UC Santa Barbara

UC Santa Barbara Previously Published Works

Title

Securing with algorithms: Knowledge, decision, sovereignty

Permalink

https://escholarship.org/uc/item/87g1b7hk

Journal

Security Dialogue, 48(1)

Authors

Raley, Rita
Amoore, Louise

Publication Date

2017-02-01

Peer reviewed

eScholarship.org Powered by the California Digital Library
University of California

Special issue on *Securing with algorithms*

SECURITY DIALOGUE

Security Dialogue
1–8
© The Author(s) 2016
Reprints and permissions:
sagepub.co.uk/journalsPermissions.nav
DOI: 10.1177/0967010616680753
sdi.sagepub.com
SAGE

Securing with algorithms: Knowledge, decision, sovereignty

Louise Amoore
University of Durham, UK

Rita Raley
University of California – Santa Barbara, USA

Abstract
Amid the deployment of algorithmic techniques for security – from the gathering of intelligence data to the proliferation of smart borders and predictive policing – what are the political and ethical stakes involved in securing with algorithms? Taking seriously the generative and world-making capacities of contemporary algorithms, this special issue draws attention to the embodied actions of algorithms as they extend cognition, agency and responsibility beyond the conventional sites of the human, the state and sovereignty. Though focusing on different modes of algorithmic security, each of the contributions to the special issue shares a concern with what it means to claim security on the terrain of incalculable and uncertain futures. To secure with algorithms is to reorient the embodied relation to uncertainty, so that human and non-human cognitive beings experimentally generate and learn what to bring to the surface of attention for a security action.

Keywords
Algorithms, decision, security, technology, violence

Introduction

In a world where data trails and pattern-of-life analyses of human beings are thought to yield new forms of knowledge and enable the detection of future threats, algorithms appear to afford a renewed potential for security. *Algorithms* – as both technical process and synecdoche for ever more complex and opaque socio-technical assemblages – imply new ways of knowing, even as their actual operations are increasingly inaccessible (Gillespie, 2016). Advances in task-based

Corresponding author:
Louise Amoore, Department of Geography, University of Durham, Science Site, South Road Durham, Durham DH1 3LE, UK.
Email: louise.amoore@durham.ac.uk

artificial intelligence, machine learning and neural network computation are radically reshaping practices of securitization and instituting new logics for the governing of populations. As Edward Snowden's disclosure of the analysis of bulk data by the US National Security Agency (NSA) and the UK's Government Communications Headquarters (GCHQ) revealed, the sifting, sorting and triage of vast streams of digital data has become possible because of algorithmic techniques such as pattern recognition, n-gram modelling and distributed querying across cloud databases (Greenwald, 2014; Harding, 2014). From the real-time stream analysis of online text read by machine learning algorithms to the anomaly-detection algorithms for the discovery of incipient sentiment and human affects, algorithms hold the promise of extending the threshold of human perception and cognition. So, too, do algorithms attend upon, and emerge from, new practices and forms of archival curation, sovereignty, politics and security (Bratton, 2016; Lemov, 2015).

Notwithstanding the resurgence of interest in how algorithmic devices and systems transform the practice of security, however, some of the most fundamental questions remain scarcely addressed. What does it mean to claim to secure against uncertain events by means of algorithms? In what sense do contemporary algorithms change the nature of uncertainty and the capacity to act upon uncertain futures? Amid the apparent proliferation of algorithmic techniques in the gathering of intelligence data from battlefield, border and city streets, what are the political and ethical stakes involved in securing with, through and via algorithms in the 21st century? In one sense, the modern history of security is saturated with the methods and technologies of computation. The rise of 20th-century cybernetics, for example, lent to 'Cold War rationality' the 'crystalline definiteness, generality, and conclusiveness of the algorithm' that could 'cope with a world on the brink' (Erickson et al., 2013: 30). It was this sense of the 'definiteness' and stability of the algorithm in a world otherwise characterized by profound uncertainty that promised a capacity to secure against unknown futures. Deeply embedded within the international relations of the mid-20th century, then, was a particular science of statistical knowledge, probabilistic modelling, data systems and behaviour analysis (Galison, 1994; Hayles, 1999). Understood in these terms, international relations is bound historically with the development of algorithmic ways of calculating. If, as Orit Halpern (2015: 25) succinctly outlines, 'cybernetics is a science of control or prediction of future events and actions', then the practice of security has historically embraced a computational capacity to act decisively and procedurally in the face of radical uncertainty.

