sup>24</sup> Daniel J. Bernstein, Tanja Lange, and Ruben Niederhagen, "Dual EC: A Standardized Back Door," in *The New Codebreakers: Essays Dedicated to David Kahn on the Occasion of His 85th Birthday*, ed. Peter Y. A. Ryan, David Naccache, and Jean-Jacques Quisquater (Dordrecht: Springer, 2016), 256–281, [https://doi.org/10.1007/978-3-662-49301-4\\_17](https://doi.org/10.1007/978-3-662-49301-4_17).

<sup>25</sup> United Nations General Assembly, *The Right to Privacy in the Digital Age*, Resolution 68/167, A/RES/68/167, adopted December 18, 2013.

<sup>26</sup> Fidler, ed., *The Snowden Reader*, 52–69, 157–161; Germany, *De-Mail-Gesetz*, April 28, 2011, BGBl. I 666; Federal Ministry for Economic Affairs and Climate Action (Germany), "The Gaia-X

## 6.2. The CLOUD Act: Extraterritoriality as Diplomatic Architecture

The Clarifying Lawful Overseas Use of Data Act, signed into law in March 2018, represents the most significant US legislative intervention in the governance of cloud data since the Patriot Act. The Act resolves the question of whether US agencies can compel US-based providers to produce data stored abroad by answering it unequivocally in the affirmative, providing that a provider 'shall comply with an obligation to preserve, backup, or disclose the contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber within such provider's possession, custody, or control, regardless of whether such communication, record, or other information is located within or outside of the United States' (18 U.S.C. § 2713).

The Act's diplomatic architecture is sophisticated. By pairing this expansive assertion of jurisdiction with a framework for bilateral executive agreements, it creates a two-tier system of cloud governance: states that have concluded CLOUD Act agreements with the United States gain privileged access to US cloud infrastructure; states that have not remain subject to the full force of US extraterritorial jurisdiction without reciprocal access. This asymmetry is not merely a technical feature of the Act; it is a deliberate diplomatic architecture that uses cloud governance as leverage in bilateral relations.

The European Union's response to the CLOUD Act has been notably ambivalent. The Act conflicts with the GDPR's requirements for lawful data transfers to third countries; Article 48 of the GDPR provides that judgements of courts or tribunals of third countries requiring a transfer of personal data shall be recognised or enforceable only where based on an international agreement.<sup>27</sup> Yet EU member states have been reluctant to foreclose the possibility of CLOUD Act executive agreements, recognising their potential utility for mutual legal assistance. This ambivalence reflects the broader tension in EU cloud diplomacy between the assertion of digital sovereignty and the maintenance of privileged security relationships with the United States.<sup>28</sup>

---

Ecosystem—A Sovereign Data Infrastructure for Europe,” accessed September 12, 2026, <https://www.bmwk.de/Redaktion/EN/Dossier/gaia-x.html>; Andreas Baur, “European Ambitions Captured by American Clouds: Digital Sovereignty through Gaia-X?,” *Information, Communication & Society* 29, no. 2 (2026): 417–434, <https://doi.org/10.1080/1369118X.2025.2516545>.

<sup>27</sup> European Data Protection Board and European Data Protection Supervisor, “EDPB-EDPS Joint Response on the US CLOUD Act,” July 10, 2019; Regulation (EU) 2016/679 (General Data Protection Regulation), art. 48.

<sup>28</sup> European Parliament and Council of the European Union, Regulation (EU) 2016/679 of April 27, 2016 (General Data Protection Regulation), *Official Journal of the European Union* L 119 (May 4, 2016): 1–88, art. 48.

### 6.3 Huawei and the 5G Intelligence Contestation

The contestation over Huawei's participation in 5G network infrastructure — which reached its diplomatic apex between 2019 and 2021 — represents perhaps the clearest illustration of the cloud diplomacy dynamic as a site of intelligence-driven statecraft. The US campaign to exclude Huawei from allied telecommunications networks was conducted primarily in the language of intelligence: the claim that Huawei equipment contained, or could contain, backdoors enabling Chinese intelligence collection from 5G-dependent cloud infrastructure.

The Huawei contestation illustrates all three dimensions of the tripartite framework. As a matter of intelligence collection, the concern was genuine and well-founded: 5G infrastructure would enable whoever controlled its architecture to collect intelligence at an unprecedented scale. As a matter of intelligence disruption, the US campaign — conducted through intelligence sharing with Five Eyes partners, through diplomatic *démarches* to allied governments, and through export control measures — systematically disrupted the commercial and diplomatic relationships that Huawei had developed over two decades. And as a matter of normative entrepreneurship, the campaign produced a set of emerging norms — the 'clean network' framework, the security evaluation requirements adopted by the EU's 5G toolbox — that structurally favour Western intelligence interests.

