13

Public–Private Cooperation in Global Security Governance

Entanglement, Infrastructure and the Affordances of Fundamental Rights

DIMITRI VAN DEN MEERSSCHE

13.1 INTRODUCTION: BLURRED BOUNDARIES/NEW COMPOSITIONS

There are many ways in which the presence and growing prominence of private actors in international public governance can be framed or understood.[1] While some portray this in the language of public–private partnerships or functional integration,[2] others, in a Marxist register, have diagnosed the work of international organizations as being guided by and serving a transnational capitalist class of private corporations and financial interests.[3] For those who approach the place of private actors within global governance with a public law sensibility, this blurring of boundaries poses particular problems

[1] I am invoking 'international public governance' in a loose manner here, referring to the multiple ways in which the work of international organizations and the authority these wield can be conceptualized. See, for example, B. Kingsbury, 'The Concept of "Law" in Global Administrative Law' (2009) 20 *European Journal of International Law* 23; A. von Bogdandy, M. Goldmann and I. Venzke, 'From Public International to International Public Law: Translating World Public Opinion into International Public Authority' (2017) 28 *European Journal of International Law* 125.

[2] See, for example, L. Andonova, *Governance Entrepreneurs: International Organizations and the Rise of Global Public–Private Partnerships* (Cambridge University Press, 2017); R. Schmidt, *Regulatory Integration across Borders: Public–Private Cooperation in Transnational Regulation* (Cambridge University Press, 2018).

[3] B. S. Chimni, 'International Institutions Today: An Imperial Global State in the Making' (2004) 15 *European Journal of International Law* 1; N. Mansouri, 'The Firm' (2022) *Völkerrechtsblog*, available at https://voelkerrechtsblog.org/the-firm/ (accessed December 2022); M. Hardt and A. Negri, *Empire* (Harvard University Press, 2000).

of power, influence and the absence of regulatory control.[4] These problematizations and the nature of our legal responses are connected to how we perceive the public and private to be tied together – contractually, transactionally, economically, culturally, ideologically, etc. In line with the ambition in this volume to theorize the ways in which international organizations engage the world (and the world engages international organizations), this chapter studies these dynamics of influence and interrelation from an infrastructural perspective: by tracing emergent – materially and relationally enacted – compositions of power and authority where the boundaries between public and private cannot easily be drawn (and where the need for doing so might dissolve).[5] 'Thinking infrastructurally', with Kingsbury, can help us observe shifts in the logic and location of global governance, while moving beyond the binary public–private divide (and the legal imagination grafted onto it).[6] Before exploring the conceptual and normative dimensions of this approach (Section 13.5), I explore different dimensions of infrastructural change in global security and their effects: infrastructures of data collection and analysis (Section 13.2), policy implementation (Section 13.3) and policy reorientation (Section 13.4). In tracing the material entanglements between international organizations and private actors in the field of global security governance, a key observation is how pre-emptive security and informational capitalism are mutually co-dependent and co-constitutive on an infrastructural level.

13.2 INFRASTRUCTURES OF DATA COLLECTION: EUROPOL AND THE ROLE OF PRIVATE PARTIES

A first case study relates to the recent amendment and expansion of Europol's mandate and how it is tied to an ongoing controversy over the institution's collection and control of vast data troves – a data 'black hole', as *The Guardian* called it.[7] This controversy was sparked by an order of the European Data

[4] See J. Klabbers, 'Transforming Institutions: Autonomous International Organisations in Institutional Theory' (2017) 6 *Cambridge International Law Journal* 105, 116–117; R. Vallejo, 'After Governance? The Idea of Private Administrative Law', in P. Kjaer (ed.), *The Law of Political Economy: Transformation in the Function of Law* (Cambridge University Press, 2020), 320.

[5] B. Kingsbury, 'Infrastructure and InfraReg: On Rousing the International Law "Wizards of Is"' (2019) 8 *Cambridge International Law Journal* 182; G. Sullivan, 'Law, Technology, and Data-Driven Security: Infra-Legalities as Method Assemblage' (2022) 49 *Journal of Law and Society* S31.

[6] Kingsbury, 'Infrastructure and InfraReg'.

[7] *The Guardian*, 'A Data "Black Hole": Europol Ordered to Delete Vast Store of Personal Data', 10 January 2022, available at www.theguardian.com/world/2022/jan/10/a-data-black-hole-europol-ordered-to-delete-vast-store-of-personal-data (accessed December 2023).

Protection Supervisor (EDPS), directed at Europol, to delete data it retained on individuals who have no established links to a criminal activity (described as a 'data subject categorization').[8] This decision concluded an investigation launched by the EDPS in 2019 into Europol's 'big data challenge',[9] which was based on the observation that the use by the organization of 'big data analytics' – the computational processing of large datasets without direct connection to pre-identified criminal activities or suspects – posed 'high risks for data subjects' and could have a 'severe impact on their fundamental rights'.[10] European Digital Rights (EDRi) – an advocacy group working to defend and advance digital rights – described this use by Europol of data mining techniques to 'identify' potential criminals as the EU's 'own Snowden scandal' – the collection and processing of big data as a form of mass surveillance.[11]

Yet, from the perspective of Europol, continued access to this data deluge is essential to develop the analytical capabilities at the heart of its pre-emptive security practices and strategies. These strategic objectives resonate, for example, in the use of new technologies in border security, where, as a study by the EU Parliament noted, 'AI algorithms … [a]part from verifying and identifying known persons … are also used to identify *unknown persons of interest* based on specific data-based *risk profiles*'.[12] This aligns with a much broader trend in security governance, as Gavin Sullivan summarizes, where '[p]atterns or clusters' distilled from large amounts of data are not exclusively 'aimed at targeting "known" threats [but] emerge from correlational associations … between heterogeneous data sources algorithmically analyzed to detect previously "unknown" risks'.[13] This 'politics of possibility', to use Louise Amoore's concept,[14] is reflected in Europol's new task to 'identify[]

[8] See EDPS, *Decision on the Retention by Europol of Datasets Lacking Data Subject Categorisation* (2022), available at https://edps.europa.eu/system/files/2022-01/22-01-10-edps-decision-europol_en.pdf (accessed December 2022).

[9] Ibid., para. 1.2.

[10] Ibid., para. 2.4. *The Guardian* reported that Europol's cache contained an astounding quantity of 'at least 4 petabytes'. See *The Guardian*, 'A Data "Black Hole"'.

[11] EDRi, *The EU's Own 'Snowden Scandal': Europol's Data Mining* (2022), https://edri.org/our-work/the-eus-own-snowden-scandal-europols-data-mining/ (accessed January 2023).

[12] European Parliament, *Artificial Intelligence at EU Borders: Overview of Applications and Key Issues* (2021). Cf. DG Home, *Opportunities & Challenges for the Use of Artificial Intelligence in Border Control, Migration & Security* (2020) (emphases added).

[13] Sullivan, 'Law, Technology, and Data-Driven Security', S41. See also D. Van Den Meerssche, 'Virtual Borders: International Law and the Elusive Inequalities of Algorithmic Association' (2022) 33 *European Journal of International Law* 171.

