Review of International Studies (2023), **49**: 1, 125–142
doi:10.1017/S0260210522000365

RIS

RESEARCH ARTICLE

Epistemic fusion: Passenger Information Units and the making of international security

Georgios Glouftsios[1]* and Matthias Leese[2]

[1]School of International Studies, University of Trento, Italy and [2]Department of Humanities, Social and Political Sciences, ETH Zurich, Switzerland
*Corresponding author. Email: georgios.glouftsios@unitn.it

(Received 10 September 2021; revised 22 April 2022; accepted 28 June 2022; first published online 28 September 2022)

Abstract

This article focuses on the control of international mobility through the gathering, processing, and sharing of air travellers' data. While a lot has been written about pre-emptive rationalities of security translated into the functionalities of IT systems used for border controls, we take a step further and investigate how these rationalities are operationalised through data transfer, screening, validation, discarding, profiling, contextualisation, calibration, and adjustment practices. These practices may seem banal and technical; however, we demonstrate how they matter politically as they underpin the making of international security. We do so by analysing the work of Passenger Information Units (PIUs) and retracing how they turn Passenger Name Record (PNR) data into actionable intelligence for counterterrorism and the fight against serious crime. To better understand the work of PIUs, we introduce and unpack the concept of 'epistemic fusion'. This explicates how security intelligence comes into being through practices that pertain to cross-domain data frictions, the contextualisation of data-driven knowledge through its synthesis with more traditional forms of investigatory knowledge and expertise, and the adjustment of the intelligence produced to make it actionable on the ground.

Keywords: Passenger Information Units; Digital Data; Epistemic Fusion; Security; Borders

Introduction

A Passenger Name Record (PNR) file is created every time someone books a flight. It contains, among other things, data on the passenger's identity and contact details, means of payment, seat and luggage information, and the itinerary of the booked journey.[1] These data serve, first and foremost, the commercial purposes of air carriers, specifically in relation to customer management and operations. Over the past decade, PNR data have, however, been additionally turned into a knowledge source for international security. Particularly in the context of the 'war on terror', they have become politically prioritised as a key means of producing intelligence[2] about global mobility patterns and potential threats associated with them. In the European Union (EU), Directive 2016/681 on the use of PNR data 'for the prevention, detection,

[1] For a complete list of categories, see European Union, 'Directive (EU) 2016/681 of the European Parliament and of the Council on the use of Passenger Name Record (PNR) Data for the Prevention, Detection, Investigation and Prosecution of Terrorist Offences and Serious Crime' (Brussels, 2016), p. Annex I.

[2] We use the term 'intelligence' to refer to the practical knowledge that informs international mobility controls for purposes of fighting serious crime and terrorism. While the term originates from the domain of (secretive) information assembly for national security and foreign policy, it has become equally used to describe the actionable knowledge that law enforcement and border control agencies produce through data analysis.

investigation and prosecution of terrorist offences and serious crime' legally obliges air carriers operating extra-EU flights to transmit 19 categories of data stored in their booking systems to state authorities.[3] According to a recent review of the implementation of the Directive, most member states are also using the option to extend the collection of PNR data to intra-EU flights.[4] This means that unprecedented amounts of data are continuously transmitted to state authorities, where they are processed for purposes relevant to international security.

International treaties on the exchange and analysis of PNR data have drawn much public and scholarly attention in the late 2000s and early 2010s[5] and there is continued debate in the EU as to the legality and proportionality of large-scale data collection and repurposing.[6] In the meantime, the low-level bureaucratic and technical implementation processes that define how exactly intelligence is produced from PNR data have been overlooked.[7] There are arguably two reasons for this neglect. Firstly, the association of PNR data with international security has resulted in access limitations for scholars. Secondly, advancements in PNR analytics are relatively recent, at least in the EU. Six years after the adoption of the EU PNR Directive, we are only now witnessing how PNR systems in EU member states are taking shape and how PNR data come to matter in the making of international security. A crucial yet so far under-researched role in this process is occupied by 'Passenger Information Units' (PIUs) set up in each EU member state to analyse PNR data. PIUs are specialised police or intelligence units that, in most cases, consist of technical and operational personnel with expertise in data analytics and information sharing for crime prevention and counterterrorism. PIU staff are also likely to have some experience working for European and international law enforcement agencies, such as Europol or Interpol.

In this article, we study the work of PIUs and retrace how they turn PNR data into intelligence. To do so, we introduce and unpack the concept of *epistemic fusion*. Epistemic fusion explicates how intelligence comes into being through practices that pertain to cross-domain data frictions, the contextualisation of data-driven knowledge through its synthesis with more traditional forms of investigatory knowledge and expertise, and the adjustment of the intelligence produced to make it actionable on the ground. In explicating these practices, epistemic fusion retraces how PIUs channel diverse actors and knowledges and turn them into a single register of intelligence for the fight against serious crime and terrorism. Our analysis contributes to IR literature that has engaged the role of digital data in international security by drawing attention to the importance of data practices and their effects on knowledge and action. The article proceeds as follows. First, we review the literature on the role of digital data in international security, with a particular emphasis on PNR data. We then introduce the concept of epistemic fusion and draw out key pointers for

[3] European Union, 'Directive (EU) 2016/681', Art. 8.

[4] European Commission, 'SWD(2020) 128 Final: Commission Staff Working Document Accompanying the Document Report from the Commission to the European Parliament and the Council on the Review of Directive 2016/681 on the Use of Passenger Name Record (PNR) Data for the Prevention, Detection, Investigation and Proesecution of Terrorist Offences and Serious Crime' (Brussels, 2020), p. 37.

[5] Evelien Brouwer, 'The EU Passenger Name Record System and Human Rights: Transferring Passenger Data or Passenger Freedom?', CEPS Working Document No. 320 (Brussels, 2009); Rocco Bellanova and Denis Duez, 'A different view on the "making" of European security: The EU Passenger Name Record system as a socio-technical assemblage', *European Foreign Affairs Review*, 17:2/1 (2012), pp. 109–24; Javier Argomaniz, 'When the EU is the "norm-taker"?: The Passenger Name Records Agreement and the EU's internalization of US border security norms', *Journal of European Integration*, 31:1 (2009), pp. 119–36.

[6] Elena Carpanelli and Nicole Lazzerini, 'PNR: Passenger Name Record, problems not resolved? The EU PNR conundrum after opinion 1/15 of the CJEU', *Air and Space Law*, 42:4/5 (2017), pp. 377–402; Sara Roda, 'Shortcomings of the Passenger Name Record directive in light of opinion 1/15 of the Court of Justice of the European Union', *European Data Protection Law Review*, 6:1 (2020), pp. 66–83; Julien Jeandesboz, 'Ceci n'est pas un contrôle: PNR data processing and the reshaping of borderless travel in the Schengen area', *European Journal of Migration and Law*, 23:4 (2021), pp. 431–56.

[7] But see William L. Allen and Bastian A. Vollmer, 'Clean skins: Making the e-border security assemblage', *Environment and Planning D: Society and Space*, 36:1 (2017), pp. 23–39; Rocco Bellanova and Marieke de Goede, 'The algorithmic regulation of security: An infrastructural perspective', *Regulation & Governance*, 16:1 (2022), pp. 102–18; Alexandra Hall, 'Decisions at the data border: Discretion, discernment and security', *Security Dialogue*, 48:6 (2017), pp. 488–504.

https://doi.org/10.1017/S0260210522000365 Published online by Cambridge University Press

our analysis. Finally, we empirically reconstruct how PIUs combine different actor perspectives and types of knowledge in intelligence production.

Methodological note

The analysis presented here builds on extensive document analysis and qualitative empirical material gathered between 2020 and 2021 through a series of semi-structured interviews with practitioners involved in the deployment of PNR data analytics. Overall, seven interviews were conducted, some of them set up as group conversations, resulting in 13 interviewees whose positions covered management, operational, and technical perspectives. The selection of respondents was largely prestructured by opportunities for access. The number of agencies directly involved in PNR analytics in the EU is limited. Out of this small group, few were willing to speak with external researchers. Most importantly, we secured access to three PIUs (nine interviewees), with two of them considering themselves at the forefront of analytical capacities among EU member states.