Understood as part of a longer genealogy of placing algorithmic routines at the service of war and security, then, the renewed contemporary interest in the politics of securing with algorithms does not take place at the point of some kind of epistemological break with past modalities. Rather, it reanimates and extends a longstanding intertwining of the practices and techniques of security with computational processes. Across the disciplines of international relations, sociology, media and cultural studies, human geography, law, security studies and political science, a key shared concern is the precise character of the 21st century's relations between algorithms and security. Responding to the spectres of the 'semi-supervised' targeting of the drone strike (Shaw, 2016; Gregory, 2011, Wilcox, 2017), the lethal decisions of autonomous weapons systems (Calo et al., 2016; Singer, 2009; Suchman and Weldes, 2016), and the anticipatory actions of 'smart' borders, cities and predictive policing, scholars have focused on the technological systems, assemblages and ensembles of which algorithms are one element. Likewise, scholars interested in security practices have traced how algorithms devised in the domains of behavioural advertising, customer relations management, finance, insurance and recommendation systems have become mobile, travelling to new sites and assuming new forms of sovereign deployment.

However, the debates on algorithmic politics within security studies have to a certain extent been conducted in isolation from a longstanding and sustained body of research: feminist and post-human analyses of science, technology and militarization (Haraway, 1988, 1997; Hayles, 1999, 2012; Braidotti, 2013; Parks, 2016). As a consequence of neglecting some of the most significant

interventions on the question of the limitations of the category of the human, security studies risks falling short in the analysis of what it means to seek human security in our times. Particularly in the context of a security regime in which algorithmic procedures are corporeally enacted, critical security studies needs feminist epistemologies more than ever before. Though there has been extensive attention paid to the materiality and agency of the objects of security (Salter, 2016), there has been little attention to the question of how algorithms act in ways that are thoroughly embodied, even while they forget the person as such. 'What embodiment secures', writes Katherine Hayles, is 'not the distinction between male and female or between humans who can think and machines which cannot', but rather that embodiment 'makes clear that thought is a much broader cognitive function' (Hayles, 1999: xiv). To draw attention to the embodied actions of algorithms, then, is precisely to reflect on how the already broad cognitive function of thought is distributed and extended through algorithms. As Lauren Wilcox writes in her contribution to this special issue, 'I ask not to what extent drone warfare is embodied or disembodied, but rather, how bodies are corporealized in drone assemblages' (Wilcox, 2016: 5). Thus, the often dominant emphasis on the surveillant assemblage or 'vertical geopolitics' of algorithmic technologies (Graham, 2016; Elden, 2013) – what Donna Haraway (1988: 581) has described as 'visualizing technologies without apparent limit' – is juxtaposed with horizontal or 'flattened' imaginaries that 'do not necessarily entail the view from above' (Mollichi, 2016: 3). To secure with algorithms, then, is to reorient the embodied relation to uncertainty, so that human and non-human beings are constantly attuned to novel events and features in their data environment, becoming perennially creatively alert (Heath-Kelly, 2016).

This special issue of *Security Dialogue* is intended to develop and extend the existing debates on how algorithms transform security practice, proposing that there is more at stake than the *application* of algorithmic technologies to the domain of security. The contributors to this special issue, though they focus on a range of different modes of algorithmic security, do share a common concern with the specific contemporary rearticulation of what it means to claim security on the terrain of the incalculable or uncertain. Each of the contributions explores the algorithm as more than a technological or mathematical apparatus. Indeed, each of the articles explores algorithms as ways of visualizing, calculating, embodying, knowing or perceiving future events such that they may be acted upon in the present. Though to an extent this is familiar territory for those who have long studied the anticipatory techniques of preemptive or premediated security (Grusin, 2010; Amoore, 2013; De Goede, 2012; Aradau and Van Munster, 2011; Anderson, 2010; Uncertain Commons, 2013), here the embodied ontological form of the algorithm itself is the central focal point.