[14] L. Amoore, *The Politics of Possibility: Risk and Security beyond Probability* (Duke University Press, 2013).

persons . . . who constitute a *high risk* for security' and hinges on an infrastructure through which 'large and complex data sets' can be accessed and analysed.[15] This is also expressed in one of the institution's key tasks: to 'collect, store, process, analyze and exchange information', which has led to some scholars labelling Europol as an 'enormous data processing agency rather than a law enforcing police office'[16] and its description in a report for LIBE (European Parliament's Committee on Civil Liberties, Justice and Home Affairs) as a 'criminal information hub' enabled by a 'computerized information system'.[17] Yet, it is precisely the collection, retention and mining of these 'large and complex data sets' – the retention of petabytes of uncategorized data, data held on people without a 'clearly established link with criminal activity' – that was the subject of the order by the EDPS.[18] In ordering Europol to delete data without appropriate categorization after a limited retention period, this formal intervention directly targeted the use of big data for purposes of 'mass surveillance and the use of predictive policing'.[19]

It is in direct response to this challenge that the legal mandate of Europol was amended in the new regulation adopted in June 2022.[20] Underlining the unique expertise of Europol in 'processing large and complex data sets',[21] the regulation, first of all, retroactively legalizes the continued storage and analysis by the organization of big data troves without appropriate data subject categorization. Article 74b now states that 'Europol may carry out a pre-analysis of [uncategorized] personal data [received before 28 June 2022] for a period of

[15] European Parliament and Council Regulation 2022/991, OJ L 169/1, Article 1. This is reflected in amended Article 4 (1) (r) of the Europol Regulation. See *Consolidated Text: Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol)*, https://eur-lex.europa.eu/eli/reg/2016/794/2022-06-28 (accessed January 2023).

[16] S. Gless, 'Europol', in V. Mitsilegas, M. Bergström and Th Konstadinides (eds.), *Research Handbook on EU Criminal Law* (Edward Elgar, 2016), 465.

[17] LIBE, *Strengthening Europol's Mandate: A Legal Assessment of the Commission's Proposal to Amend the Europol Regulation* (2021). This report was drafted by experts Niovi Vavoula and Valsamis Mitsilegas.

[18] See EDPS, *Decision on the Retention by Europol of Datasets Lacking Data Subject Categorisation*, para. 4.9.

[19] S. Tas, 'Europol's Big Data Challenge: A Neutralisation of the European Watchdog', *The Digital Constitutionalist* (2022), https://digi-con.org/europols-big-data-challenge-a-neutralisation-of-the-european-watchdog/ (accessed January 2023). See also EDRi, 'Secret Negotiations about Europol: The Big Rule of Law Scandal', 31 January 2022.

[20] European Parliament and Council Regulation 2022/991, OJ L 169/1. In the following paragraphs, I also refer to specific articles in the consolidated Europol Regulation (referred to as 'Consolidated Regulation'). See note 15.

[21] European Parliament and Council Regulation 2022/991, OJ L 169/1, Recital 22.

up to 18 months from the date the data were first received'.[22] This retroactive legalization renders the order by the EDPS void and thereby, some argued, poses a distinct rule of law challenge.[23] With the 'amended regulation', the EDPS laments, its 'order to delete these large datasets would become ineffective'.[24] In addition to this retroactive legalization, the new regulation also provides a more structural resolution to Europol's 'big data challenge', in stipulating that the organization can conduct a 'pre-analysis' of uncategorized data – the petabytes of collected raw data targeted by the EDPS – to finds patterns, links and relations with existing criminal activity.[25] In addition, the regulation also provides legal ground for the processing of big data in the context of 'ongoing specific criminal investigation[s] within the scope of Europol's objectives'.[26] The new data processing powers reflected in Article 18 (6a) and 18a, as the Meijers Committee also argued, express a form of technological determinism, where the infrastructural affordances and demands of big data sources and processing capacities alter and expand institutional mandates and powers.[27]

Closely aligned with this storage and 'pre-analysis' of 'large and complex data sets' is the attention in the updated regulation to Europol's development of new algorithmic tools of risk assessment and analysis. As *The Guardian* observed, indeed, the new regulation would 'legalize the data cache and preserve its contents as a testing ground for new AI and machine learning

[22] Consolidated Regulation, Article 74b.

[23] Tas, 'Europol's Big Data Challenge'.

[24] EDPS, 'Amended Europol Regulation weakens data protection supervision', Press Statement, 27 June 2022.

[25] Consolidated Regulation, Article 18 (6a). See also European Parliament and Council Regulation 2022/991, OJ L 169/1, Recital 20 ('Such pre-analysis should take place prior to, and separate from, Europol's data processing for cross-checking, strategic analysis, operational analysis or the exchange of information, and after Europol has established that the data in question are relevant and necessary for the performance of its tasks'). In the LIBE report, these 'large datasets' are defined as 'datasets which, because of the volume, the nature or the format of the data they contain, cannot be processed with regular tools, but require the use of specific tools … in particular digital forensics'. These datasets, the report notes, 'do not allow from the outset to ascertain that all the information contained in these large datasets comply with the limitations prescribed in [the regulation], with the volume of information so big that its content is often unknown until the moment when the analyst extracts relevant entities for their input into the relevant database'. See LIBE, *Strengthening Europol's Mandate*, 34.

[26] Consolidated Regulation, Article 18a. The Meijers Committee has noted in this regard that '[t]he pre-analysis of data and the processing of data in support of a specific criminal investigation are regulated by open norms that are difficult to oversee or supervise by external bodies such as the European Parliament or EDPS'. See Meijers Committee, 'Comment on Proposed Extensive Data Processing Powers for Europol', October 2021, www.commissie-meijers.nl/wp-content/uploads/2021/10/CM2114_EN.pdf (accessed January 2023), 3.

[27] Meijers Committee, 'Comment', 2.

tools'.[28] In the regulation, this resonates in 'Europol's new task to proactively monitor and contribute to research and innovation activities' which is clarified to include 'the development, training, testing and validation of algorithms for the development of tools for the use by law enforcement authorities'.[29] 'Europol should play a key role', the regulation additionally sets out, 'in promoting the development and deployment of ethical, trustworthy and human-centric artificial intelligence'.[30] This extended, proactive mandate in the field of AI development is underlined by the provisions that the automated processing of personal data – including special categories of data that reveal 'racial or ethnic origin, political opinions, religious or philosophical beliefs, ... trade union membership [or a] persons' sex life or sexual orientation' – can, under specific conditions, be justified as a part of research and innovation activities (which could be understood as the development by Europol of computational tools for pre-emptive algorithmic risk assessment).[31] This extended mandate in relation to technological development also situates Europol as a focal point in relation to its member states ('Europol should play a key role in assisting Member States in developing new technological solutions based on artificial intelligence that are relevant to the achievement of Europol's objectives') and to an expanding range of external partners and private parties (as we notice in the creation of 'the EU Innovation Hub for Internal Security as a collaborative network of innovation labs').[32] Intimately intertwined with the objective to mine and analysis big data troves (through the forms 'pre-analysis'), this mandate to proactively develop new AI analytics is a crucial development in the relation of Europol to its members and the outside world.

In order to expand the data sources that Europol can use for these analytical purposes, one of the key innovations of the new regulation, central to my argument here, is that the organization now has the mandate to 'receive personal data from private parties'.[33] 'Private parties', a recital to the regulation amending Europol's mandate notes, 'hold increasing amounts of personal data, including subscriber, traffic and content data, that is potentially relevant for criminal investigations'.[34] This can relate to data held by large tech platforms, financial institutions, airline companies or online service providers. Europol, the regulation observes, 'should have measures in place to facilitate

[28] *The Guardian*, 'A Data "Black Hole"'.

[29] Consolidated Regulation, Article 4 (1) (v).

[30] European Parliament and Council Regulation 2022/991, OJ L 169/1, Recital 49.

[31] Consolidated Regulation, Articles 18 (2) (e), 30 and 33a.

[32] European Parliament and Council Regulation 2022/991, OJ L 169/1, Recitals 48–49.