Limited access is a common problem in the empirical study of security actors. Our inquiry can thus only account for the perspectives of these particular PIUs. However, as PIUs exchange experiences and best practices under the coordination of Europol, our interviewees assured us that their colleagues in other EU member states were confronted with similar challenges and were implementing similar processes. Moreover, the perspectives of PIUs were triangulated with those of experts from Europol (one interviewee), the European Commission's DG HOME (two interviewees), and a private company involved in the development of PNR systems (one interviewee). We also attended three webinars organised by an informal network of law enforcement and border control practitioners that focused on the utility of PNR data for mobility controls. Finally, one of us was able to complete the European Union Agency for Law Enforcement Training (CEPOL) online training course on PNR data analysis. Taken together, we believe that our empirical material allows us to draw sufficiently robust conclusions about the data practices of PIUs and their significance for international security.

All interviews were recorded and transcribed or, in cases where no recording was allowed, detailed notes were produced. The resulting text corpus was coded using qualitative data analysis software (MaxQDA). Coding followed an in-vivo approach, that is, initial code categories were created directly from the topics that respondents talked about. The resulting code structure was revised and refined, resulting in a code tree containing 211 coded segments distributed among seven main categories and two levels of subcategories. This structure allowed us to identify relevant clusters and substantiate cross-cutting themes that informed the analysis and conceptual development presented in this article. Per agreement with our informants, all quotations and references have been anonymised to prevent the identification of specific agencies or individuals.

Digital data and international security

Over the past two decades, IR scholars have broadly engaged with the question of how digital data shape international security politics and practices.[8] While it is impossible to review this literature in its totality, we will discuss some key contributions and concepts that allow us to understand the repurposing of PNR data into a source for intelligence production.

[8] See, for example, Louise Amoore and Marieke de Goede (eds), *Risk and the War on Terror* (London, UK and New York, NY: Routledge, 2008); Karen Lund Petersen, 'Risk analysis: A field within security studies?', *European Journal of International Relations*, 18:4 (2011), pp. 693–717; Louise Amoore and Rita Raley, 'Securing with algorithms: Knowledge, decision, sovereignty', *Security Dialogue*, 48:1 (2017), pp. 3–10; Didier Bigo, 'The (in)securitization practices of the three universes of EU border control: Military/navy – border guards/police – database analysts', *Security Dialogue*, 45:3 (2014), pp. 209–25; Mark B. Salter, 'Imagining numbers: Risk, quantification, and aviation security', *Security Dialogue*, 39:2–3 (2008), pp. 243–66; Fleur Johns, 'Global governance through the pairing of list and algorithm', *Environment and Planning D: Society and Space*, 34:1 (2015), pp. 126–49.

https://doi.org/10.1017/S0260210522000365 Published online by Cambridge University Press

PNR systems are, first and foremost, exemplary of an international 'biopolitics of security',[9] that is, the 'sifting' of cross-border flows of people and goods, whereby 'bad' elements are removed from the flow without interrupting the circulation of 'good' ones.[10] The intelligence produced through the analysis of PNR data is used to sort out and arrest the mobilities of subjects considered to be risky while at the same time speeding up and facilitating the journeys of those who are deemed 'bona fide' travellers.[11] William Walters has, in this context, argued that the contemporary border no longer functions as a 'wall designed to arrest all movement' but rather as a 'filter that aspires to reconcile high levels of circulation, transmission and movement with high levels of security'.[12] This is done, partially, based on inferences about potential future individual conduct, for example, assessments of whether someone would be likely to commit a crime or overstay a visa. The security rationale reflected in data analytics is a pre-emptive one that seeks to imagine, speculate upon, and calculate possibilities, thus securing the future 'by anticipating the "next terrorist attack" and apprehending potential criminals before they can strike'.[13] As Louise Amoore puts it, the processing of datasets such as PNR is 'not centred on who we are, nor even on what our data says about us, but on what can be imagined and inferred about who we might be'.[14]

Importantly, PNR files contain both biographical and 'transactional' data categories, that is, 'data generated as a digital by-product of routine transactions between citizens, consumers, business and government'.[15] Transactional data such as information on luggage, frequent flier status, or means of payment support the registration and tracing of passengers' conduct, which is considered crucial for anticipating potential future individual behaviour (as well as for the investigative reconstruction of past conduct). The functionalities of PNR systems – specifically their capacity to screen passengers by matching their data against targeting rules and watchlists, as well as the facilitation of searches in archival data – bring specific individuals (that is, suspects and their associates) to the attention of authorities, thus circumscribing decisions on who to prevent from travelling in the first place and who to check upon arrival. In other words, PNR data delimit decision-making processes on who (and what) comes to be perceived as bona fide or risky by 'generating the bounded conditions of … a border crossing' and 'what good looks like at the border'.[16]

Generally speaking, data analytics in international security are underpinned by the idea that more (and more fine-grained) data would almost by default result in better operational efficacy, as the produced intelligence would be more accurate and reliable. PNR data are, from this perspective, considered a valuable asset, as they include complementary information to information that authorities already have at their disposal. Their commercial origin reveals details and preferences that would otherwise remain inaccessible – for example the decision to buy an airline ticket

[9] Michael Dillon and Luis Lobo-Guerrero, 'Biopolitics of security in the 21st century: An introduction', *Review of International Studies*, 34:2 (2008), pp. 265–92.

[10] Michel Foucault, *Security, Territory, Population: Lectures at the Collège de France, 1977–78* (New York, NY: Palgrave Macmillan, 2007), p. 65.

[11] Matthew B. Sparke, 'A neoliberal nexus: Economy, security and the biopolitics of citizenship on the border', *Political Geography*, 25:2 (2006), pp. 151–80; Matthias Leese, 'Exploring the security/facilitation Nexus: Foucault at the "smart" border', *Global Society*, 30:3 (2016), pp. 412–29.

[12] William Walters, 'Rethinking borders beyond the state', *Comparative European Politics*, 4:2–3 (2006), pp. 141–59 (p. 152).

[13] Claudia Aradau and Tobias Blanke, 'Politics of prediction: Security and the time/space of governmentality in the age of Big Data', *European Journal of Social Theory*, 20:3 (2017), pp. 373–91 (p. 374).

[14] Louise Amoore, 'Data derivatives: On the emergence of a security risk calculus for our times', *Theory, Culture & Society*, 28:6 (2011), pp. 24–43 (p. 28).

[15] Roger Burrows and Mike Savage, 'After the crisis? Big Data and the methodological challenges of empirical sociology', *Big Data & Society*, April–June (2014), pp. 1–6 (p. 2).

[16] Louise Amoore, *Cloud Ethics: Algorithms and the Attributes of Ourselves and Others* (Durham, NC and London, UK: Duke University Press, 2020), p. 4.

https://doi.org/10.1017/S0260210522000365 Published online by Cambridge University Press

through a travel agency or through the airline's website, the choice to combine multiple flights to reach a destination, the selection of a seat and checked-in luggage, or the decision to pay for tickets by cash or by credit card. The more options are offered to passengers to adjust their bookings, and the more decisions they make *vis-à-vis* those options, the more data representing those decisions are generated. PNR data, as Rocco Bellanova and Denis Duez put it, presuppose a 'certain "freedom" in acting "as a passenger"'[17] and form the basis of what Marieke de Goede describes as a chain of security 'whereby commercial data are analysed, collected, reported, shared, moved, and eventually deployed as a basis for intervention by police and prosecution'.[18] In other words, PNR data that serve the commercial interests of airlines are repurposed – or 're-composted'[19] – for the production of surplus-value in the form of security intelligence.