Encouraging a more active engagement with the humanities, where 'conceptualization is intimately tied with implementation, design decisions have theoretical consequences, and algorithms embody reasoning' (Hayles, 2012: 35), this special issue foregrounds precisely the matter of how the world to be known and secured is surfaced in and through the algorithm. As the following articles show, the conceptual and empirical encounters with algorithmic security necessarily involve new ways of reading signals, detecting disturbances and shaping action (Roberts and Elbe, this issue; Lally, this issue). In short, it is not merely that algorithms are applied as technological solutions to security problems, but that they filter, expand, flatten, reduce, dissipate and amplify what can be rendered of a world to be secured.

Data, knowledge, worlds

Though, as we have suggested, one could reasonably situate the birth of algorithmic security within a history of cybernetics, there can be little doubt that the post-9/11 world has provided the context for much of the research on algorithmic forms of security. However, the algorithms that were most widely connected to the desire to 'connect the dots', to break the data silos and to act preemptively

were of a specific type of rules-based and statistical-regression form. The algorithms available for data mining in 2001 were predominantly designed to identify patterns in a volume of transactions, so that rules could be generated for the detection of future events. Though such rules-based systems remain extraordinarily important in security practices – and they are depicted in this special issue in the form of classifiers and relevancy scores (Roberts and Elbe, this issue) – the exponential growth in the availability of so-called big data has accelerated the development of other non-rules-based forms of algorithm. The rise of big data has been accompanied by a new set of promises for how the world might be rendered securable. What Kenneth Cukier and Viktor Mayer-Schönberger (2013) describe as an increase in the volume, variety and velocity of data has held out the possibility for the analysis of unstructured or semi-structured data stored in NoSQL databases. This representation of data as synchronic, or 'real time', notwithstanding its illusory and fragile nature (Crary, 2013), brings with it the imagination of a horizon of security in which the detection of new events can reject traditional statistical risk criteria and embrace emergent futures (Cooper, 2008). Moreover, the migration of data from drives and servers to cloud-based data centres opens up offshore data spaces that defy conventional territorial jurisdictions (Hu, 2015; Bratton, 2016). Put simply, the advances in non-rules-based machine learning algorithms are producing new forms of political authority. The algorithms authorize what or whom is surfaced for the attention of a security analyst who, in turn, cannot meaningfully access this process of authorizing and surfacing.

Algorithms increasingly have the capacity to analyse across different forms of data (images, text, video, audio) and across cloud-based spatial locations of data, as with the US intelligence agencies' 'ICITE' cloud system (Amoore, 2016), which has been facilitated by the shift from rules-based to generative forms of algorithms. Where rules-based algorithmic security would conduct actions on all of the data patterns within the rules, deep machine learning-based systems will find, learn and apply new rules. As Luciana Parisi (2013: 2) writes, 'it is not by chance that the age of the algorithm has also come to be recognized as an age characterized by forms of emergent behaviour that are determined by continual variation and uncertainty'. Understood in Parisi's terms, the very problem space of security – human dwelling in relations of continual variation and uncertainty – actually underwrites the existence of algorithms that 'derive rules from contingencies' (Parisi, 2013: 2), or indeed supplies the conditions they require to learn. Though rules-based algorithms do continue to be present in security practice, the historical significance of the increased use of generative machine learning algorithms cannot be overstated. The abductive logics of many of these families of algorithms contrast with deductive reasoning so that they are closer to experimental processes of learning and verifying through the available data. In the context of security, abductive and generative processes do not begin with a fixed set of criteria for threat or target, but instead they abductively generate the threats and targets via the recognition of patterns in vast volumes of data. In practice this means, for example, that the conventions of 'blacklisting' and security listing begin to generate an adaptive real-time list based on the extrapolation of patterns (De Goede and Sullivan, 2016), or that a social movement is censored in and via its social media activities (Gillespie, 2012), or that a drone targets data-based 'signature strikes' (Wilcox, 2016: 5).