The Huawei contestation also illustrates the limits of existing international law in governing intelligence-driven cloud diplomacy. The invocation of national security as justification for trade restrictions under the GATT Article XXI security exception created a potentially unlimited carve-out from trade law obligations. The WTO Appellate Body's engagement with the national security exception in Russia — Measures Concerning Traffic in Transit (2019) has begun to subject these claims to scrutiny, but the application of that scrutiny to cloud-specific intelligence claims remains embryonic.<sup>29</sup>

## 7. Toward a Framework of Digital Sovereign Accountability: *De Lege Ferenda* Reflections

The analysis presented above establishes that intelligence services occupy a constitutive role in cloud diplomacy that existing international law is inadequate to govern. Existing frameworks were designed for a world in which intelligence collection was episodic rather than ambient, in which the principal threat to diplomatic communications was physical interception rather than

---

<sup>29</sup> World Trade Organization, *Russia—Measures Concerning Traffic in Transit*, DS512, Panel Report WT/DS512/R, April 5, 2019, <https://doi.org/10.30875/9a582d67-en>.

systematic digital surveillance, and in which the governance of information infrastructure was a technical matter rather than a site of strategic contestation. The cloud era has rendered all of these assumptions obsolete.

The principle of digital sovereign accountability, advanced here as a framework for reform, builds on existing doctrines of state responsibility, sovereignty, and human rights while extending them in three directions. First, it requires states to accept accountability for the intelligence collection activities of their agencies in cloud environments, including activities conducted through the exploitation of domestic legal processes directed at cloud providers rather than through direct cyber intrusions. This extension of the traditional attribution framework acknowledges the structural reality that the CLOUD Act model constitutes a consequential form of intelligence diplomacy that falls outside the scope of the Tallinn Manual's attribution analysis.

Second, the principle requires states to extend the protection of the Vienna Convention on Diplomatic Relations to cloud-based diplomatic communications, including the metadata of those communications. This extension is not textually compelled by the Convention's existing provisions but is normatively required by its foundational purpose: the protection of the confidential character of diplomatic exchanges.<sup>30</sup> In the cloud era, the structural conditions for diplomatic communication include the security of cloud-based channels against intelligence exploitation.

Third, the principle requires the development of a multilateral treaty framework governing cross-border intelligence collection in cloud environments—an instrument that the article designates a Cloud Intelligence Convention. Such a Convention would draw on the Budapest Convention's architecture of mutual legal assistance while extending it to address intelligence collection specifically; it would establish minimum standards of proportionality and necessity for cloud-based surveillance; it would create a mechanism for interstate consultation and dispute resolution concerning intelligence activities with significant cloud diplomacy implications; and it would establish an international monitoring mechanism analogous to the UN Special Procedures system.

The proposal for a Cloud Intelligence Convention will strike some readers as utopian. Yet the history of arms control law, of international environmental law, and of international human rights law suggests that even structurally resistant domains of state behaviour can be progressively constrained by international legal frameworks, provided that the normative case is sufficiently compelling and the diplomatic coalition sufficiently broad.<sup>31</sup> The post-Snowden

---

<sup>30</sup> Vienna Convention on Diplomatic Relations, April 18, 1961, 500 UNTS 95, arts. 27(1)–(2); Eileen Denza, *Diplomatic Law: Commentary on the Vienna Convention on Diplomatic Relations*, 4th ed. (Oxford: Oxford University Press, 2016), 178–190, <https://doi.org/10.1093/law/9780198703969.001.0001>.

<sup>31</sup> Finnemore and Sikkink, “International Norm Dynamics,” 909; Stephen D. Krasner, *Sovereignty*:

diplomatic environment, and the growing recognition among mid-sized and smaller states of their vulnerability to intelligence-driven cloud diplomacy, provides a diplomatic basis for such a coalition that did not exist a decade ago.