The incorporation of airlines and the IT companies that manage their reservation systems further underlines the changing role of private actors in international security. As de Goede argues, the involvement of private companies in data exchange frameworks should not be seen as evidence for the ongoing privatisation and outsourcing of international security but rather as a 'process of authorisation and appropriation' in which private companies 'reluctantly learn to see the world through a security lens'.[20] Such a shift of focus (from privatisation to appropriation) implies that the interests of private actors may not always align with those of security authorities, and such misalignment might produce tensions in rendering PNR fit for new analytical purposes.[21] More recently, scholars have taken such tensions as a starting point for inquiries into the 'fragility' of data exchange schemes[22] and have pointed to the sometimes intricate and convoluted relations through which intelligence comes into being.[23]

Finally, IR scholars have investigated how data analytics in international security relate to law and ethics, inquiring specifically into the construction of threat profiles with and through data. In most countries, categories such as race, ethnicity, gender, or religion must not be used for sorting and assessment purposes due to their discriminatory nature. However, studies have shown how these categories can often be replaced with proxies in large datasets, thus enabling authorities to circumvent legal restrictions.[24] Moreover, scholars have cautioned that data-driven profiling may result in black-boxed, dynamic, and emergent forms of discrimination that escape the scope of traditional regulatory regimes, as the creation of profiles through data analytics (that is, when algorithms search for patterns in datasets) signifies a turn towards inductive forms of knowledge production.[25] When profiling is done in such a way, the relations between different data categories 'serve as a base for the extrapolation of possible criminal futures'[26] and analytics function as

[17] Bellanova and Duez, 'A different view on the "making" of European security', p. 121.

[18] Marieke de Goede, 'The chain of security', *Review of International Studies*, 44:1 (2018), pp. 24–42 (p. 25).

[19] Rocco Bellanova and Gloria González Fuster, 'Composting and computing: On digital security compositions', *European Journal of International Security*, 4:3 (2019), pp. 345–65.

[20] de Goede, 'The chain of security', p. 26.

[21] Allen and Vollmer, 'Clean skins', pp. 33–4; Bellanova and de Goede, 'The algorithmic regulation of security', p. 2.

[22] Rocco Bellanova and Georgios Glouftsios, 'Controlling the Schengen Information System (SIS II): The infrastructural politics of fragility and maintenance', *Geopolitics*, 27:1 (2020), pp. 160–84.

[23] Louise Amoore, *The Politics of Possibility: Risk and Security Beyond Probability* (Durham, NC and London, UK: Duke University Press, 2013), p. 2; Debbie Lisle and Mike Bourne, 'The many lives of border automation: Turbulence, coordination and care', *Social Studies of Science*, 49:5 (2019), pp. 682–706.

[24] Monique Mann and Tobias Matzner, 'Challenging algorithmic profiling: The limits of data protection and anti-discrimination in responding to emergent discrimination', *Big Data & Society*, 6:2 (2019), pp. 1–11; Alexandra Hall and Jonathan Mendel, 'Threatprints, threads and triggers: Imaginaries of risk in the "war on terror"', *Journal of Cultural Economy*, 5:1 (2012), pp. 9–27.

[25] Amoore, 'Data derivatives'; Matthias Leese, 'The new profiling: Algorithms, black boxes, and the failure of anti-discriminatory safeguards in the European Union', *Security Dialogue*, 45:5 (2014), pp. 494–511.

[26] Mareile Kaufmann, Simon Egbert, and Matthias Leese, 'Predictive policing and the politics of patterns', *British Journal of Criminology*, 59:3 (2019), pp. 674–92 (p. 674).

https://doi.org/10.1017/S0260210522000365 Published online by Cambridge University Press

'instruments of perception … by which subjects and objects of interest are partitioned from a remainder and singled out for attention'.[27]

In light of the increasingly complex ways in which security decisions come into being based on data and analytics, IR scholars have turned to theoretical frameworks that allow for an account of the multiplicity of social and technical elements involved in the production and implementation of intelligence. Especially the notion of assemblage, building on the work of Gilles Deleuze and Félix Guattari[28] and Manuel DeLanda,[29] has been prominently mobilised, as it models social reality through the relations between heterogeneous, networked parts and thus 'offers an approach that is capable of accommodating the various hybrids of material, biological, social and technological components that populate our world'.[30] Work on security and border assemblages highlights how digital data correspond to organisations, processes, and infrastructures, forming dynamic and rarely coherent structures.[31] Thinking along these lines has enabled scholars to account for previously neglected elements in the making of international security, such as remotely located technical personnel or analysts,[32] the architectures of communication infrastructures that allow for information sharing,[33] or the role of technological innovations and the private industry.[34]

Overall, IR scholars have primarily concentrated on the governmental rationales that underpin the use of digital data in international security contexts, the changing actor constellations created by the turn to digital data, and how algorithmically supported decision-making comes into being and unfolds legal and normative consequences. We contribute to this literature by drawing attention to the practices that define how exactly data come to matter through the everyday work of those involved in digitally mediated security knowledge production. IR scholarship can, so we contend, benefit significantly from the study of such practices and insights about the specific ways in which data are transmitted, validated, combined, and finally fitted into larger empirical contexts. IR scholars have already argued that a practice-oriented approach allows capturing and studying how high-level policy and regulation are turned into concrete actions that produce political orders.[35] To understand how international security is informed by PNR data, it is crucial to focus on the work of PIUs. This allows us to account for the 'actions of experts who give security

[27] Louise Amoore and Volha Piotukh, 'Life beyond Big Data: Governing with little analytics', *Economy and Society*, 44:3 (2015), pp. 341–66 (p. 349).

[28] Gilles Deleuze and Félix Guattari, *A Thousand Plateaus: Capitalism and Schizophrenia* (Minneapolis, MN: University of Minnesota Press, 1987).

[29] Manuel DeLanda, *A New Philosophy of Society: Assemblage Theory and Global Complexity* (London, UK: Continuum, 2006).

[30] Michele Acuto and Simon Curtis, 'Assemblage thinking in international relations', in Michele Acuto and Simon Curtis (eds), *Reassembling International Theory: Assemblage Thinking and International Relations* (Basingstoke, UK: Palgrave Macmillan, 2014), pp. 1–16 (p. 2).

[31] Allen and Vollmer, 'Clean skins'; Christophe Sohn, 'Navigating borders' multiplicity: The critical potential of assemblage', *Area*, 48:2 (2016), pp. 183–9.

[32] Amoore, *The Politics of Possibility*; Bigo, 'The (in)securitization practices of the three universes of EU border control'.

[33] Georgios Glouftsios, *Engineering Digitised Borders: Designing and Managing the Visa Information System* (Basingstoke, UK: Palgrave Macmillan, 2021); Julien Jeandesboz, 'Smartening border security in the European Union: An associational inquiry', *Security Dialogue*, 47:4 (2016), pp. 292–309.

[34] Theodore Baird, 'Interest groups and strategic constructivism: Business actors and border security policies in the European Union', *Journal of Ethnic and Migration Studies*, 44:1 (2018), pp. 118–36; James Alexander and Emmanuel-Pierre Guittet, 'Hot Spots of Security High Tech: Mapping Emerging Trends in the International Market of Promotion of Security Technologies', NESTA Working Paper 15/01 (2015), available at: {https://www.nesta.org.uk/documents/392/1501_working_paper_hosset_0.pdf} accessed 20 April 2022.

[35] Emanuel Adler and Vincent Pouliot, 'International practices', *International Theory*, 3:1 (2011), pp. 1–36; Christian Bueger and Frank Gadinger, *International Practice Theory: New Perspectives* (London, UK: Palgrave Macmillan, 2014); Thierry Balzacq, Tugba Basaran, Didier Bigo, Emmanuel-Pierre Guittet, and Christian Olsson, 'Security practices', in Robert A. Denemark and Renée Marlin-Bennett (eds), *The International Studies Encyclopedia Online* (Oxford, UK: Oxford University Press, 2010), n.p.

https://doi.org/10.1017/S0260210522000365 Published online by Cambridge University Press

meaning and identify threats, as well as devices such as algorithms, databases, and risk analysis tools'.[36] Explicating these practices then enables us to understand how PIUs turn a distributed assemblage of social, technical and, importantly, epistemic elements into a single, authoritative register of intelligence for international mobility controls. In the next section, we introduce and unpack the concept of epistemic fusion as an analytical tool that is helpful to understand how PIUs produce intelligence in practice.