The contributions of this special issue address the generative capacities of algorithms to make worlds in and through data, and they do this in ways that animate the politics of algorithmic world-making. In her discussion of how the British National Health Service (NHS) works to identify possible future radicalized individuals, Charlotte Heath-Kelly traces how 'inductive calculative methods from the digital realm' (Heath-Kelly, 2016: 2) begin to be deployed in the broader profiling of vigilant NHS professionals. The profiles of who or what may be a threat are not accorded a set of criteria for judgement, but are generated and induced through a generalized 'alertness to radicalisation' (Heath-Kelly, 2016: 3). The inscription of racialized and prejudicial religious profiles thus begins to adopt a pattern-recognition style of reasoning and action. Similarly, as Nick Lally illustrates in his essay on crowdsourced surveillance, the 'racist imaginaries of terrorism' are written, in part, through

'algorithmic affordances', so that algorithms are 'a matter not only of watching the world' in a surveillant or observational form, but 'also of constructing worlds' (Lally, 2016: 4, 5, 9). The material from which this world is constructed is increasingly offered up by open-source internet data, as suggested by Stephen Roberts and Stefan Elbe in their essay on a global syndromic surveillance regime tracking the movements of viruses and bacteria. The stream analysis of online indirect and open source data, as Roberts and Elbe explain, becomes a means of 'rendering visible and intelligible future-facing knowledge' so that 'signals of unusual clusters of illnesses' become readable and detectable (Roberts and Elbe, 2016: 2, 3). Algorithms, in other words, act on other algorithms, humans and non-human entities alike. Across the articles in the special issue, one can see how computational and algorithmic forms become embodied, material and everyday ways of enacting security, from identifying radicalization to the targeting of populations by drones. In her compelling argument on algorithmically generated camouflage, however, Silvia Mollichi sounds an important note of caution in the debates on anticipation and the making of actionable worlds. The art of military camouflage, as Mollichi elucidates for us, is 'the art of anticipating perception', though not to render the world legible but to work on 'unreadability' and 'impairing the capacity for making distinctions' (Mollichi, 2016: 4). Citing Orit Halpern's (2015) account of the cybernetic reformulation of the visual apparatus, Mollichi vividly shows how algorithmically generated mimetic patterns are remaking the observer within the system of visualization.

Decision, responsibility, ethics

Contemporary security decisions are made by a complex amalgam of human and machine elements. The algorithm is an integral part of human action and culture (Striphas, 2015). It not only contains within it a teeming array of past human decisions – which training dataset to use, where to set the threshold for sensitivity, whether to use this nearest neighbour algorithm or another one in the same family, how to verify the model for operational use – but, as the following articles show, also extends and modifies embodied human action itself. The figure of the observing security subject is thus impossible definitively to identify, for she is a composite figure of distributed human and non-human agency. The moment of security decision, then, remains an indefinite moment of profound uncertainty. Who or what authorizes the algorithmic security decision? Who or what takes responsibility for the errors, misfires, inconsistencies and mistakes so abundantly documented in this special issue? What would an ethical security decision look like in the context of the human–algorithm composite, in the entangled nexus of what Tarleton Gillespie (2014: 183) terms a 'recursive loop between the calculations of the algorithm and the "calculations" of people'?

The critical and political responses to these kinds of questions have overwhelmingly sought to reinstate the human as the proper figure of sovereignty, its executive decisions bound by juridical and ethical codes of conduct. Thus the 'human in the loop' often functions as a fail-safe for the speculative imaginary of driverless cars, autonomous weapons and robotic surgery. However, taking seriously the generative and world-making capacities of algorithms means troubling the human as the sole locus of security decision, authorship, interpretation and ethico-political responsibility (Raley, 2016). After all, humans and algorithmic systems can be said to have co-evolved in complex processes of technogenesis, with human knowledge and logical structures migrating between people and software agents (Hayles, 2012). As N. Katherine Hayles (1999: 287) has elsewhere written, 'what is lethal is not the posthuman as such but the grafting of the posthuman onto a liberal humanist view of the self'. Such a conception of the self, as Hayles (1999: 286) points out, applies to a 'fraction of humanity' whose 'wealth, leisure and power' affords a life of apparent autonomy and 'individual agency'. Perhaps we can extend this to contemporary posthuman forms of security, suggesting that what is lethal is not the posthuman as such – not the posthuman soldier, analyst, border guard or drone pilot – but the grafting of this figure onto a liberal humanist subject 'in the