In the shorter term, three more modest reforms deserve attention. First, the bilateral executive agreement framework established by the CLOUD Act should be multilateralised, brought within the ambit of a multilateral instrument that establishes baseline standards of data protection and reciprocity. Second, the mandate of the UN Group of Governmental Experts (GGE) on Cyber should be expanded to address intelligence collection in cloud environments explicitly, moving beyond its current focus on military cyber operations. Third, states should adopt domestic legislation requiring intelligence agencies to conduct formal diplomatic impact assessments before initiating cloud-based surveillance programmes affecting allied governments — a procedural safeguard that would ensure that diplomatic consequences were considered at the highest levels of government.

## 8. Conclusions

Intelligence services are not merely participants in cloud diplomacy; they are its shadow architects. Through their collection activities, their disruptive operations, and their normative entrepreneurship, they have shaped the cloud environment in ways that structure the possibilities available to states in their diplomatic interactions. The PRISM revelations demonstrated the scale of intelligence access to cloud-based diplomatic communications. The CLOUD Act institutionalised that access in domestic law with international diplomatic effect. The Huawei contestation transformed the governance of cloud infrastructure into a site of intelligence-driven geopolitical competition. In each case, the intelligence dimension was not peripheral to the diplomatic story; it was central to it.

The analytical framework developed in this article — intelligence as collector, disruptor, and normative entrepreneur — provides a theoretically integrated account of this centrality. It moves beyond the existing literature's tendency to treat intelligence and diplomacy as parallel but separate domains, revealing instead the deep structural interdependence that characterises their relationship in the cloud era.

The principle of digital sovereign accountability represents one possible normative response to this governance deficit. It is advanced not as a comprehensive solution but as a normative orientation: a set of principles that could guide the progressive development of international law in a domain where the existing framework is demonstrably inadequate. The development of that framework is one of the central tasks facing international lawyers and political

scientists in the decades ahead. It is a task whose urgency, in an era of accelerating digital transformation and intensifying geopolitical competition, is difficult to overstate.

The cloud may be ephemeral as metaphor, but it is enduringly material as infrastructure. It connects states, exposes their secrets, and mediates their conflicts. Intelligence services understood this before diplomats did. The task of international law is now to catch up.

## Bibliography

### I. Books and Article

1. Aldrich, Richard J., and John Kasuku. "Escaping from American Intelligence: Culture, Ethnocentrism and the Anglosphere." *International Affairs* 88, no. 5 (2012): 1009–1028. <https://doi.org/10.1111/j.1468-2346.2012.01116.x>.
2. Barrinha, André, and Thomas Renard. "Cyber-diplomacy: The Making of an International Society in the Digital Age." *Global Affairs* 3, nos. 4–5 (2017): 353–364. <https://doi.org/10.1080/23340460.2017.1414924>.
3. Baur, Andreas. "European Ambitions Captured by American Clouds: Digital Sovereignty through Gaia-X?" *Information, Communication & Society* 29, no. 2 (2026): 417–434. <https://doi.org/10.1080/1369118X.2025.2516545>.
4. Bernstein, Daniel J., Tanja Lange, and Ruben Niederhagen. "Dual EC: A Standardized Back Door." In *The New Codebreakers: Essays Dedicated to David Kahn on the Occasion of His 85th Birthday*, edited by Peter Y. A. Ryan, David Naccache, and Jean-Jacques Quisquater, 256–281. Dordrecht: Springer, 2016. [https://doi.org/10.1007/978-3-662-49301-4\\_17](https://doi.org/10.1007/978-3-662-49301-4_17).
5. Born, Hans, and Ian Leigh. *Making Intelligence Accountable: Legal Standards and Best Practice for Oversight of Intelligence Agencies*. Oslo: Publishing House of the Parliament of Norway, 2005.
6. Bradford, Anu. *The Brussels Effect: How the European Union Rules the World*. Oxford: Oxford University Press, 2020. <https://doi.org/10.1093/oso/9780190088583.001.0001>.
7. Corera, Gordon. *Intercept: The Secret History of Computers and Spies*. London: Weidenfeld & Nicolson, 2015.
8. Daskal, Jennifer. "The Un-Territoriality of Data." *Yale Law Journal* 125, no. 2 (2015): 326–398. <https://yalelawjournal.org/article/the-un-territoriality-of-data>.
9. Deibert, Ronald J. *Black Code: Inside the Battle for Cyberspace*. Toronto: McClelland & Stewart, 2013.
10. Denza, Eileen. *Diplomatic Law: Commentary on the Vienna Convention on Diplomatic Relations*. 4th ed. Oxford: Oxford University Press, 2016. <https://doi.org/10.1093/law/9780198703969.001.0001>.
11. Fidler, David P., ed. *The Snowden Reader*. Bloomington: Indiana University Press, 2015. <https://doi.org/10.2307/j.ctt16gh840>.
12. Finnemore, Martha, and Kathryn Sikkink. "International Norm Dynamics and Political Change." *International Organization* 52, no. 4 (1998): 887–917. <https://doi.org/10.1162/002081898550789>.