Epistemic fusion

The term epistemic fusion takes inspiration from nuclear physics. Fusion is the reaction that combines two hydrogen atoms and transforms them into a single helium atom. As a side effect, this process is productive of energy, as the total mass of the helium atom is less than the mass of the two original hydrogen atoms, leaving the delta as free leftover. Importantly, fusion describes how distinct elements are channelled through a centre from which they emerge in a novel form. Fusion, so we claim, presents a suitable metaphor to conceptualise and study the epistemic work of PIUs. PIUs act, within an otherwise distributed assemblage, as the 'centre of calculation'[37] through which data-driven and other forms of knowledge from different actors and domains are synthesised and turned into intelligence.

Epistemic fusion, in this sense, points to questions of centralisation and governance. Alexander R. Galloway, in his work on Internet governance, starts from the question of how control is possible in the first place in centre-less network structures that are distributed both physically and technically.[38] As he argues, protocol – the standards that enable machines to communicate with each other – can be understood as both the enabler of distributed structures and a tool to govern their functioning. For Galloway, going beyond the purely technical layer, the power of the protocol as a sociotechnical form of governance lies in providing 'a language that regulates flow, directs netspace, codes relationships, and connects life forms.'[39] We suggest that Galloway's work can serve as an analytical point of departure to ask how PIUs act as centres of calculation that lie between and interconnect a multiplicity of private and state actors who, in one way or another, are involved in the making of international security. Although there is undoubtedly a difference between Internet protocol and international security, PIUs channel and fuse heterogeneous data and knowledges, allowing a seemingly decentralised network of actors (airlines, different law enforcement and intelligence agencies) to productively work together.

It is important to emphasise, at this point, that epistemic fusion should not be mistaken for a straightforward process. In their everyday practices, PIUs are faced with various challenges related to: (1) the resolution of data frictions; (2) the contextualisation of data-driven knowledge through its synthesis with more traditional forms of investigatory knowledge and expertise; and (3) the adjustment of intelligence to make it actionable on the ground. Below we discuss these three core aspects of epistemic fusion in more detail.

Paul N. Edwards, in his work on climate modelling, has used the notion of *friction* to show the incompatibilities and resistances that are likely to occur as data are moved and merged across infrastructures and organisations.[40] Data cannot be easily separated from their creation contexts, as they are gathered and processed with particular purposes in mind.[41] These purposes shape

[36] Bueger and Gadinger, *International Practice Theory*, p. 5.

[37] See Kevin D. Haggerty and Richard V. Ericson, 'The surveillant assemblage', *British Journal of Sociology*, 51:4 (2000), pp. 605–22.

[38] Alexander R. Galloway, *Protocol: How Control Exists After Decentralization* (Cambridge, MA: MIT Press, 2004).

[39] Galloway, 'Protocol', p. 244.

[40] Paul N. Edwards, *A Vast Machine: Computer Models, Climate Data, and the Politics of Global Warming* (Cambridge, MA: MIT Press, 2010).

[41] Rob Kitchin, *The Data Revolution: Big Data, Open Data, Data Infrastructures & Their Consequences* (Los Angeles, CA and London, UK, New Delhi/Singapore/Washington, DC: Sage Publications, 2014); Lisa Gitelman (ed.), *'Raw Data' is an*

https://doi.org/10.1017/S0260210522000365 Published online by Cambridge University Press

data's form and content – and changing such purposes ex post facto might lead to considerable misalignment between data properties and new use cases. Friction, in this context, impedes the effective production of knowledge through data and thus makes involved actors 'spend a great deal of time seeking ways to reduce it'.[42] For Edwards, analyses should thus pay attention to 'the costs in time, energy, and attention required simply to collect, check, store, move, receive, and access data'.[43]

Notably, the circulation of data from one organisation or infrastructure to another, while often depicted as seamless from the outside, is not smooth at all, resulting in loss of informational value.[44] Scholars studying data have thus highlighted how they are adapted, recoded, standardised, and harmonised to make them transmittable, computable, and intelligible by different actors.[45] The case of PNR data is pertinent in this regard, as PIUs need to find ways to deal with the frictions that occur by moving PNR data from the commercial sector to international security contexts. A particular challenge for PIUs is how data transmitted by air carriers can be effectively screened and validated to render them suitable for analysis. As we detail below, using PNR data in the fight against terrorism and serious crime means transferring them into an ecosystem that comes with high demands regarding their accuracy and completeness, thus requiring dedicated processes and resources to render data ready for analysis.

Furthermore, epistemic fusion draws attention to how data-driven knowledge is *contextualised through its synthesis with investigative knowledge and expertise*. Mareile Kaufmann et al. have shown how police departments flank pattern recognition algorithms with criminological theories, institutional knowledge, or narrative elements, allowing them to narrow down search parameters and create results that are more likely to correspond to actual criminal phenomena.[46] Similarly, Laurent Bonelli and Francesco Ragazzi have identified how algorithmic analysis in counterterrorism is complemented by several forms of 'low-tech' modes of knowledge production, speaking to deeply rooted institutional habitus.[47] These accounts foreground how data-driven knowledge, while scalable and powerful, becomes contextualised and resonates with more traditional forms of security work. In the case of PNR data, this is reflected in the ways in which PIUs combine insights that are directly derived from patterns in PNR data with experience-based knowledge of international air travel and localised investigative insights provided by other law enforcement and intelligence agencies.

Finally, epistemic fusion speaks to how intelligence becomes *adjusted and turned into action*. As Karine Côté-Boucher shows, there are almost by default structural disconnects between processes of knowledge production and actual decisions and forms of implementation within complex security assemblages.[48] To render intelligence actionable, security actors have to deal with multiple challenges relating to 'fragmentary and unverified data, gaps between decisions and the infrastructures to enact them and disjunctures between frontline data collection and

Oxymoron (Cambridge, MA: MIT Press, 2013); Yanni Alexander Loukissas, *All Data Are Local: Thinking Critically in a Data-Driven Society* (Cambridge, MA: MIT Press, 2019).

[42] Edwards, *A Vast Machine*, p. 84.

[43] Ibid., p. 84.

[44] Christine L. Borgman, *Big Data, Little Data, No Data: Scholarship in the Networked World* (Cambridge, MA and London, UK: MIT Press, 2015).

[45] Evelyn Ruppert, John Law, and Mike Savage, 'Reassembling social science methods: The challenge of digital devices', *Theory, Culture & Society*, 30:4 (2013), pp. 22–46; Annalisa Pelizza, 'Disciplining change, displacing frictions: Two structural dimensions of digital circulation across land registry database integration', *Tecnoscienza: Italian Journal of Science and Technology Studies*, 7:2 (2016), pp. 35–60; Jo Bates, Yu-Wei Lin, and Paula Goodale, 'Data journeys: Capturing the socio-material constitution of data objects and flows', *Big Data & Society*, July–December (2016), pp. 1–12.

[46] Kaufmann, Egbert, and Leese, 'Predictive policing and the politics of patterns'.

[47] Laurent Bonelli and Francesco Ragazzi, 'Low-tech security: Files, notes, and memos as technologies of anticipation', *Security Dialogue*, 45:5 (2014), pp. 476–93.

[48] Karine Côté-Boucher, *Border Frictions: Gender, Generation and Technology on the Frontline* (London, UK and New York, NY: Routledge, 2020).

https://doi.org/10.1017/S0260210522000365 Published online by Cambridge University Press

centralized data analysis'.[49] This observation implies that data-driven intelligence must be fitted into the control ecosystem within which it is supposed to become actionable – otherwise, it might not produce any effects.[50] For example, Simon Egbert and Matthias Leese, in their work on predictive policing, have shown how police analysts, being aware of the limited resources of patrol officers in the field, 'actively tinker with the evaluation criteria in the software configuration to bring the number of alerts down'.[51] Similarly, we detail how PIUs adjust insights about behavioural patterns linked to international travel to accommodate them within existing processes and routines of international mobility controls. Specifically, we explicate how PIUs tweak targeting rules to ensure that the intelligence produced through their deployment is meaningful and that it can be turned into action without creating unnecessary frictions on the ground (for example, delays and disruption of screening procedures at airports caused by an excessive number of hits).