[33] Ibid., Recital 32, as reflected in amended Article 26.

[34] Ibid., Recital 33.

cooperation with private parties, including with respect to the exchange of information', thereby providing a 'single point of contact' for private parties to share data sets that are scattered across multiple jurisdictions and not easily attributable.[35] In this sense, the provisions of data exchange with private parties have an explicit jurisdictional purpose: Europol's role is to receive and analyse multi-jurisdictional data with the aim of identifying and informing the relevant national authorities. Interestingly, we observe here that the spatial, material and legal disjunction between the digital infrastructures curated by private companies and the territorial jurisdiction of national law enforcement agencies generates a need for the expansion of Europol's legal mandate and the construction of a transnational infrastructure for data exchange.

The new regulation now provides Europol with a mandate to receive data directly from private parties (without member state involvement),[36] to transmit and transfer data to private parties (under specific conditions of necessity and proportionality)[37] and to request data held by private parties (via member states).[38] Importantly, Europol will also be providing the 'infrastructure ... for exchanges between the competent authorities of member states and private parties', even in relation to crimes that do not fall within Europol's objectives (in which case the institution merely serves as a data processor).[39] This is a remarkable expression of how the organization's authority and importance in transnational security governance are tied to the construction and curation of a digital infrastructure through which states, security agencies and private parties are connected. The new regulation underlines and extends these infrastructural interdependencies, which are tied to Europol's existing SIENA platform (Secure Information Exchange Network Application) and its integrated data management concept.[40] This integrated approach entails an 'architectural infrastructure' of data management where separated silos of data were replaced by 'an overarching EU database of criminal data and criminal intelligence' so that 'linkages between data and behavioural patterns may be discerned'.[41] Infrastructural design choices do not only determine Europol's

[35] Ibid.

[36] Consolidated Regulation, Article 26 (2).

[37] Ibid., Article 26 (5).

[38] Ibid., Article 26 (6b) and Recital 39.

[39] Ibid., Article 26 (6c) and Recital 42.

[40] European Parliament and Council Regulation 2016/794, OJ L 135/53, Recital 24.

[41] LIBE, *Strengthening Europol's Mandate*, 18. Indeed, as the 2016 Europol Regulation clarifies, the purpose is to 'use new technologies to process data', to 'swiftly detect links' and to 'have a clear overview of trends', which means that 'Europol databases should be structured in such a way as to allow Europol to choose the most efficient IT structure'. European Parliament and Council Regulation 2016/794, OJ L 135/53, Recital 24.

position within the security landscape and the technological possibilities of intervention, in this sense, but also shape the affordance of legal protection – with the prospects of privacy, purpose limitation and other data protection standards being severely eroded.[42]

In a report on the proposed amendment to Europol's regulation (which has now been adopted) drafted for LIBE, this expanded mandate to directly demand, receive and transfer data from (and to) private parties has been described as 'a considerable paradigm shift from the existing powers of the agency'.[43] The new structure places the institution in direct relation with private parties, thereby circumventing member states, and, the report notes, poses 'significant risks for the protection of fundamental rights, in particular privacy and protection of personal data'.[44] This positioning of Europol as a focal point in a network between states and corporate actors reflects 'the emergence of the trend in the past years to establish direct channels of communication between law enforcement and private parties and foster a public–private partnership'.[45] These material channels, the report notes, 'fundamentally change the powers of the agency and the relationship it has with Member States'.[46] This change is not unique to Europol's engagement with private actors. In its significant Resolution 2396 from 2017 on threats of terrorism and extremism, the UN Security Council underlines the importance of digital infrastructures for pre-emptive practices of 'evidence-based risk assessments' and 'screening procedures'.[47] To this end, the resolution states, the Security Council '[e]ncourages … cooperation with the private sector … especially with information communication technology companies, in gathering digital data'.[48] It is through the alignment and infrastructural integration of private digital platforms with international organizations that the practices and politics of global security governance are being rewritten today.

The changes – and associated controversies – regarding Europol's mandate and pre-emptive security practices show a particular pathway by which international organizations 'engage the world'. The ever-closer cooperation and partnership with private parties, I argued, is not sustained through 'contracting

[42] LIBE, *Strengthening Europol's Mandate*, 18.

[43] Ibid., 30.

[44] Ibid. This is echoed in the analysis of Europol's new regulation by the Meijers Committee, which observed that '[w]hen Europol is empowered to process personal data directly received from private parties, these procedural and other legal requirements that protect individual rights are circumvented'. Meijers Committee, 'Comment', 4.

[45] LIBE, *Strengthening Europol's Mandate*, 30.

[46] Ibid., 26.

[47] UNSC, Resolution 2396 (2017), para. 4.

[48] Ibid., para. 21.

out' specific tasks but through the material configuration of Europol as an infrastructural focal point for the collection, analysis and distribution of data. This consolidation of Europol as a 'criminal information hub' – a 'centre of calculation' where private actors are inserted – significantly alters and extends its mandate. The associated legal problems of privacy, data protection and non-discrimination can be situated in a context of data-driven, pre-emptive security practices, where big data is algorithmically analysed to find patterns, inferences, propensities of 'high risk' behaviour and detect previously unknown threats.[49] Europol's updated regulation provides the legal architecture for precisely this mode of governance: a mandate for the storage and retention of 'large and complex datasets', a pro-active aim of developing algorithms and AI tools to 'pre-analyse' these big data sources with the aim of identifying 'high risk' individuals, and a formal integration of private parties into this emergent data ecology. This paradigm shift, as I argued, is infrastructurally enacted and it is by 'thinking infrastructurally' that the authority of Europol (in relation to states as well as affected individuals) as well as the impact on fundamental rights can be understood. As private platforms are displacing states and international organizations as privileged sites for the creation and accumulation of data about people and populations,[50] we can observe the emergence of global security infrastructures marked by what Mark Andrejevic describes as 'the blurred boundaries between state and consumer surveillance and, thus, between control, convenience, and care'.[51]

[49] This displacement of the rule of law by pre-emptive practices of (algorithmic) risk assessment is underlined in K. Yeung, 'Algorithmic Regulation: A Critical Interrogation' (2018) 12 *Regulation & Governance* 505. This phenomenon is tied to a more general orientation in security practices towards the performative and materially mediated enactment of risk and the governance of unknown threats. Cf. L. Amoore, 'Risk before Justice: When the Law Contests Its Own Suspension' (2008) 21 *Leiden Journal of International Law* 847; Amoore, *The Politics of Possibility*; C. Aradau and T. Blanke, 'Politics of Prediction: Security and the Time/Space of Governmentality in the Age of Big Data' (2017) 20 *European Journal of Social Theory* 373.

[50] This is important considering how, as some have argued, it was precisely this power of counting and collecting that constituted the birth of the modern state and the practice of liberal reform beyond the state. This is powerfully argued in the analysis by Guy Fiti Sinclair who connects these technologies of observation through which the Global South is rendered legible and manageable by international organizations to Foucault's theories on governmentality and biopolitics. G. F. Sinclair, *To Reform the World: International Organizations and the Making of Modern States* (Oxford University Press, 2017).

[51] M. Andrejevic, 'Automating Surveillance' (2019) 17 *Surveillance & Society* 7. Gavin Sullivan has defined these 'global security infrastructures' as 'novel governance constellations that allow diverse actors (states, private platforms, international organizations, and global governance bodies) to collaborate across borders through the extraction, exchange, and interconnection of vast amounts of data for countering potential threats using AI techniques, ADM [i.e.

