Datawars: reflections twenty years after 9/11

Amoore, L.; de Goede, M.

DOI
10.1080/17539153.2021.1982117
Publication date
2021
Document Version
Final published version
Published in
Critical Studies on Terrorism

CRITICAL STUDIES ON TERRORISM
2021, VOL. 14, NO. 4, 425–429
https://doi.org/10.1080/17539153.2021.1982117

Routledge
Taylor & Francis Group

SPECIAL ISSUE

Datawars: reflections twenty years after 9/11

Louise Amoore[a] and Marieke de Goede[b]

[a]Department of Geography, Durham University, Durham, UK; [b]Faculty of Social and Behavioural Sciences, University of Amsterdam, Amsterdam, Netherlands

At the time of writing in spring 2021, Guantanamo Bay continues to hold the last forty prisoners who were captured and held without trial at the US Naval Base in Cuba since the US invasion in Afghanistan in 2001. The oldest prisoner is soon to be 74. Multiple detainees died in captivity, without ever being brought to trial. Although the Obama government transferred over 700 detainees out of the camp, Obama failed to keep his election promise of closing it (The New York Times 2021). Twenty years after 9/11, is this the last visible violence of the War on Terror finally coming to an end?

In our joint work, begun in the wake of the events of 9/11, we have drawn attention to the "other" violences of the War on terror, namely its "Datawars" (Amoore and de Goede 2005, 2008, 2011; de Goede 2012; Amoore 2013). After 9/11, many states adopted a so-called data-led approach to combating terrorism. This approach stresses proactive, large-scale information gathering, and data exchange in the name of pre-empting terrorist attacks (Aradau and van Munster 2011; Heath-Kelly 2017; Amoore and Raley 2017). The 9/11 Commission report retrospectively speculated that the attacks could have been pre-empted if the "information available in US government databases" had been connected with the data on "characteristic travel patterns" (Council of the 9/11 Commission 2004, 384).

The framing of 9/11 as a catastrophic failure to use available data thus became the condition of possibility for the datawars on terror. "Smart solutions" technologies, pioneered in realms such as retail consumer data mining and the detection of financial fraud, appeared to enable the "connecting of dots" through profiling, data mining, social network analysis and other predictive technologies. Data have become framed as the answer to contemporary security problems and their fluid and unpredictable nature. Data derived from already existing databases – everyday financial transactions, airline passenger manifests and welfare and social security information – have become strategically important forms of intelligence to sovereign power (Bellanova and González Fuster 2019; Hoijtink and Leese 2019; Gilbert 2015). The invisible violences and political authority of this contemporary turn to data storage, retrieval, interpretation and analysis in the global security landscape, is what we term the Datawar.

In this contribution, we reflect on the contours of the Datawar twenty years after 9/11. The Datawar is a war by other means; it echoes the architecture of war, yet works to conceal the violences of its classification, sorting, and banning of human lives (Coward 2009; Graham 2006). After the Snowden disclosures, and with increasing attention to data

CONTACT Louise Amoore louise.amoore@durham.ac.uk

architectures and algorithmic systems within critical data studies (Milan and Treré 2019; Hayles 2012; Benjamin 2019), the Datawar is perhaps no longer a "war that no one sees". Yet the precise connections between the overt violences of – for example – drone attacks and immigration detention, and the invisible violences of data-analytics remain obfuscated and responsibility is evaded.

For example, the Dutch state is being held responsible in a Dutch court case for complicity in a US-led drone attack in Somalia in 2014. Two Somali nomads lost family members and limbs in the attacks for which they are now suing the Dutch state. Dutch marines participated in the EU-led Mission Atalanta to fight piracy off the coast of Somalia. Seemingly a humanitarian mission and supported by the UN World Food Programme, Atalanta was perhaps foremost a "surveillance mission",[1] yielding large sets of mobile phone and geospatial location data, thought to have been shared with the US and subsequently deployed in drone targeting. Only if and when the Somali nomads' case is able to appear before court, may we learn about the precise infrastructures that connect the humanitarian mission to its military targeting via maritime surveillance.

The datawar has profoundly transformed everyday life in the wake of the War on Terror. It affects everyone with a bank account, everyone who participates in social media platforms, and everyone who boards a plane – yet it does not affect everyone equally. We briefly discuss three themes concerning how practices of targeting and spaces of governing are taking shape in the Datawar, and why it remains an important research agenda twenty years after 9/11.