Overall, epistemic fusion allows us to account for how PIUs manage to produce what Annalisa Pelizza has called an 'authentic register', that is, a unified version of information that merges multiple actors and types of knowledge and combines them into a single output.[52] The data practices enacted by PIUs are geared towards combining multiple social, technical, and epistemic elements into an authoritative version of intelligence mobilised in the fight against serious crime and terrorism. In the following, we substantiate these data practices through our empirical material.

Making international security

During a meeting with an EU official, we were intrigued by what they described as the 'syndrome of not knowing' (Interview 1). This refers to the perception that there is still a lack of data on people crossing borders and a constant concern about the effectiveness of tools that security actors use to analyse them. As they framed it: 'People feel reassured when they sit on a pile of data. But the question is: Are you able to make something out of this pile of data? Do you have the analytical capacities to deal with it?' (Interview 1). The syndrome of not knowing can be understood as the *raison d'être* of PIUs. They are set to make something of the pile of data, turning PNR records into intelligence about global mobility patterns and potentially associated threats. In doing so, PIUs must address accuracy and completeness concerns related to cross-domain data transfer, contextualise data-driven knowledge, and make related adjustments so as to render intelligence actionable.

Data frictions

The transmission of PNR data from air carriers to PIUs is the starting point for intelligence production. In theory, data transmission is a straightforward mechanism whereby air carriers choose from a list of communication protocols and data formats[53] and then transfer data directly from their booking systems. In practice, however, our interviewees unanimously pointed out that transmission is characterised by multiple data frictions that can pose major challenges in the subsequent production of intelligence. Generally speaking, frictions are linked to the bad quality of PNR data, referring primarily to inaccuracy and incompleteness. The European Commission has in this regard noted that PNR data are likely to feature misspelled names, misplaced data

[49] Ibid., p. 67.

[50] James Sheptycki, 'Liquid modernity and the police *Métier*: Thinking about information flows in police organisation', *Global Crime*, 18:3 (2017), pp. 286–302.

[51] Simon Egbert and Matthias Leese, *Criminal Futures: Predictive Policing and Everyday Police Work* (London, UK and New York, NY: Routledge, 2021), p. 103.

[52] Pelizza, 'Disciplining change, displacing frictions'.

[53] European Union, 'Commission Implementing Decision (EU) 2017/759 on the Common Protocols and Data Formats to be Used by Air Carriers when Transferring PNR Data to Passenger Information Units' (Brussels, 2017).

https://doi.org/10.1017/S0260210522000365 Published online by Cambridge University Press

elements, or abbreviations and that they are therefore not immediately suited for the production of reliable intelligence.[54] As PIUs try to render PNR data fit for analysis, they are likely to change their form and informational value, engendering considerable repercussions for how 'data derivatives'[55] emerge – that is, risk scores crafted through the algorithmic processing of the digital traces that passengers leave behind when they book a flight.

Frictions related to the inaccuracy and incompleteness of PNR data are predominantly seen as resulting from their self-declaratory origin (that is, data are provided by passengers or travel agencies) and the lack of effective validation mechanisms during the booking process and the actual journey. Our interlocutors clarified that, in most cases, inaccurate or incomplete PNR data are not provided intentionally to deceive the authorities. Rather, data frictions emerge, for example, when passengers produce typos or mix up data fields or when ticket counter personnel try to 'cheat' the booking system with imaginary passport numbers because their customers are in a hurry:

> Sometimes you get 'extra seat' as last name when someone booked an additional seat. So you'll get a Mr Extra Seat who travels on seventy flights simultaneously because the system merged these entries. … Or a passenger buys a ticket at the airport, for a flight with otherwise great data quality. And the guy at the counter enters 11111111 as a passport number so that the system gets a value for that field. For us, these things make it really tough. Completeness levels vary massively, even within flights. (Interview 7)

Data frictions can also be attributed to the competitive nature of the travel business. Travel agencies are often unwilling to transfer complete passenger data to airlines because they can use these data to approach customers directly to promote their services, thus excluding non-carrier operators from the booking process.[56] One interviewee told us that it is common for PNR files to feature a travel agency's email address for all passengers who booked through that agency instead of the passengers' private email addresses (Interview 7). Some non-carrier operators may also transfer only a list of passenger names to airlines without additional information.[57] The political economy of the travel business matters in relation to security since promotional, marketing, and other financial considerations may affect the completeness of the information that is shared and made available to PIUs.

In this regard, it is crucial to highlight that air carriers are not required to validate the PNR data they collect. They are thus not particularly keen on voluntarily guaranteeing the factual accuracy of data as long as they prove sufficient to manage customer needs. Some airlines, especially smaller ones, even collect only a minimum of data, at times including 'only the name and surname of the passenger, combined with the basic information about the flight (date, itinerary)'.[58] As one interviewee summarised: 'The only thing that is interesting for the airline is whether someone paid for this seat. … There are so many fields that are not mandatory, or if they are mandatory there is no check on the quality of the data inserted by the traveller. I could be flying as Mickey Mouse or Osama Bin Laden' (Interview 4). From a business perspective, this makes sense, as any engagement with PNR data beyond operative requirements would only cause additional costs for air carriers while yielding no additional benefits. However, this poses a major problem from a security perspective: inaccurate and unreliable data can lead to faulty intelligence.

The seemingly mundane practices that result in inaccurate and incomplete data are often overlooked in the literature that interrogates the datafication of security. While a lot has been written

[54] European Union, 'SWD(2020) 128 Final', p. 41.

[55] Amoore, 'Data derivatives'.

[56] European Commission, 'SWD(2020) 128 Final', p. 39.

[57] European Commission, 'Feasibility Study on a Centralised Routing Mechanism for Advance Passenger Information (and Passenger Name Records), Volume 1: Main Report' (Brussels, 2019), p. 35.

[58] European Commission, 'SWD(2020) 128 Final', p. 42.

about how data processing tools may contribute to the pre-emption of future risks, there are only a few contributions that inquire directly into how errors[59] and potential malfunctions[60] create data frictions that hinder the production of security intelligence. Such errors and malfunctions are not necessarily generated by the work security actors but by the practices of those who become the targets of security measures (for example, passengers) or by the private actors who become enrolled in international security.

The initial misalignment between PNR data and international security requirements causes what Edwards calls 'frictional costs' that result in 'attempts to recover or correct lost or corrupted data'.[61] What from a professional point of view is usually framed as data quality – that is, the representativeness, completeness, accuracy, consistency, etc. of data – can be understood as a question of trust. For Rob Kitchin, the central question that organisations need to answer regarding the data they work with is: 'Do we believe the integrity of a dataset to tell us something meaningful about the world?'[62] If the answer to this question is no or 'total garbage' (Interview 7), measures need to be implemented to rebuild trust to data. PIUs thus have to put up with what they believe should already have been the task of air carriers: to validate PNR data up to the point where they appear trustworthy enough to inform international security (Interview 6).

The most pertinent practical approaches to dealing with frictions and establishing trust in PNR files include detecting and flagging inaccurate and/or incomplete data, cross-validation with other data sources, and discarding PNR files that cannot easily be salvaged under time pressure. For purposes of detection and flagging, PIUs are developing data screening rules based on experiences acquired since the implementation of PNR systems. In most national cases, these experiences are limited, as PIUs have only recently become operational after a lengthy process of setting up the infrastructures and technical specifications for PNR data transfer. As our interviews told us, PIUs are still studying the characteristics of PNR data to determine where the most common shortcomings appear and how to effectively screen for them in automated ways. One analyst summarised the current progress of their PIU as follows:

> That's a long learning process, lots of work with actual PNR data. … Over time, you learn to identify certain things. A sequential number, 1234567, that's not a reasonable passport number, so we flag that. Two different persons on the same flight with the same passport number, that can't be right. And so we create rules to flag all these things, and we will at some point exchange these rules [with other PIUs]. (Interview 7)

This resonates well with what Debbie Lisle describes as the learning-through-failure mode of doing security, whereby security actors internalise wider organisational norms about the need to learn from previous mistakes.[63] In dealing with data frictions and assembling security knowledge, PIUs learn to detect inaccurate data – data that they may have previously believed to be trustworthy due to the lack of the necessary experience.