13.3 INFRASTRUCTURES OF IMPLEMENTATION: HASH-SHARING AND ALGORITHMIC CONTENT MODERATION

In Section 13.2, we observed how private actors are tied to contemporary infrastructures of security governance as important sites of data collection and data sharing. In this section, I map out a different mode of public–private cooperation, in which international organizations involve online platforms and corporate actors to directly implement transnational security policies. This is specifically relevant in relation to practices of countering terrorism online, or – to use the language of the UN CTC (Counter-Terrorism Committee) and CTED (Counter-Terrorism Committee Executive Directorate) – to 'counter terrorist narratives'.[52] Private actors – and particularly large online platforms – are perceived here as essential in containing the use by terrorist and violent extremist organizations of the internet for the purpose of recruitment, propaganda or the dissemination of terrorist and violent extremist content.[53] In the wake of the Christchurch mosque shootings in 2019, which had been accompanied by a white supremacist manifesto and a live-streamed video of the shooting, both of which had been widely shared on online platforms, the Christchurch Call to Action was adopted with the stated aim to 'eliminate terrorist and violent extremist content online'.[54] Remarkably, this call, initiated by New Zealand and France, did not only target states and public actors but also involved obligations for 'online service providers' to – among other commitments – 'take transparent . . . measures seeking to prevent the upload of terrorist and violent extremist content and to prevent its dissemination on social media and similar content-sharing services, including its immediate and permanent removal'.[55] To fulfil these promises, private

automated decision-making] processes, and forms of algorithmic regulation'. Sullivan, 'Law, Technology, and Data-Driven Security', S32.

[52] This is set out specifically in the 'Comprehensive international framework to counter terrorist narratives' developed by the CTC and CTED in 2017. This comprehensive framework is annexed to UNSC, *Letter dated 26 April 2017 from the Chair of the Security Council Committee established pursuant to resolution 1373 (2001) concerning counter-terrorism addressed to the President of the Security Council*, S/2017/375. This comprehensive framework to counter terrorist narratives builds on UNSC, Resolution 2178 (2014); UNSC, Resolution 2354 (2017); UNSC, Resolution 2396 (2017).

[53] This agenda is currently at the heart of the EU's regulation on the dissemination of terrorist content online and the UK's online safety bill. Cf. European Parliament and Council Regulation 2021/784, OJ L 172/79; UK Parliament, Online Safety Bill 220, 2022-23 [as amended on re-committal, in Public Bill Committee].

[54] Christchurch Call (2019), www.christchurchcall.com/assets/Documents/Christchurch-Call-full-text-English.pdf (accessed January 2023).

[55] Ibid.

platforms pledged to make 'cross-industry efforts' by 'investing in and expanding the GIFCT' – the Global Internet Forum to Counter Terrorism (a coalition of large tech corporations with the mission to 'to prevent terrorists and violent extremists from exploiting digital platforms').[56]

The emergence of this forum, and the enrolment of private actors in the struggle to 'counter terrorist narratives' more generally, has a longer lineage. In the *Comprehensive International Framework to Counter Terrorist Narratives* – developed by the CTC and CTED – the UN Security Council stressed that it 'has long noted the importance of public–private partnerships in efforts to counter incitement to commit acts of terrorism',[57] devoting an entire section of the framework to this theme. Underlining the role of ICT and social media platforms, the framework specifically stresses the need to develop novel technological tools to monitor, study, block, filter and remove terrorist content online.[58] This resonates in resolution 2396, where the Security Council stresses the need for 'cooperation with [the] private sector' in countering terrorism online, by 'developing counter-terrorist narratives and through innovative technological solutions'.[59] The Security Council further calls on 'the GIFCT to continue to increase engagement with governments' and points to the UN CTED – ICT4 Peace's initiative of Tech Against Terrorism to 'protect the internet' from terrorist use.[60] Working in close collaboration with the GIFCT network, Tech Against Terrorism – a private actor launched through UN CTED in April 2017 and implemented by the UK-based NGO QuantSpark Foundation – works 'on behalf of the UN CTED to support the global tech industry to tackle terrorist exploitation of their technologies'.

The development of 'innovative technological solutions' is central to the work of both TAT and the GIFCT. Within the context of TAT, the Terrorist Content Analytics Platform (TCAP) was developed to conduct a 'scalable automated data analysis of terrorist content including its symbolism,

[56] Ibid. See GIFCT, 'About', https://gifct.org/about/ (accessed January 2023).

[57] UNSC, *Comprehensive International Framework to Counter Terrorist Narratives*, S/2017/375, para. 8. The strategy summarizes that '[t]he work of the United Nations … in promoting public–private partnerships should be considered a core element of the comprehensive international framework to counter terrorist narratives'. Ibid., para. 14.

[58] Ibid., para. 9–10. The Christchurch call equally underlined the need to develop 'technical solutions to prevent the upload of and to detect and immediately remove terrorist and violent extremist content online'.

[59] UNSC, Resolution 2396 (2017).

[60] Ibid. See TAT, 'About Tech against Terrorism', www.techagainstterrorism.org/about/ (accessed January 2023).

narratives, and metadata, in order to identify and classify at scale'.[61] Working with advanced technological tools of content identification (including automatic web scraping), classification (in line with an institution-specific inclusion list of terrorist organizations), automated notification of affected platforms, and the development of a 'hashing function to create an algebraic record of each content type', TCAP seeks to 'automate[] the swift detection and removal of verified terrorist content'.[62] In this chain of content moderation, TCAP sees a significant role for 'AI driven processes'.[63] The 'hashing function' to which TCAP refers is central to the GIFCT's digital infrastructure for removing online terrorist content: the 'hash-sharing database' (HSDB). The HSDB, the GIFCT states, is 'a shared, safe and secure industry database of perceptual hashes of known images and videos produced by terrorist entities on the UN's designated terrorist groups list, which GIFCT members had chosen to remove'.[64] These 'hashes', the GIFCT's Interim Executive Director and Director of Technology explain, are 'digital signatures' of image or video content that 'cannot be reverse-engineered' to the original files.[65] Access to the HSDB allows all participating platforms to rapidly and proactively review and remove terrorist content from their platforms without having to share the specific content. Considering the intractable and inherently political problem of defining terrorism and violent extremism (in contrast to, for example, opposition or political resistance), the GIFCT's initial standard for inclusion in the database – which is now being expanded – was the relation between online content and entities listed on the UN Security Council consolidated list of designated terrorist entities.[66] The HSDB, in

[61] Cf. N. Bowie, 'Terrorism Databases and Data Sets: A New Inventory' (2021) 15 *Perspectives on Terrorism* 147, 155.

[62] See Terrorist Content Analytics Platform (TCAP), 'How It Works', https://terrorismanalytics.org/about/how-it-works (accessed January 2023).

[63] TCAP, https://terrorismanalytics.org/ (accessed January 2023). This aligns with the observation that 'amidst significant technical advances in machine learning … automated tools are not only being increasingly deployed to fill important moderation functions, but are actively heralded as the force that will somehow save moderation from its existential problems'. R. Gorwa, R. Binns and Ch Katzenbach, 'Algorithmic Content Moderation: Technical and Political Challenges in the Automation of Platform Governance' (2020) 7 *Big Data & Society*. For a more general analysis and critique of algorithmic content moderation, see T. Gillespie, *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions that Shape Social Media* (Yale University Press, 2018).

[64] GIFCT, 'GIFCT's Hash-Sharing Database', https://gifct.org/hsdb/ (accessed January 2023).

[65] 'The hashes used in the GIFCT hash-sharing database are "perceptual hashes" – which means visually similar content creates hashes that are mathematically close to each other'.