Temporality and possibility

A key feature of the Datawar is its objective to intervene in advance – before the threat materialises, before the traveller boards the plane, before the plot is financed. This logic has permanently widened the *space* and the *time* of security (de Goede 2012). Acting on suspicion and through association are no longer beyond the rule of law; they have become explicitly acknowledged objectives of contemporary security politics. In our earlier work, we made an explicit connection between the guilt by association logics of social network analysis and the association rules that characterise the "if, and, then" grammar of data mining algorithms (Amoore and de Goede 2008). For the first decade after 11 September 2001, it was the formulation of association rules that allowed for security interventions to be made pre-emptively and in anticipation of possible future threats.

Indeed, the years after 9/11 fostered direct and intense collaboration between the mathematical and computer sciences and the agendas of homeland security. The work of IBM Almaden computer scientist, Rakesh Agrawal, for example, had pioneered "the ability to find patterns in accumulated data" for commercial retail companies since the 1980s (Agrawal, Imielinski, and Swami 1993, 207). Ten years later, these same ordinary algorithms were to become the mainstay of homeland security systems, with Agrawal pointing to "different characteristics" such as "financial support, Islamic leaders" that would be "written into the rules" (cited in Amoore 2013, 43). In the current hype around algorithmic decision systems, it is very often forgotten that 9/11 played such a crucial role in suturing together the racialised association rules of security with the mundane possibilities of retail

data mining (Benjamin 2019). Without the capacity to *speculate* about *possible* connections, and to write these possibilities into algorithmic rules, the temporalities of pre-emptive security could not have become so deeply established as they are today.

Data infrastructures

The language of "big data" does not always offer the right vocabulary and tools to analyse the ways in which data are captured, combined and rendered transportable in the context of the Datawar. Data do not simply "flow" across jurisdictions and across public and private spheres; they have to be rendered transportable, translatable, and transformable. The technical and legal infrastructures of contemporary Datawars have come to permeate everyday lives. Every bank transaction is scrutinised for a potential link to terrorism financing – broadly defined. Every country holds millions of financial transaction reports of citizen non-suspects in its classified FIU databases. Every airline journey generates advanced passenger information to security authorities. We have argued that further attention to the legal and technical data infrastructures is crucial to understanding and critiquing its politics. These infrastructures make it possible to capture and identify data points, carve off databases, render them transportable to other jurisdictions, render them accessible and analysable, and, eventually, lead to concrete security interventions in opaque ways (Amoore and Piotukh 2015; Bellanova and de Goede 2021). These data infrastructures are often built in ad-hoc ways, stretching the limits of existing law.

As cloud infrastructures and platform-based infrastructures have transformed the Datawar, so too the development of machine learning tools have radically re-shaped the second decade of post-9/11 security. Where the association rules of data mining underpinned the security deployed at borders and in the financial system, the growth of deep neural networks has witnessed greater automation of systems and the generation of rules by algorithms. In this contemporary turn to automation in the Datawar – from autonomous weapons systems to facial recognition – the data infrastructure yields the patterns and features that become of security interest.

The mobile norm and racialised exclusion

The Datawar, while being risk-based, does not revolve around conventional notions of surveillance and profiling. The ambition of the Datawar is no longer to define pre-existing profiles of suspicion and normality against which citizens can adjudicate their behaviours. Instead, the Datawar depends upon a "mobile norm" that is both flexible and unknowable. If discipline works through regularity so that the citizen knows how to behave; the mobile norm governs unpredictably and through the surprise effect. Security algorithms have generated "bounded conditions of what a democracy, a border crossing, … or a public protest *could be* in the world" (Amoore 2020, 4, emphasis added). The "'other' is algorithmically enacted as an anomaly" in big data technologies (Aradau and Blanke 2015, 3). As one element of a broader shift from statistical and demographic forms of ordering (Fourcade 2021), the rise of the mobile norm has extended the forms of racialised violence that take place through surveillance and enumeration. Post-9/11 worlds of risk and security have deepened the postcolonial racialised imaginaries of who or what is to be feared, who or what to be secured (Puar 2007; Browne 2015). The

dissolution of the criteria for the "norm" has also undercut the juridical and rights-based interventions available to us in challenging racism and discrimination. How does one intervene in the algorithm that is constantly adjusting its own parameters of what or who is suspicious?

Note

1. See, https://publications.parliament.uk/pa/ld200910/ldselect/ldeucom/103/10304.htm

Acknowledgments

Many thanks to Lee Jarvis for encouraging us to write this piece and to the special issue editorial team of *Critical Studies on Terrorism*.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Funding

This project has received funding from the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme (grant agreements No. 682317 and No. 883107).