loop'. For it is this liberal human subject who has animated the violences and sovereignties of international relations and yet simultaneously appears at the core of the drafting of 'ethical frameworks' for the design of military software, legal 'due process' for myriad algorithmic decisions (Crawford and Schultz, 2014) and juridical reviews of bulk data mining for security.

The articles in this special issue offer a politics of algorithmic security that exceeds and undercuts the search for a singularly human agency and responsibility, yet they do not evade the necessity of confronting the embodied violence of entangled human–algorithmic security action. As Lauren Wilcox (2016, 3) writes in her contribution, reflecting on the responsibility of the drone operator, 'the question of the embodiment of decisionmaking remains vitally important'. Her account is a powerful corrective to notions of the disembodied, non-human, robotic or automated actions of algorithms, urging us to consider that all action at the human–algorithm interface is embodied and to attend to precisely how the putatively immaterial algorithm becomes materialized in the moment of decision. Wilcox's insights signal an ethics of algorithmic security that could never be captured by an appeal to the critical judgement of the human in the machinic loop. To situate sovereign decisionmaking and ethical responsibility solely within the realm of the autonomous machine, or within the realm of the 'human' – itself a dematerialized abstraction that has historically depended on the erasure of the body – is to forget the extent to which algorithms are necessarily instantiated within both.

There are similar moments in the accounts of the other contributors to the volume. Charlotte Heath-Kelly, for example, documents a 'blurring' of social security and national security, where the intuition and inference of algorithmic forms begin to encompass the reasoning and racialized judgements of all of the many humans in the national security/social security loop or, better, feedback loop. Roberts and Elbe ask directly in their essay how there could be any accountability of the forms of knowledge that make up global syndromic surveillance systems. What might it mean, for example, to hold a relevance score accountable for its onward future actions? As Nick Lally (2016: 3) proposes in his contribution, 'algorithms establish a framework that contributes to shaping the possibilities for action'. Perhaps to give an account of such actions is not a matter of uncovering or visualizing a complete picture, nor indeed of opening the so-termed black box of algorithms, but rather of beginning from indeterminate lines of sight and partial perspectives as sites of political contestation, negotiation and refusal. A defining feature of the security–algorithm relation is the act of surfacing something for action. How the person of interest or object of concern is surfaced for security action is a matter of politics. In her account of the camouflage algorithms that work 'against depth', Silvia Mollichi reflects on what she calls the 'privileged observation points' that do not quite fit the prevailing debates on the bird's eye view that reveals all aspects of an environment or system (Mollichi, 2016: 3). 'The possibility of unwiring and rewiring input threads' in the operative logic of this family of algorithms 'is limited', she argues, because 'the data are the wiring design itself' (Mollichi, 2016: 14). Mollichi initiates beautifully the challenge for critical responses to such algorithms in security: where the data generate the design, an ethical response cannot be to modify the design but must begin from the unreadability and illegibility of the pattern.

In sum, the contributions of this special issue map out the many political and ethical dilemmas emerging as algorithms implement, but also transform, existing practices of knowledge production, decisionmaking and securitization. Considered together, the articles offer a timely reminder of the need to situate and interrogate the algorithm as both artefact and precept, technologized procedures that order our perception of control systems. Responding critically to often secretive, black-boxed or obscure techniques and technologies, the authors remind us that algorithmic systems are in fact not inscrutable, and that the calculative modalities that inform their programing can be examined. The work of this special issue, then, is to open up the space for future work on the security–algorithm relation.