Additionally, PIUs cross-validate PNR data with data from other sources, most notably Advance Passenger Information (API) data, illustrating their attempts to fuse disaggregated fragments of information. API data are collected by air carriers during check-in and boarding. They mainly include passengers' biographic data extracted from travel documents and meta-data on

[59] Claudia Aradau and Sarah Perret, 'The politics of (non-)knowledge at Europe's borders: Errors, fakes, and subjectivity', *Review of International Studies* (2022) 48: 3, pp. 405–424.

[60] Bellanova and Glouftsios, 'Controlling the Schengen Information System (SIS II)'.

[61] Edwards, *A Vast Machine*, p. 84.

[62] Rob Kitchin, *Data Lives: How Data are Made and Shape our World* (Bristol, UK: Bristol University Press, 2021), p. 9.

[63] Debbie Lisle, 'Failing worse? Science, security and the birth of a border technology', *European Journal of International Relations*, 24:4 (2018), pp. 887–910.

https://doi.org/10.1017/S0260210522000365 Published online by Cambridge University Press

the travel documents themselves.[64] Compared to PNR data, API data are considered more reliable because they are in principle not self-declaratory. Cross-validation is facilitated by the temporal characteristics of data production and submission. Air carriers transmit PNR files 24 to 48 hours before the scheduled flight departure time and immediately after 'flight closure' once boarding is complete.[65] Such repetitive data transfers allow PIUs to fuse booking data (PNR) with API data produced during check-in and boarding procedures. This is not only done to validate the accuracy of PNR data, but also to determine the travel status of a suspect passenger – for example, whether the individual in question has not changed elements of their booking last minute, whether they checked in, and whether they boarded (Interview 3).

Fusing and cross-validating PNR and API data is not, nevertheless, a frictionless process. Some of our interviewees uttered doubts about the actual reliability of API data, as they would in theory be consistent with travel documents, but frequently non-validated in practice. (Interview 7). According to the relevant EU legislation, API data are queried to carry out checks at external EU borders with third countries – but not for controls at the common borders of the member states.[66] This means that API data are not collected for intra-Schengen flights, even though airlines do transfer PNR data for those flights in most member states.[67] Additional issues with API data may emerge depending on the method of check-in. Contrary to the check-in and baggage drop processes at airports where a passenger's travel document can be scanned, the data 'collected from online and mobile services are generally declarative in nature, as they are invariably manually entered by the passenger'.[68] Here the tensions between commercial and law enforcement interests become evident once more: airlines tend to prefer online, self-service check-in processes to accelerate passenger mobility in airports, but this means that 'for many passengers travelling without checked-in baggage, there is often no opportunity during airport transit to validate [API data].'[69]

Overall, concerns regarding the accuracy and completeness of PNR data are not easily remedied. This goes up to the point that, due to the sheer volume of data produced by flights daily – and against the pressures to produce intelligence in a timely fashion – PIUs see themselves forced to discard flagged data that could not be corrected through cross-validation processes (Interview 7). This means that, depending on the overall data quality for specific flight routes, a portion of PNR data may never end up being analysed, thus potentially obscuring travel behaviours that analysts are searching for. Particularly the discarding of flagged and unvalidated data means that during analysis, as we will discuss in more detail below, pattern recognition algorithms may yield distorted results, and screening processes via targeting rules may produce different hits. Data frictions have thus already potentially impacted the informational value of PNR files in the fight against serious crime and terrorism. They now tell a partly truncated story about international mobility, which is one of the reasons why PIUs go on to fuse them with other, more traditional forms of investigative knowledge and expertise.

Knowledge contextualisation

Once PNR data are considered sufficiently trustworthy, PIUs subject them to three types of analysis: (1) they are archived and – upon request from investigators – made available to inform

[64] European Union, 'Council Directive 2004/82/EC on the Obligation of Carriers to Communicate Passenger Data. Official Journal of the European Union, 29 April, L 261/24-27' (2004).

[65] European Union, 'Directive (EU) 2016/681', p. Art. 8.

[66] European Union, 'Council Directive 2004/82/EC on the Obligation of Carriers to Communicate Passenger Data: Official Journal of the European Union, 29 April, L 261/24-27', p. Art. 3.

[67] European Commission, 'SWD(2020) 128 Final', p. 42.

[68] European Commission, 'Feasibility Study on a Centralised Routing Mechanism for Advance Passenger Information (and Passenger Name Records). Volume 1: Main Report', pp. 26–7.

[69] Ibid., p. 27.

https://doi.org/10.1017/S0260210522000365 Published online by Cambridge University Press

ongoing criminal investigations and judicial proceedings;[70] (2) they are matched against national and international databases (most notably the Schengen Information System and Interpol's database for Stolen and Lost Travel Documents) and, depending on national legislation, also against specific watchlists; and (3) they are used to identify hitherto unknown suspects within global mobility flows. The first two use cases are comparably straightforward, although inaccurate and incomplete PNR files complicate investigation and matching procedures. In the following, we will therefore concentrate on the third use case and retrace how PIUs construct threat profiles used for the screening of air travel. Adding to the literature that emphasises the data-driven, algorithmic nature of intelligence and security knowledge production,[71] our analysis shows that profiles come into being through the fusion of both insights generated through the processing of PNR data and more traditional 'low-tech' investigative knowledge and expertise.[72] In this sense, the work of PIUs demonstrates how data in international security are complemented by investigative hints, clues, speculations, and experiences that also feed into the production of intelligence.

Per the EU PNR Directive, PNR data can be used to create and update 'targeting rules' for the identification of unknown suspicious passengers within international mobility flows.[73] The rationale that underpins the construction and use of such targeting rules is to build a model for travel behaviour that allegedly corresponds to a specific type of offence (for example, human trafficking, narcotics trafficking, persons travelling to certain regions to act as foreign terrorist fighters) through a combination of (weighted) PNR data categories (for example, nationality, means of payment, itinerary). In practice, this model is then used as an automated search query that continuously screens all incoming PNR data. In simple terms, targeting rules calculate a score for each incoming PNR file based on points assigned to each category. A fictional, oversimplified example for a targeting rule would be the following: male subject (U points); under thirty years of age (V points); booked ticket in cash (W points); travelling with more than L kg of luggage (Y points); flying late at night (X points); flying to a destination through transit (Z points). If a passenger exceeds a predefined threshold of points, it is assumed that they could potentially be associated with criminal or terrorist activities and may be subjected to security measures, that is, be stopped and questioned at an airport or be put under surveillance.

To model allegedly suspicious behaviour, PIUs use different methods. One such method is to conduct targeted searches in archival PNR data to trace the past travel behaviour of known offenders and find 'clues' (Interview 4) about the modus operandi of criminal and terrorism networks. One interviewee illustrated this process as follows: 'Let's say, hypothetically, that after a bombing, the police identified the suicide bomber. … They will ask us to trace his previous journeys and identify his background and potential associates' (Interview 3). Through this process, PIUs might be able to refine targeting rules based on new information about the background of known individuals and the logistics of their travels (for example, where they travelled in the past, how they transited, through what travel agencies they booked tickets). In this regard, even non-PNR-related arrests can become relevant, as PIUs might be able to reconstruct the past travel behaviour of arrested individuals and use it as a starting point for the construction of new targeting rules. The production of intelligence about past offences through searches in archival PNR data can thus feed into the redesign of targeting rules deployed to address future risks. Conversely, the preemption of future risks through rule-based targeting and the real-time screening of passengers can feed back into ongoing investigations since it may result in the detection of previously unknown associations between, for example, suspects, travel agencies, or blacklisted credit cards.

[70] National authorities could obtain historical PNR data from airlines directly in the past. The PNR Directive in this regard primarily provides efficiency gains by pooling PNR data.

[71] Aradau and Blanke, 'Politics of prediction'; Amoore and Piotukh, 'Life beyond Big Data'; Hall and Mendel, 'Threatprints, threads and triggers'.

[72] Bonelli and Ragazzi, 'Low-tech security'.