[66] The TCAP, more explicitly and controversially, derives this from the 'designation lists of democratic nation states'. See https://terrorismanalytics.org/policies/inclusion-policy (accessed January 2023).

other words, entails a direct response to the engagement by international organizations – with the Security Council and the EU Internet Forum leading the way – of private platforms in the international framework to counter terrorist narratives.

Tied to the standard-setting process of the UN's sanctions list,[67] the HSDB thereby allows platforms to moderate online content at an enhanced speed and scale – with large platforms reporting millions of images and videos corresponding with included hashes having been taken down automatically and quasi instantaneously.[68] The hash-sharing database thus entails an *infrastructural implementation of counterterrorism policy* enacted through the automated filtering of online content with technological tools of hashing and algorithmic content classification. As Gavin Sullivan has argued, this is a regulatory practice that works at an 'architectural level': it does not reactively respond to harmful online behaviour but proactively prevents it from manifesting.[69] This 'infrastructural' or 'architectural' mode regulation through the HSDB entails significant regulatory effects: it allows for automated forms of content moderation; aligns and amplifies the power of large online platforms in what Evelyn Douek has described as 'content cartels';[70] changes the temporal mode of intervention (from reactive to proactive); deflects the legislative demands for more stringent platform regulation; displaces definitional questions and political controversies on the notion of what constitutes terrorism (as elaborated in Section 13.4); and leads to new configurations of global governance – 'bringing', as Sullivan demonstrates, 'states and platforms, and the dynamics of global security and informational capitalism, into novel and productive relation'.[71] To grasp these changes in global security governance, I believe it is important to study digital infrastructures and technologies

[67] G. Sullivan, *The Law of the List: UN Counterterrorism Sanctions and the Politics of Global Security Law* (Cambridge University Press, 2020).

[68] This is also necessary in light of tightening legal obligations for online platforms. The platform governance regulations of the EU – including the EU Regulation on the Dissemination of Online Terrorist Content and the Digital Services Act – now set out a takedown period of only one hour.

[69] See G. Sullivan, 'Infra-legalities: Global Security Infrastructures, Artificial Intelligence and International Law' (unpublished paper, 2023) (draft on file with author). This 'architectural' or 'design-based' regulation, as Bronwen Morgen and Karen Yeung observe, seeks to 'eliminate undesirable behaviour by designing out the possibility for its occurrence'. B. Morgan and K. Yeung, *An Introduction to Law and Regulation: Text and Materials* (Cambridge University Press, 2012), 102.

[70] E. Douek, 'The Rise of Content Cartels', (2020) *Knight First Amendment Institute at Columbia University*, https://knightcolumbia.org/content/the-rise-of-content-cartels (visited 12 March 2025).

[71] See Sullivan, 'Law, Technology, and Data-Driven Security', S37.

such as the HSDB or the TCAP not as passive tools employed for already existing policy agendas but as active agential forces that shape how global security problems are perceived, performed and addressed.[72] The focus hereby shifts from a study of governance *of* infrastructure to governance *by* infrastructure.[73]

Significant legal concerns have been raised regarding the workings of the HSDB as a global security infrastructure. Observing that this technology – and its corporate creation and ownership – entails a form of 'regulatory power over discourse that has never been privately possessed before', Jennifer Cobbe warns for the advent of 'algorithmic censorship' as a mode of governmentality with possibly detrimental effects for 'open and inclusive spaces for communication and discourse'.[74] Danielle Keats Citron, in a similar vein, has observed a 'censorship creep' in how detection tools for child sexual abuse material have entered a much more politically contested domain of online violent extremism.[75] Human rights scholars such as Thiago Dias Oliva, in turn, have signalled specific legal concerns related to algorithmic content moderation in relation to freedom of expression and access to information,[76] while Gavin Sullivan shows that the pre-emptive and proactive logic of the HSDB erodes the rule of law and disables legal accountability and practices of contestation and review.[77] For the purposes of this chapter, however, the key claim is that tools such as the HSDP and the TCAP display a distinct way in which international organizations engage the world: they exemplify the enrolment of corporate actors into practices of global security governance formally set out by international institutions. This enrolment is only in limited ways expressed and implemented in formal legal or institutional forms. It rather unfolds through the construction of emergent socio-technical infrastructures of implementation. In tracing these new infrastructural relations, divisions between public versus private or global versus local can no longer be taken for granted but dissolve into novel, entangled and material compositions of global regulatory power.

[72] Cf. J. Bennett, *Vibrant Matter: A Political Ecology of Things* (Duke University Press, 2009).

[73] See the references in note 5.

[74] J. Cobbe, 'Algorithmic Censorship by Social Platforms: Power and Resistance' (2020) 34 *Philosophy and Technology* 739.

[75] D. Citron, 'Extremist Speech, Compelled Conformity, and Censorship Creep' (2018) 93 *Notre Dame Law Rev*iew 1035, 1050–1051.

[76] Th Dias Oliva, 'Content Moderation Technologies: Applying Human Rights Standards to Protect Freedom of Expression' (2020) 20 *Human Rights Law Review* 607. See also B. Sander, 'Freedom of Expression in the Age of Online Platforms: The Promise and Pitfalls of a Human Rights-based Approach to Content Moderation' (2020) 43 *Fordham International Law Journal* 939.

[77] Sullivan, 'Infra-Legalities'.

13.4 INFRASTRUCTURAL LOGICS: EXPERIMENTALISM AND THE SCRIPTS OF GLOBAL SECURITY GOVERNANCE

Sections 13.2 and 13.3 have pointed to the importance of public–private partnerships in the field of global security governance in relation to practices of data collection and the implementation of an international institutional agenda of countering terrorism online. In this section, I aim to trace the role of private actors, public–private partnerships and their material entanglements to the ways in which global security concerns are perceived, known, enacted and acted upon – to the changing rationalities and logics of security governance. In line with the preceding sections, I argue that these changes are best understood by situating them at a socio-technical or infrastructural level.

The role of private actors in shaping the orientation and agenda of new security practices is obvious in their direct involvement with the drafting of strategies for technology adopted. While the recent strategic report by EU DG Home on *Opportunities and Challenges for the Use of Artificial Intelligence in Border Control, Migration and Security* was drafted by Deloitte,[78] the Frontex report on *Artificial Intelligence-Based Capabilities for the European Border and Coast Guard* was written by the RAND Corporation.[79] This 'resonance' between security practices and corporate risk consultancy, as Louise Amoore has described it,[80] translates itself in the experimental, open-ended and ongoing process by which new data-driven decision-making tools are designed as a series of use cases and modules that can be iteratively 'sequenced', 'adapted' and 'plugged in'.[81] This experimental orientation is explicit in the 2025 UK Border Strategy, which states that 'the private sector must take the lead on border innovation', with the role of government being limited to 'creating an environment that encourages experimentation and technology adoption'.[82] This shift in governance logic, sparked by private actors and sustained by the recourse to new digital technologies, instantiates what Claudia Aradau described as 'experiments without protocols' – a distinct mode of governmentality that is not based on rational plans and formal causal

[78] EU DG Home, *Opportunities and Challenges for the Use of AI in Border Control, Migration and Security* (2020).

[79] Frontex, *Artificial Intelligence-Based Capabilities for the European Border and Coast Guard* (2020).

[80] Amoore, *The Politics of Possibility*.

[81] EU DG Home, *Opportunities and Challenges*, 58–59.