References

Agrawal, R., T. Imielinski, and A. Swami. 1993. "Mining Association Rules between Sets of Items in Large Databases." *ACM SIGMOD Record* 2 (2): 207–217. doi:10.1145/170036.170072.

Amoore, L. 2013. *The Politics of Possibility: Risk and Security beyond Probability*. Durham: Duke University Press.

Amoore, L. 2020. *Cloud Ethics: Algorithms and the Attributes of Ourselves and Others*. Durham: Duke University Press.

Amoore, L., and M. de Goede. 2005. "Governance, Risk and Dataveillance in the War on Terror." *Crime, Law and Social Change* 43: 149–173. doi:10.1007/s10611-005-1717-8.

Amoore, L., and M. de Goede. 2008. "Transactions after 9/11: The Banal Face of the Preemptive Strike." *Transactions of the Institute of British Geographers* 33 (2): 173–185. doi:10.1111/j.1475-5661.2008.00291.x.

Amoore, L., and M. de Goede. 2011. "Risky Geographies: Aid and Emnity in Pakistan." *Environment and Planning D: Society and Space* 29 (2): 193–202. doi:10.1068/d2902ed2.

Amoore, L., and R. Raley. 2017. "Securing with Algorithms: Knowledge, Decision, Sovereignty." *Security Dialogue* 48 (1): 3–10. doi:10.1177/0967010616680753.

Amoore, L., and V. Piotukh. 2015. "Life beyond Big Data: Governing with Little Analytics." *Economy & Society* 44 (3): 341–366. doi:10.1080/03085147.2015.1043793.

Aradau, C., and R. van Munster. 2011. *Politics of Catastrophe*. London: Routledge.

Aradau, C., and T. Blanke. 2015. "The (Big) Data Security Assemblage: Knowledge and Critique." *Big Data & Society* 2: 205395171560906. doi:10.1177/2053951715609066.

Bellanova, R., and G. González Fuster. 2019. "Composting and Computing: On Digital Security Compositions." *European Journal of International Security* 4 (3): 345–365. doi:10.1017/eis.2019.18.

Bellanova, R., and M. de Goede. 2021. "The Algorithmic Regulation of Security: An Infrastructural Perspective." *Regulation & Governance*.

Benjamin, R. 2019. *Race after Technology: Abolitionist Tools for the New Jim Code*. Cambridge: Polity.
Browne, S. 2015. *Dark Matters: On the Surveillance of Blackness*. Durham NC: Duke University Press.
Council of the 9/11 Commission, 2004. *The 9/11 Commission Report*. W.W Norton: Washington.
Coward, M. 2009. "Network-Centric Violence, Critical Infrastructure and the Urbanization of Security." *Security Dialogue* 40 (4–5): 399–418. doi:10.1177/0967010609342879.
de Goede, M. 2012. *Speculative Security: The Politics of Pursuing Terrorist Monies*. Minneapolis: University of Minnesota Press.
Fourcade, M. 2021. "Ordinal Citizenship." *The British Journal of Sociology* 72 (2): 154–173. doi:10.1111/1468-4446.12839.
Gilbert, E. 2015. "Money as a "Weapons System" and the Entrepreneurial Way of War." *Critical Military Studies* 1 (3): 202–219. doi:10.1080/23337486.2015.1063810.
Graham, S. 2006. "Cities and the War on Terror." *International Journal of Urban and Regional Research* 30 (2): 255–276. doi:10.1111/j.1468-2427.2006.00665.x.
Hayles, N. K. 2012. *How We Think*. Chicago: University of Chicago Press.
Heath-Kelly, C. 2017. "Algorithmic Autoimunity in the NHS: Radicalisation in the Clinic." *Security Dialogue* 48 (1): 29–45. doi:10.1177/0967010616671642.
Hoijtink, M., and M. Leese, eds. 2019. *Technology and Agency in International Relations*. London: Routledge.
Milan, S., and E. Treré. 2019. "Big Data from the South(s): Beyond Data Universalism." *Television & New Media* 20 (4): 319–335. doi:10.1177/1527476419837739.
Puar, J. 2007. *Terrorist Assemblages: Homonationalism in Queer Times*. Durham NC: Duke University Press.
The New York Times. 2021. "The Guantánamo Docket." *The New York Times*, June 9.