13. Gill, Peter, and Mark Phythian. *Intelligence in an Insecure World*. 2nd ed. Cambridge: Polity Press, 2012.
14. Johnson, Loch K. *National Security Intelligence: Secret Operations in Defense of the Democracies*. Cambridge: Polity Press, 2012.
15. Krasner, Stephen D. *Sovereignty: Organized Hypocrisy*. Princeton, NJ: Princeton University Press, 1999.
16. Kurbalija, Jovan. *An Introduction to Internet Governance*. 7th ed. Geneva: DiploFoundation, 2016.
17. Mueller, Milton L. *Networks and States: The Global Politics of Internet Governance*. Cambridge, MA: MIT Press, 2010. <https://doi.org/10.7551/mitpress/9780262014595.001.0001>.
18. Nye, Joseph S., Jr. *Soft Power: The Means to Success in World Politics*. New York: PublicAffairs, 2004.
19. Omand, David. *Securing the State*. London: Hurst, 2010.
20. Rid, Thomas. *Active Measures: The Secret History of Disinformation and Political Warfare*. New York: Farrar, Straus and Giroux, 2020.
21. Santaniello, Mauro. "Attributes of Digital Sovereignty: A Conceptual Framework." *Geopolitics* 31, no. 2 (2026): 788–809. <https://doi.org/10.1080/14650045.2025.2521548>.
22. Schmitt, Michael N., ed. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. 2nd ed. Cambridge: Cambridge University Press, 2017. <https://doi.org/10.1017/9781316822524>.
23. Schmitt, Michael N., ed. *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press, 2013.
24. Waltz, Kenneth N. *Theory of International Politics*. Reading, MA: Addison-Wesley, 1979.
25. Zuboff, Shoshana. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: PublicAffairs, 2019.

## II. Legislation and Official Sources

1. Clarifying Lawful Overseas Use of Data Act (CLOUD Act), Pub. L. No. 115-141, div. V, 132 Stat. 348 (2018), codified in relevant part at 18 U.S.C. § 2713.
2. Council of Europe. *Convention on Cybercrime (Budapest Convention)*, ETS No. 185. Budapest, November 23, 2001.
3. European Data Protection Board and European Data Protection Supervisor. "EDPB-EDPS Joint Response to the LIBE Committee on the Impact of the US CLOUD Act on the European Legal Framework for Personal Data Protection." July 10, 2019. [https://www.edps.europa.eu/data-protection/our-work/publications/opinions/edpb-edps-joint-response-us-cloud-act\\_en](https://www.edps.europa.eu/data-protection/our-work/publications/opinions/edpb-edps-joint-response-us-cloud-act_en).
4. European Parliament and Council of the European Union. Regulation (EU) 2016/679 of April 27, 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation). *Official Journal of the European Union* L 119 (May 4, 2016): 1–88.
5. Federal Ministry for Economic Affairs and Climate Action (Germany). "The Gaia-X Ecosystem—A Sovereign Data Infrastructure for Europe." Accessed

- September 12, 2026. <https://www.bmwk.de/Redaktion/EN/Dossier/gaia-x.html>.
6. International Law Commission. “Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries.” *Yearbook of the International Law Commission* 2, pt. 2 (2001): 26–143. UN Doc. A/56/10.
  7. Privacy and Civil Liberties Oversight Board. *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*. Washington, DC, July 2, 2014. <https://www.pclob.gov/Oversight>.
  8. United Nations General Assembly. *The Right to Privacy in the Digital Age*. Resolution 68/167, A/RES/68/167. Adopted December 18, 2013.
  9. Vienna Convention on Diplomatic Relations. April 18, 1961. 500 UNTS 95.
  10. World Trade Organization. *Russia—Measures Concerning Traffic in Transit*, DS512, Panel Report WT/DS512/R, April 5, 2019. <https://doi.org/10.30875/9a582d67-en>.

### III. Cases and Decisions

1. Court of Justice of the European Union. *Data Protection Commissioner v. Facebook Ireland Ltd and Maximillian Schrems (Schrems II)*, Case C-311/18, ECLI:EU:C:2020:559, July 16, 2020.