[82] HM Government, *2025 UK Border Strategy* (2020), 29.

criteria but opens up to the space of play of machine learning models.[83] What we observe, then, is the advent in global governance of what Fleur Johns qualifies as 'an open-ended, opportunistic, now-oriented disposition [t]hat has been identified with entrepreneurship'.[84] As private actors become enrolled in (the design of) institutional practices of security governance, we see the emergence of what Johns describes as a 'lean start-up' mentality that 'favours experimentation over elaborate planning … and iterative design over traditional "big design up front"'.[85]

The effects of these emergent infrastructural logics, where adaptiveness and operational actionability figure as central concern,[86] can be observed in the different empirical spheres of Section 13.3. The 'digital forensics' envisaged and employed by Europol in its newly mandated 'pre-analysis' has an explicit orientation, in this sense, towards the iterative and open-ended detection of links, patterns and propensities in 'big data'. The importance of 'new technologies to process data' to 'swiftly detect links [and] trends' was already recognized in Europol's prior regulation,[87] and now resonates in the institutional task to pre-emptively identify 'who constitute[s] a high risk for security' and contribute to the 'development, training, testing and validation of algorithms' necessary for this task.[88] Echoing the language of corporate technology development, the design of new 'solutions based on artificial intelligence' should be supported by an 'EU Innovation Hub for Internal Security as a collaborative network of innovation labs'.[89] The infrastructural and technological developments that are inscribed in this new regulation, in short, express a distinct logic of governing security problems – a logic by which interventions are not (exclusively) guided by pre-determined formal rules and criteria (about who constitutes a risk or what the properties of deviant behaviour precisely entail) but by inferences and 'behavioural patterns' that tools of machine learning are able to distil and render actionable.[90]

[83] C. Aradau, 'Experimentality, Surplus Data and the Politics of Debilitation in Borderzones' (2022) 27 *Geopolitics* 26. The concept of 'experiment without protocol', as Claudia Aradau notes, is coined by Sarah Perret.

[84] F. Johns, 'From Planning to Prototypes: New Ways of Seeing Like a State' (2019) 82 *Modern Law Review* 833, 850. See also D. Van Den Meerssche and G. Gordon, 'Is This the Rhizome? Thinking Together with Fleur Johns' (2022) 33 *Law and Critique* 237.

[85] Johns, 'From Planning to Prototypes', 855.

[86] Cf. D. Van Den Meerssche and G. Gordon, 'The Contemporary Values of Operadiction Regimes', in I. Feichtner and G. Gordon (eds.), *Constitutions of Value* (Routledge, 2023) 236.

[87] European Parliament and Council Regulation 2016/794, OJ L 135/53, Recital 24.

[88] Consolidated Regulation, Article 4 (1) (r) and (v).

[89] European Parliament and Council Regulation 2022/991, OJ L 169/1, Recitals 48–49.

[90] Cf. LIBE, *Strengthening Europol's Mandate*, 18 (noting that '[o]perational effectiveness remains the key goal so that linkages between data and behavioral patterns may be discerned').

A similar development is noticeable in the strategic ambition of EU DG Home 'to harness AI for the benefit of borders, migration and security in Europe'.[91] At the core of this agenda is a focus on 'risk assessment' with the 'general aim to find patterns and cluster individuals for further investigation'.[92] The '[c]lassification categories' guiding this assessment, the strategy further notes, could be 'defined based on a risk threshold or specific indicators' or could be 'less pre-defined where applications are grouped based on some "learned" similarity'.[93] AI would be essential in this process to 'partition data into clusters' and to 'identify patterns which were not observed (as "strange" before)'.[94] This entails a logic of governance inherently tied to the affordances of new technological tools and infrastructures where the identification of security risks – as well as the interventions these invite – results not from fixed legal classifiers of enmity but, at least in part, from continuous and 'unsupervised uncovering of correlations'.[95] This logic resonates in the development of ETIAS (European Travel Information and Authorisation System) which relies on AI to uncover hidden correlations and craft an 'algorithm enabling profiling' to counter security-, illegal immigration- and epidemic risks.[96]

The most explicit manifestation of this changing governance logic, perhaps, relates to the GIFCT and its inclusion policy or taxonomy of what constitutes terrorist and violent extremist context.[97] In the initial stages of the forum and with the aim of finding 'common ground' with the approach taken by states and international organizations,[98] the HSDB would only include hashes associated with terrorist entities on the UN Security Council's Consolidated Sanctions List. We can observe an infrastructural alignment between the

This shift in governance logic is conceptualized and criticized, for example, in E. Isin and E. Ruppert, 'The Birth of Sensory Power' (2020) 7 *Big Data and Society*; R. Amaro, 'Machine Learning, Surveillance and the Politics of Visibility', in B. Vickers and K. Allado-McDowell (eds.), *Atlas of Anomalous AI* (Ignota, 2021); L. Amoore, 'The Deep Border', *Political Geography* (2021) 102547; L. Amoore, 'Machine Learning Political Orders' (2022) 49 *Review of International Studies* 20.

[91] EU DG Home, *Opportunities and Challenges*, 6.

[92] Ibid., 10.

[93] Ibid., 89.

[94] Ibid., 89–90.

[95] Ibid., 90.

[96] Council Regulation 2018/1240, OJ L 236/1, Article 33. See M. Petersmann and D. Van Den Meerssche, 'On Phantom Publics, Clusters and Collectives: Be(com)ing Subject in Algorithmic Times' (2024) 39 *AI and Society* 107.

[97] See GIFCT, *HSDB Taxonomy* (2022), https://gifct.org/hsdb/ (accessed February 2023).

[98] GIFCT, 'Transparency Report' (2020), https://gifct.org/wp-content/uploads/2020/10/GIFCT-Transparency-Report-July-2020-Final.pdf (accessed February 2022). On the legitimacy challenges faced by the GIFCT and the ways in which this 'content cartel' responds to those, see also Douek, 'The Rise of Content Cartels', and Sullivan, 'Infra-Legalities'.

UNSC and GIFCT, in other words, in how the technical content moderation tools of the latter encode the listing practices of the former – a dynamic of automated censorship that renders the controversies over what qualifies as terrorist content (in contrast to political criticism, for example) only more salient. Yet, as Tom Thorley (Director of Technology at GIFCT) observed, the strict reliance on this list imported a set of political and ideological biases embedded in the history of counterterrorism.[99] To overcome this problem of bias and the inability of static state-centred lists to adapt to a changing security landscape, the GIFCT undertook an initiative to broaden its hash-sharing database taxonomy.[100] In expanding the taxonomy of terrorist and violent extremist content, the list-based approach is supplemented with a method that would detect and classify content on the basis of 'behavioural indicators'.[101] The qualification of what constitutes terrorist or violent extremist content would be guided, in this sense, by the distillation of 'behavioural patterns' in real-time data aided by the use of AI. The use of machine learning for content classification differs strongly from the process of hash-matching in that actively extracts and generates features of what qualifies – on a behavioural level – as prohibited content.[102] In one of the proposed tools – the Dynamic Matrix of Extremism and Terrorism (DMET) – the idea is to 'develop models that algorithmically classify groups (or content) into categories' where 'large baskets of indicators would be associated probabilistically with each level [of extremism]' on a continuum from 'partisanship' to 'terrorism'.[103] This classification model is described as 'dynamic', 'iterative' and based on 'cognitive and behavioural cues' that translate in patterns and profiles of extremist content.[104] Interestingly, the designers of the matrix recognize that this behavioural

[99] Cyber5 Podcast, 'Combating Terrorist Messaging on the Open Internet' (2021), www.nisos.com/podcast/ep60/ (accessed February 2022). Cf. E. Saltman and T. Thorley, 'Practical and Technical Considerations in Expanding the GIFCT Hash-Sharing Database', in Global Internet Forum to Counter Terrorism, *Broadening the GIFCT Hash-Sharing Database Taxonomy: An Assessment and Recommended Next Steps* (2021), 16–17; D. Byman and Ch Meserole, 'Expanding the Hash-Sharing Database' in GIFCT, ibid., 28 ('both the U.N. list and national terrorist designation lists are not the result of independent and objective processes but instead reflect political priorities … As a result, nearly all the hashes currently in the database refer to content linked to the Islamic State, Al-Qaeda, the Taliban, and other groups designated as terrorist organizations by the United Nations').