Acknowledgements

The authors acknowledge the editors and anonymous reviewers of *Security Dialogue* for their insightful comments; Claudia Aradau for first persuading us, in a Toronto café, to edit this special issue; Volha Piotukh, Sarah Hughes, Alice Cree, Peter Forman and Vanessa Schofield for their work in support of Durham University workshops at which some of these articles were first presented; and finally, the contributors to the special issue who have generously committed their work and creative energies. Thank you.

Funding

Louise Amoore's contribution to this work was supported by the RCUK Global Uncertainties Fellowship 'Securing Against Future Events: Pre-emption, Protocols and Publics' (Grant number ES/K000276/1) and Leverhulme Trust Major Research Fellowship 'The Ethics of Algorithm'.

References

Amoore L (2013) *The Politics of Possibility: Risk and Security Beyond Probability*. Durham, NC: Duke University Press.

Amoore L (2016) Cloud geographies: Computing, data, sovereignty. *Progress in Human Geography*. Epub ahead of print 11 August 2016. DOI: 10.1177/0309132516662147.

Anderson B (2010) Preemption, precaution, preparedness: Anticipatory action and future geographies. *Progress in Human Geography* 34(6): 777–798.

Aradau C and Van Munster R (2011) *Politics of Catastrophe: Genealogies of the Unknown*. London: Routledge.

Braidotti R (2013) *The Posthuman*. Cambridge: Polity.

Bratton B (2016) *The Stack: On Software and Sovereignty*. Cambridge, MA: MIT Press.

Calo R, Froomkin M and Kerr I (eds) (2016) *Robot Law*. Cheltenham: Edward Elgar.

Cooper M (2008) *Life as Surplus: Biotechnology and Capitalism in the Neoliberal Era*. Seattle, WA: University of Washington Press.

Crary J (2013) *24/7: Late Capitalism and the Ends of Sleep*. London: Verso.

Crawford K and Schultz J (2014) Big data and data protection: Toward a framework to redress predictive privacy harms. *Boston College Law Review* 55(1): 93–128.

Cukier K and Mayer-Schönberger V (2013) *Big Data: A Revolution That Will Transform How We Live, Work and Think*. New York: Houghton Mifflin Harcourt.

De Goede M (2012) *Speculative Security: The Politics of Pursuing Terrorist Monies*. Minneapolis, MN: University of Minnesota Press.

De Goede M and Sullivan G (2016) The politics of security lists. *Environment and Planning D: Society and Space* 34(1): 67–88.

Elden S (2013) Secure the volume: Vertical geopolitics and the depths of power. *Political Geography* 34(1): 35–51.

Erickson P, Klein J, Daston L, Lemov R, Sturm T and Gordin M (2013) *How Reason Almost Lost Its Mind: The Strange Career of Cold War Rationality*. Chicago, IL: Chicago University Press.

Galison P (1994) The ontology of the enemy: Norbert Wiener and cybernetic anxiety. *Critical Inquiry* 21(1): 228–266.

Gillespie T (2012) Can an algorithm be wrong? *Limn* 2. Available at: http://limn.it/can-an-algorithm-be-wrong (accessed 12 September 2016).

Gillespie T (2014) The relevance of algorithms. In: Gillespie T, Boczkowski P and Foot K (eds) *Media Technologies: Essays on Communication, Materiality, and Society*. Cambridge, MA: MIT Press, 167–194.

Gillespie T (2016) Algorithm. In: Peters B (ed.) *Digital Keywords: A Vocabulary of Information Society & Culture*. Princeton, NJ: Princeton University Press, 18–30.

Graham S (2016) *Vertical: The City from Above and Below*. London: Verso.

Greenwald G (2014) *No Place to Hide: Edward Snowden, the NSA, and the Surveillance State*. London: Penguin.