[73] European Union, 'Directive (EU) 2016/681', p. Art. 6.2(c).

https://doi.org/10.1017/S0260210522000365 Published online by Cambridge University Press

Another method to model suspicious behaviour is to search for patterns within PNR data via algorithmic analysis tools. Once an algorithm has identified a pattern in past data, it can be used as the starting point for modelling criminal or terrorist phenomena that authorities had no prior knowledge of. As one interviewee explained: 'Let's say in the last few years [we] have seen women from member state X between 17 and 25 [years of age] that travel on these dates and travel by themselves and have booked the ticket only one day before – there might be a possibility that they are drug mules' (Interview 4). The problem with targeting rules based on patterns is that they might not necessarily correspond to actual criminal or terrorist activity. This is even more important to highlight because some PIUs explore whether machine learning methods can enhance pattern discovery in PNR data. Our interviewees were, however, somewhat cautious about this possibility, as the creation of targeting rules through pattern discovery could only be considered reliable if archival PNR data used to train algorithmic systems are complete and accurate (Interview 5) – characteristics that, as discussed above, cannot be taken for granted. As one interviewee highlighted, without sufficiently good quality data, PIUs 'risk creating profiles that are not useful for investigations' (Interview 1).

Caution was also expressed regarding the ability to effectively anticipate future risks based on pattern discovery. As any targeting rule needs to correspond to patterns reflected in past PNR data, this approach can only be applied to specific types of offences that take on the form of routinised actions. Said one analyst: 'We won't be able to target sex offenders because there is hardly any standard sex offender behaviour. It's more likely to apply to things like trafficking, where you get mules that keep on using the same travel route, with a certain set of luggage, same age group, and so on' (Interview 7). This means that targeting rules crafted through pattern recognition would not necessarily allow anticipating the unknown unknowns of security – that is, rare behaviours and events not represented in past data. Instead of predicting unknown futures, the results of pattern recognition tend to represent a future that looks very much like the past.[74]

Furthermore, with large amounts of data, there is always the risk of identifying random correlation patterns.[75] To discern such patterns and determine whether they can lead to actionable intelligence, PIUs fuse pattern recognition with actual domain expertise – that is, knowledge about the specific characteristics of air travel. As one analyst framed it, 'you need to know stuff like, for example, the average weight of luggage, the ways flight routes change in summer and winter, whether morning flights are booked more often by businessmen, and so on' (Interview 2). A profound understanding of international mobility, so the underpinning rationale here, can be used as a baseline to identify specific patterns as 'normal' travel behaviour and others as 'strange and abnormal behaviour' (Interview 6), with the latter potentially indicating security-relevant phenomena.

In many cases, instead of pattern recognition and data-driven knowledge, the modelling of suspicious behaviour by PIUs starts with hints provided by other authorities operating at the frontline of crime prevention and counterterrorism. As our interviewees explained, PIUs receive information about known criminal and terrorist networks from national agencies (for example, police units specialised in money laundering, smuggling, and trafficking; customs; intelligence services), which are expected to deliver specific insights about mobility patterns based on past experience or ongoing investigations. PIUs then screen for these patterns in PNR data, aiming to discover individuals that could be connected to specific known (or suspected) organisations or types of offence. Investigative knowledge provided by police and intelligence agencies is thus considered key for producing intelligence. As one interviewee put it: 'There is no one better than our colleagues who are based in a certain place [for example, a city where a narcotics

[74] Lyria Bennett Moses and Janet Chan, 'Algorithmic prediction in policing: Assumptions, evaluation, and accountability', *Policing and Society*, 28:7 (2018), pp. 806–22 (p. 810).

[75] Amoore, 'Data derivatives'.

https://doi.org/10.1017/S0260210522000365 Published online by Cambridge University Press

trafficking network operates] to tell us about the specific risk in that place and its characteristics [for example, drug mule travel behaviour]' (Interview 1).

But information exchange related to the construction of targeting rules (or ongoing investigations) does not only take place at the national level. According to the EU PNR Directive,[76] the PIUs of different Member States can exchange PNR data – and the results of their processing – among each other and with Europol.[77] A PIU can either transfer data on its own initiative or as a reply to a specific request lodged by other PIUs or Europol. While such information exchange is often imagined as a perfectly organised, seamless flow of bulk data, in practice it tends to be piecemeal and unsystematic. For example, problems emerge in relation to 'broad and unspecified'[78] requests for information submitted to many different PIUs. This renders their interpretation and assessment difficult and raises the workload of PIUs that are expected to share data and intelligence feeding into the design of targeting rules. At the same time, there is limited spontaneous information sharing among PIUs. This is not only because PIUs may consider the information that they have irrelevant to investigations conducted in other member states (Interview 4), but also due to limitations in 'human and technical capacity to conduct assessments targeted at the needs of other member states and to engage in proactive transfers of data'.[79]

In summary, by fusing data-driven insights with other forms of knowledge circulated nationally and at the EU level, PIUs seek to create additional informational value that supersedes patterns detected through the analysis of PNR files alone. Notably, this foregrounds how intelligence is profoundly hybrid, relying on the co-constitutive effects of pattern recognition and domain expertise. Despite the diverging epistemic characteristics of data analytics and investigatory knowledge, PIUs synthesise and condense them into unified expressions of suspicion, that is, targeting rules that serve as a key tool to screen international air travel. At this stage, PIUs act as centres of calculation that produce intelligence by fusing data-driven insights with heterogeneous knowledges produced within a dispersed network of local, national, and European authorities. Targeting rules relate both to the future, as they are used in the screening of incoming PNR data to anticipate and pre-empt security risks, and to the past, as they can be related to previous or ongoing investigations. Before being put to practice, however, targeting rules must still be subjected to a final set of modifications.

Adjustments and actionability

As detailed in the previous section, PIUs are mindful that intelligence exclusively predicated on data analysis runs the risk of being disconnected from actual empirical phenomena. Targeting rules do not make any objective statements about the intentions or the dangerousness of passengers. Rather, they rely on 'speculative' criteria[80] that become associated with risk through investigative work and pattern recognition. Travellers are 'enacted'[81] as risky subjects based on behavioural patterns, biographical characteristics, and travel logistics that change 'the process by which people and things are rendered perceptible and brought to attention'.[82] Risky travellers are, in the words of Evelyn Ruppert, 'not always and already there awaiting identification',[83] but

[76] European Union, 'Directive (EU) 2016/681', p. Art. 9 & 10.

[77] It is important to note that PNR data can also be exchanged with third countries. We do not have the space to engage with such exchanges here, but see Argomaniz, 'When the EU is the "norm-taker"?'; Carpanelli and Lazzerini, 'PNR: Passenger Name Record, problems not resolved?'; Roda, 'Shortcomings of the Passenger Name Record directive in light of opinion 1/15 of the Court of Justice of the European Union'.

[78] European Commission, 'SWD(2020) 128 Final', p. 35.

[79] Ibid., p. 36.

[80] Marieke de Goede, *Speculative Security: The Politics of Pursuing Terrorist Monies* (Minneapolis, MN: University of Minnesota Press, 2012).

[81] Evelyn Ruppert, 'Population objects: Interpassive subjects', *Sociology*, 45:2 (2011), pp. 218–33.

[82] Amoore, *Cloud Ethics*, p. 15.

[83] Ruppert, 'Population objects', p. 224.

https://doi.org/10.1017/S0260210522000365 Published online by Cambridge University Press

instead are brought into being in particular ways through the fusion of data-driven insights and investigatory knowledge by PIUs. Profiling, through the construction of targeting rules, reverses the presumption of innocence against passengers[84] who are stopped at airports not because there is evidence that they committed an offence in the past, but because their data match the criteria that constitute a targeting rule, based on which it is inferred that they embody crime or terrorism risks.