[100] GIFCT, ibid.

[101] GIFCT, ibid., 59.

[102] Cf. Gorwa et al., 'Algorithmic Content Moderation', 5 ('matching and classification have … important differences; while matching requires a manual process of collating and curating individual examples … classification involves inducing generalisations about features of many examples from a given category into which unknown examples may be classified').

[103] GIFCT, *Broadening*, 70.

[104] Ibid.

classification may flag content expressing the 'collective right to self-determination' or instantiating the exercise of fundamental rights – in which case platforms should use 'discretion'.[105] We observe how these international legal questions are now addressed by different actors and in very different terms, mediated by the global infrastructure of hash-sharing and the algorithmic processes of content identification and classification on which it hinges.[106] Yet, while recognizing the normative choices that are involved in this process, the recurring promise in the GIFCT's taxonomy expansion is to classify content in a manner that is 'agnostic to ideology' – a 'value-free modularity' that works around the intractable political problem of qualifying and addressing violent extremist content.[107]

While the current GIFCT taxonomy remains closely centred around the UN's Consolidated Sanctions List, we have now seen the initial introduction of behavioural indicators.[108] This is a conscious project of expanding the taxonomy 'iteratively', which, as Sullivan notes, entails 'an approach to regulation driven less by normative considerations than practical and infrastructural conditions'.[109] In moving beyond the 'biased' list, we can see the emergence of '[AI] processes' which rely 'on a pipeline of real-time, open-source media [to] bas[e] inclusion decisions on behavior rather than ideology or third-party designations'.[110] This shift from designated, state-based, formal lists to an expanded, adaptive taxonomy of behavioural indicators reconfigures the very notion of what terrorism entails and how it can be acted upon. In its orientation towards emergent patterns, behavioural indicators and cognitive cues, this mode of security governance clearly resonates with the ambition of Europol's algorithmic 'pre-analysis' of large and complex datasets, and the strategic aspirations by DG Home to use AI to 'find patterns and cluster individuals for further investigation'. This changing governance rationality is mediated by specific technological possibilities and infrastructural conditions where the public and private are entangled and mutually recomposed. It expresses a distinct logic, which, Fleur Johns has noted, entails an 'attentiveness to emergent patterns of all kinds' – a logic of governance that consists of 'automated dives into vast and shifting oceans of data' where possibilities are being 'worked up iteratively and inductively from the inferences that may be

[105] Ibid., 69.

[106] This is problematized in Sullivan, 'Infra-Legalities'.

[107] GIFCT, *Broadening*, 28 and 68. For a critique of this de-politicising move, see Gorwa et al., 'Algorithmic Content Moderation'; Sullivan, 'Infra-Legalities'.

[108] GIFCT, *HSDB Taxonomy*.

[109] Sullivan, 'Infra-Legalities'.

[110] GIFCT, *Broadening*, 117.

drawn from the data available, as limited or partial as those data may be'.[111] In this distinct mode of governance, Mark Andrejevic argues, the 'homogeneity of discipline is replaced by continual processes of experimentation and environmental modulation calculated to generate more data and ... anticipate and foreclose through intervention'.[112] The diagnosis of this particular governance logic is not primarily about the rising power of private actors or the tremendous opportunity for private profit in this field (although both phenomena are widely documented), but about the ways in which security problems are perceived or addressed. The relationship between international organizations and private parties, in this context, is not one of 'contracting out' public tasks: the practice of data collection and analysis that structures governance routines in the security domain now relies on private infrastructures and 'derives its animus and logic from the market'.[113]

13.5 CONCLUSION: THINKING INFRASTRUCTURALLY: THE MATERIALITY OF RULE AND AFFORDANCES OF RIGHTS

Much can be said about the technologies of security governance and infrastructures of public–private partnership canvassed in Section 13.4. We could focus our critical analyses on the expansion of organizational mandates, the synergies between informational capitalism and security governance, the change in regulatory scripts and rationalities and the associated erosion of fundamental rights. In relation to these important research strands, the intervention of this chapter is a modest one: to grasp the evolving dynamics through which international organizations 'engage the world' – along the invitation in this volume – I want to highlight the importance, as noted by Benedict Kingsbury, of 'thinking infrastructurally'.[114] This mode of thinking, I have argued, allows us to grasp salient changes in global security governance which I described by mapping emergent infrastructures of data collection, policy implementation and standard-setting in this field. It is through infrastructural changes that we see how new entanglements and compositions of public–private ordering emerge – how international organizations 'engage the world' and are materially engaged by it. This perspective opens up a distinct mode of studying the law and governance of (and by) international organizations that disrupts the traditional doctrinal dilemmas and categories within the

[111] Johns, 'From Planning to Prototypes', 850 and 853.

[112] Andrejevic, 'Automating Surveillance', 10.

[113] F. Johns, 'Governance by Data' (2021) 17 *Annual Review of Law and Social Science* 53, 62.

[114] Kingsbury, 'Infrastructures and InfraReg'.

field and holds both methodological and normative potential. In concluding, I touch briefly on both elements.

Thinking infrastructurally about the public–private partnerships that we observed in the extension of Europol's mandate or in the tasks performed by TAT and the GIFCT implies, first, a methodological reorientation to the agency and vibrancy of material and socio-technical actants. Inspired by different strands of new materialism, actor-network theory and science and technology studies, this implies an attentiveness to how material objects, sites or relations produce patterns of social ordering – how they enable and constrain institutional or political projects.[115] Rather than considering the human and non-human – the social and material – as distinct ontological zones, this implies an account of international law and global governance where latent and often invisibilized infrastructural conduits (the 'missing masses' that Bruno Latour refers to) are allowed to (re)appear on stage as active agential elements.[116] This entails what Bowker and Star described as an 'infrastructural inversion': a change in our objects of analysis from formal legal rules or institutional forms to modes of governance by infrastructure.[117]

In my view, this methodological reorientation, which is making inroads in the field of international law,[118] revolves around three dimensions. First, it urges us to recognize the agency of things: the ways in which infrastructures are not only (and never fully) defined by legal or political aspirations but also – and this is the central claim here – reshape, disrupt or displace these aspirations through their own distinct and materially mediated forms of normative ordering. This perspective invites us to approach GIFCT's hash-sharing database or Europol's 'digital forensics' of 'pre-analysis' and infrastructures for public–private data-sharing not as passive tools for already existing governance

[115] Bennett, *Vibrant Matter*; T. Lemke, *The Government of Things: Foucault and the New Materialisms* (NYU Press, 2021).

[116] B. Latour, 'Where Are the Missing Masses? The Sociology of a Few Mundane Artifacts', in W. Bijker and J. Law (eds.) *Shaping Technology/Building Society: Studies in Sociotechnical Change* (MIT Press, 1992), 225; B. Latour, 'From Realpolitik to Dingpolitik: An Introduction to Making Things Public', in B. Latour and P. Weibel (eds.), *Making Things Public: Atmospheres of Democracy* (MIT Press, 2005), 14; A. Leander, 'Locating (New) Materialist Characters and Processes in Global Governance' (2021) 13 *International Theory* 157.