Gregory D (2011) From a view to a kill: Drones and late modern war. *Theory, Culture & Society* 28(7–8): 188–215.
Grusin R (2010) *Premediation: Affect and Mediality After 9/11*. Basingstoke: Palgrave Macmillan.
Halpern O (2015) *Beautiful Data: A History of Vision and Reason Since 1945*. Durham, NC: Duke University Press.
Haraway D (1988) Situated knowledges: The science question in feminism and the privilege of partial perspective. *Feminist Studies* 14(3): 575–599.
Haraway D (1997) *Modest_Witness@Second_Millennium. FemaleMan©_Meets_ Oncomouse*. New York: Routledge.
Harding L (2014) *The Snowden Files: The Inside Story of the World's Most Wanted Man*. New York: Vintage.
Hayles NK (1999) *How We Became Posthuman: Virtual Bodies in Cybernetics, Literature and Informatics*. Chicago, IL: University of Chicago Press.
Hayles NK (2012) *How We Think: Digital Media and Contemporary Technogenesis*. Chicago, IL: Chicago University Press.
Heath-Kelly C (2016) Algorithmic autoimmunity in the NHS: Radicalisation and the clinic. *Security Dialogue.* Epub ahead of print 18 October 2016. DOI: 10.1177/0967010616671642.
Hu TH (2015) *A Pre-History of the Cloud*. Cambridge, MA: MIT Press.
Lally N (2016) Crowdsourced surveillance and networked data. *Security Dialogue*. Epub ahead of print 5 September 2016. DOI: 10.1177/0967010616664459.
Lemov R (2015) *Database of Dreams: The Lost Quest to Catalog Humanity*. New Haven, CT: Yale University Press.
Mollicchi S (2016) Flatness versus depth: A study of algorithmically generated camouflage. *Security Dialogue.* Epub ahead of print 5 September 2016. DOI: 10.1177/0967010616650227.
Parisi L (2013) *Contagious Architecture: Computation, Aesthetics, and Space*. Cambridge, MA: MIT Press.
Parks L (2016) Drones, vertical mediation, and the targeted class. *Feminist Studies* 42(1): 227–235.
Raley R (2016) Algorithmic translations. *CR: The New Centennial Review* 16(1): 115–137.
Roberts SL and Elbe S (2016) Catching the flu: Syndromic surveillance, algorithmic governmentality and global health security. *Security Dialogue*. Epub ahead of print 7 September 2016. DOI: 10.1177/0967010616666443.
Salter M (ed.) (2016) *Making Things International 2: Catalysts and Reactions*. Minneapolis, MN: University of Minnesota Press.
Shaw I (2016) *Predator Empire: Drone Warfare and Full Spectrum Dominance*. Minneapolis, MN: University of Minnesota Press.
Singer P (2009) *Wired for War: The Robotics Revolution and Conflict in the 21st Century*. New York: Penguin.
Striphas T (2015) Algorithmic culture. *European Journal of Cultural Studies* 18(4–5): 395–412.
Suchman L and Weldes J (2016) Human–machine antinomies. In: Bhuta N, Beck S, Geiss R, Liu H and Kress C (eds) *Autonomous Weapons Systems: Law, Ethics, Policy*. Cambridge: Cambridge University Press, 75–102.
Uncertain Commons (2013) *Speculate This!* Durham, NC: Duke University Press.
Wilcox L (2016) Embodying algorithmic war: Gender, race, and the posthuman in drone warfare. *Security Dialogue*. Epub ahead of print 7 September 2016. DOI: 10.1177/0967010616657947.

Louise Amoore is Professor of Political Geography at Durham University. She is the author of *The Politics of Possibility* (Duke University Press, 2013), co-editor of *Algorithmic Life* (Routledge, 2016) and has recently published articles on data analytics and cloud computing. She holds a Leverhulme Major Research Fellowship (2016–2018) in which she is writing a book on the *Ethics of Algorithm.*

Rita Raley is Associate Professor of English at the University of California – Santa Barbara. Her research interests lie at the intersection of digital media and humanist inquiry, with a particular focus on cultural critique, artistic practices, language and textuality. She is the author of *Tactical Media* (University of Minnesota Press, 2009), co-editor of the *Electronic Literature Collection 2* (Electronic Literature Organization, 2011) and has recently published articles on media arts practices and digital poetics.