In this context, a major concern for PIUs is that even carefully crafted and refined targeting rules might not be suitable for meaningful screening because their scope might be too broad and thus 'unworkable' in international mobility controls. As one interviewee put it, a targeting rule that would 'lead you to arrest half of the plane' is considered untenable and must thus be further calibrated to become actionable and yield the desired results (Interview 6). This is particularly pertinent *vis-à-vis* false positives, that is, wrongfully suspected persons. As targeting rules model travel behaviour that is believed to be associated with criminal or terrorist activities, any screening hits produced are, from a security perspective, initially treated as potentially suspicious – even though it might turn out that the individuals in question have no connections to the alleged activities at all. This is why our interviewees were careful to emphasise that travellers identified based on targeting rules should not, by default, be considered criminals or terrorists. It is in fact assumed that 'in rule-based targeting, in most cases, the hits are good guys' (Interview 6).

A second concern relates to operative capacities on the ground. Intelligence needs to be meaningful and actionable, meaning that it must not produce inflated numbers of hits that would lead to large numbers of passengers being stopped for additional screening and thereby overburden operative forces at airports and delaying travellers' transportation and transit (Interview 7). From the perspective of PIUs, it is therefore considered paramount that targeting rules correspond not only with suspected criminal or terrorist behaviour but also with established international mobility control processes and routines. The primary means to achieve this is by lowering the number of hits produced by a targeting rule. As a rule of thumb, as one interviewee told us, hits per flight should be limited to no more than two passengers (Interview 6). Targeting rules are tested on archival PNR data, estimating the number of hits that a specific profile would have generated in the past. If that number is too high or low, the profile can be calibrated, making it either more specific (producing fewer hits) or more general (producing more hits). Such calibration can, for instance, be achieved through the weighting scores assigned to particular data categories, the addition of new categories, or simply by adapting the overall scoring threshold required for the generation of a hit. Additionally, after having been implemented for automated screening of PNR data, targeting rules are reviewed in regular intervals to ensure that they remain workable *vis-à-vis* incoming data, and also up to date in relation to emerging investigative knowledge (Interview 6).

A practical example of how targeting rules are adjusted, calibrated, and rendered more specific to produce fewer hits would look like the following. PIUs may have information on a suspicious travel agency, including its IATA number (that is, registration number accredited by the International Air Transport Association), associated telephone numbers, and email addresses. By inserting this information into the criteria of a targeting rule, PIUs can detect passengers who have booked their tickets through that particular travel agency. Of course, this does not mean that every passenger who has booked a ticket through a suspicious travel agency can and will in fact be stopped at the airport. As an analyst framed it, PIUs have no interest in elderly people who prefer to book a ticket through the travel agency in their neighbourhood instead of doing that online (Interview 4). So they opt to use additional investigatory information, if

[84] Paul de Hert and Vagelis Papakonstantinou, 'Repeating the mistakes of the past will do little good for air passengers in the EU: The comeback of the EU PNR directive and a lawyer's duty to regulate profiling', *New Journal of European Criminal Law*, 6:2 (2015), pp. 160–5.

https://doi.org/10.1017/S0260210522000365 Published online by Cambridge University Press

available, to filter these persons. If there is, for instance, information about a trafficking network and corresponding traveller profiles, this can be used as an additional criterion to calibrate the targeting rule – which would then only produce a hit if someone with a specific profile would book a ticket through a suspicious travel agency. The rationale at play here is to make targeting rules as specific and detailed as possible to reduce the number of false positives.

Through the adjustment and calibration of targeting rules, PNR data undergo one final transformation. At this final stage, their informational value becomes deliberately modified to neither overstrain operative mobility control resources nor put untenable hardships on regular travellers. Actionability requirements in intelligence production, in line with the above discussions of data frictions and the fusion of different types of knowledge, portray the work of PIUs as deeply enmeshed in a wider ecosystem of international security. Alignment with this ecosystem requires what Egbert and Leese have described as a form of 'tinkering' that builds on the discretion of analysts, leaving them free to consider factors that are excluded from automated data analysis with algorithms.[85] Rather than a purely technical process, such tinkering shows how PIUs manage to produce a single register of intelligence and how this register remains in itself flexible and subjected to further adjustments and modifications.

Conclusion

Throughout this article, we have conceptualised and empirically substantiated how PNR data come to matter in the making of international security. Contributing to the wider literature in IR that has interrogated the datafication, digitisation, and sociotechnical reassembly of security, we have suggested to pay attention to the practices of the involved actors, in our cases the PIUs that are tasked with making sense of PNR data. We have introduced the concept of epistemic fusion to provide a holistic and contextualised account of how digital data are shared, synthesised, and analysed to create actionable intelligence. Epistemic fusion, as we have shown, involves dealing with frictions linked to data accuracy and completeness, combining data-driven insights with investigative knowledge, and adjusting analytical products to make them fit into the broader ecosystem of international mobility controls. Importantly, our analysis highlights how PIUs act as centres of calculation that turn an otherwise dispersed assemblage of heterogeneous actors, knowledges, and data into a single, authoritative register of intelligence. Epistemic fusion is, in this sense, productive of a structure within which PIUs emerge as centres that channel not only data flows, but also various hints, clues, and insights relevant to international security, specifically regarding the fight against serious crime and terrorism.

While a lot has been written about pre-emptive rationalities of control translated into the functionalities of surveillance infrastructures, this article takes a step further and has investigated how these rationalities are operationalised through data transfer, screening, validation, discarding, profiling, contextualisation, calibration, and adjustment practices. At first sight, these practices may seem banal and technical – however, as the work of PIUs forcefully demonstrates, they matter politically as they underpin the making of international security. Analysing data practices furthermore allows us to challenge discourses about straightforward enhanced efficiency and effectiveness of security through digital means. Instead, staying with the frictions, sociotechnical complexities, and patchy character of intelligence production provides an analytical incision point to probe how complex and distributed security assemblages play out in the everyday. This is crucial, as it helps us to problematise essentialist and deterministic understandings of digitisation according to which technological developments associated with the processing of large amounts of data inevitably lead to 'better' intelligence, allowing to fill information gaps, shed light on blind spots and, ultimately, anticipate unknown future risks. This is also important to avoid analyses that internalise, perhaps involuntary, imaginaries about the increased

[85] Egbert and Leese, *Criminal Futures*, p. 103.

https://doi.org/10.1017/S0260210522000365 Published online by Cambridge University Press

automation of security whereby decisions about who to stop at a border are made by software applications that acquire the ontological status of a somewhat autonomous agent whose recommendations exceed the knowledges, experiences, and discretionary power of those human actors who perform security in practice.

We contend that analyses of internationally relevant data practices will benefit the wider discipline of IR. More empirical and theoretical work is needed to fully grasp the multiple ways in which data analytics impact key variables of the international: new actors and reshuffled actor relations, novel forms of power that emerge from knowledge work, data economies, or the regulation of data exchange across borders, to name just a few. It is our modest hope that our analysis and conceptual elaborations will be useful for scholars interested in these topics.

Acknowledgements. We would like to thank Nisha Shah and the three anonymous reviewers for their constructive comments. We would also like to thank Rocco Bellanova, Anna Casaglia, Myriam Dunn Cavelty, Carla Monteleone, Annalisa Pelizza, as well as the participants of the Research Colloquium at ETH Zurich's Center for Security Studies for providing feedback on previous versions of this article.

Funding. This research was supported by Fondazione Caritro in the context of the research project 'Digitised Borders: How Data Infrastructures Shape the Control of Mobilities in Europe'.

Georgios Glouftsios is Assistant Professor (RTDA) in Political Sociology at the School of International Studies, University of Trento. His work sits at the intersection of Critical Security Studies, International Political Sociology, and Science and Technology Studies. He is the author of *Engineering Digitised Borders: Designing and Managing the Visa Information System* (Springer Nature, 2021). Author's email: georgios.glouftsios@unitn.it.

Matthias Leese is Assistant Professor for Technology and Governance at the Department of Humanities, Social and Political Sciences, ETH Zurich. His research is interested in the effects of digital technologies on social order. It pays specific attention to security organisations and their rationales and practices that are co-constituted between the technological and the social. Author's email: mleese@ethz.ch

Cite this article: Glouftsios, G., Leese, M. 2023. Epistemic fusion: Passenger Information Units and the making of international security. *Review of International Studies* **49**, 125–142. https://doi.org/10.1017/S0260210522000365

https://doi.org/10.1017/S0260210522000365 Published online by Cambridge University Press