[117] G. Bowker and S. Star, *Sorting Things Out: Classification and Its Consequences* (MIT Press, 1999); Sullivan, 'Law, Technology, and Data-Driven Security'; Sullivan, 'Infra-Legalities'.

[118] Kingsbury, 'Infrastructures and InfraReg'; Sullivan, 'Law, Technology, and Data-Driven Security'; Sullivan, 'Infra-Legalities'; R. Vatanparast, 'The Infrastructures of the Global Data Economy: Undersea Cables and International Law' (2020) 61 *Harvard International Law Journal Online*; J. Hohmann, 'Diffuse Subjects and Dispersed Power: New Materialist Insights and Cautionary Lessons for International Law' (2021) 34 *Leiden Journal of International Law* 585.

projects but as agential participants in emergent governance networks. Second, and related, this reorientation adopts a relational ontology where agency – including regulatory agency in global security governance – is not seen as a property of particular (institutional) actors but as 'a matter of relation, and a process that entails a potentially infinite spectrum of matter around and within us'.[119] In this sense, the a priori public–private binary cannot be maintained: we are witnessing new relational compositions in which material infrastructures perform a pivotal role.[120] Finally, thinking infrastructurally, from my point of view, also implies attention to the performative or world-making dimension of material technologies. This points to how material tools – such as those employed for sensing, ordering and translating data – enact the normative categories and forms of knowledge upon and through which they intervene (as we observed in the category of 'high risk' individuals or the very notion of 'terrorism' itself).[121] From this perspective, thinking infrastructurally would allow us to trace the socio-technical cuts between what *matters* and what is excluded from *mattering*.[122] In short, a methodological orientation towards more-than-human agency, relational ontology and performativity allows us to appreciate the active participation of technological tools and infrastructural compositions in practices of global governance – in how problems are defined, rules implemented, power assembled and distributed. I see mapping and designing these emergent compositions as a critical avenue for international (institutional) law.

In addition to a methodological reorientation, this infrastructural perspective, secondly, also entails a normative agenda. Concerns about the effect of new digital technologies of surveillance and content moderation on human

[119] Hohmann, 'Diffuse Subjects', 595; K. Barad, *Meeting the Universe Halfway: Quantum Physics and the Entanglement of Matter and Meaning* (Duke University Press, 2007), 141, 334 ('agency is not an attribute but the ongoing reconfigurings of the world. The universe is agential intra-activity in its becoming' ... 'Relata do not pre-exist relations'). See also M. Petersmann, 'Response-abilities of Care in More-than-human Worlds' (2021) *Journal of Human Rights and the Environment* 102.

[120] As Gavin Sullivan argued, this perspective allows us to perceive how 'boundaries (public–private, human–machinic, legal–non-legal) [are] redrawn or stabilized through global security infrastructures'. Sullivan, 'Law, Technology, and Data-Driven Security', S37.

[121] D. Van Den Meerssche, 'International Organizations and the Performativity of Measuring States: Discipline through Diagnosis' (2018) 15 *International Organizations Law Review* 168; A. Lang, 'International Lawyers and the Study of Expertise: Representationalism and Performativity', in M. Hirsch and A. Lang (eds.), *Research Handbook on the Sociology of International Law* (Edward Elgar, 2018), 122.

[122] I am inspired here by Barad's 'agential realist elaboration of performativity', which 'allows matter its due as an active participant in the world's becoming'. In Barad, *Meeting the Universe Halfway*, 136.

rights figure prominently in the different initiatives discussed in this chapter. While the GIFCT pledges to a policy of 'countering terrorism while respecting human rights',[123] Europol's new regulation notes that the institution 'should ensure that the development, use and deployment of new technologies are guided by the principles of transparency, explainability, fairness and accountability, do not undermine fundamental rights and freedoms and are in compliance with Union law'.[124] These legal considerations relate specifically to the prevention of bias and the protection of personal data.[125] There is a risk, however, that these repeated normative commitments underestimate how the existence and exercise of human rights are tied to specific material decision-making practices. As Julie Cohen has convincingly observed: 'discourses about fundamental rights have relied on a set of unstated and unexamined assumptions about the material environment's affordance – the conditions of possibility that material environments offer for individual, collective and organizational activity'.[126] The concept of affordances is key here. Originating in design studies and environmental psychology, it has been developed in social theory to highlight how human thought and action is both enabled and conditioned by the properties of material and socio-technical settings.[127] This inspired legal scholars to stress how also the exercise of (fundamental) rights hinges on particular material configurations.[128]

Thinking infrastructurally, in this sense, allows us to critically explore how new technological tools, practices and systems impact (or erode) the exercise of human rights. What is the salience of privacy and purpose limitation principles in relation to Europol's curation and analysis of large and complex datasets or its infrastructures of integrated data management? (as signalled in Section 13.2). How do the proactive algorithmic content moderation practices enabled by the hash-sharing database influence prospects of legal review and

[123] GIFCT, 'Introducing GIFCT Working Group Output' (2022), https://gifct.org/wp-content/uploads/2022/07/GIFCT-22WG-CR-Lifecycle-1.1.pdf (accessed February 2022), 2.

[124] European Parliament and Council Regulation 2022/991, OJ L 169/1, Recital 48.

[125] Ibid.

[126] J. Cohen, *Between Truth and Power: The Legal Constructions of Informational Capitalism* (Oxford University Press, 2019), 246.

[127] As Gavin Sullivan observed, '[a]ffordances are not intrinsic properties of objects, but relationships between objects and users, "jointly determined by the qualities of the object and the abilities of the agent that is interacting"'. Sullivan, 'Law, Technology, and Data-Driven Security', S40.

[128] M. Hildebrandt, *Smart Technologies and the End(s) of Law: Novel Entanglements of Law and Technology* (Edward Elgar, 2016); J. Cohen, 'Affording Fundamental Rights' (2017) 4 *Critical Analysis of Law* 78.

redress? (as Section 13.3 analysed).[129] How can we make anti-discrimination claims against decisions that are not based on fixed normative criteria but on real-time patterns and relational associations detected in data? (as I pointed to in Section 13.4). The infrastructures of governance described in this chapter, in other words, risk to undermine the material conditions for human rights protection – to disable the affordances on which the exercise of rights has always implicitly hinged. The exercise of thinking – and acting – infrastructurally, then, aims to guide our normative attention and interventions to practices of material and socio-technical design, which are aimed at (re)opening possibilities for individual or collective legal and political action and imagination.[130] This practice of critical infrastructural design opens promising pathways for the field of international institutional law beyond its orientation towards institutional design or its preoccupation with public law analogies.

[129] Sullivan, 'Infra-Legalities' (analysing 'how the specific affordances of the hash-sharing database are altering the terrain for human rights and online speech').

[130] A promising opening in this direction was made in a recent symposium in AJIL unbound. See B. Kingsbury, 'Introduction to the Symposium on Infrastructuring International Law' (2023) 117 *AJIL Unbound* 1. There are, of course, many forms and foundations for such infrastructural interventions. I am particularly inspired by projects of critical design and fabulation, inspired, for example, by J. Austin and A. Leander, 'Designing-With/In World Politics: Manifestos for an International Political Design' (2021) 2 *Political Anthropological Research on the International Social Sciences* 83; K. Easterling, 'We Will Be Making Active Form' (2012) 82 *Architectural Design* 58; D. Rosner, *Critical Fabulations: Reworking the Methods and Margins of Design* (MIT Press, 2018).