Forthcoming Chapter in: Daniela Agostinho, Solveig Gade, Nanna Thylstrup & Kristin Veel (eds) **(W)archives. Archival imaginaries and contemporary wars (2020)** Berlin: Sternberg Press

Archives of Enmity and Martial Epistemology

Kevin McSorley

Introduction

How might we think the linkages between war and the archive? At a foundational level, war is itself an act of political contestation *and* inscription, a continuous and injurious process of archiving that is written upon the myriad bodies of the victims it generates and the lifeworlds it transforms. As Elaine Scarry notes, it is bodily injury that is ultimately crucial to war's political mattering, that provides the radical material force to suture and substantiate the political "crisis of substantiation" that war entails.[1] War unmakes and remakes worlds, then, its outcomes recorded in an archive of broken bodies and destroyed lives, a transubstantiation of political ideals into flesh.

At another level, war-fighting is also underpinned by myriad processes of intelligence-gathering, surveillance, and reconnaissance, and other techniques of operational data collection about the nature of "enemy" forces, formations, and activities. The planning of military violence fundamentally depends upon the compilation, organization, and interrogation of such information to generate actionable reports in the form of kill lists, enemy orders of battle, target mappings and matrices. It is through such archival procedures that particular bodies, infrastructures, and environments ultimately become identified as targets for the subsequent injury and destruction that underwrites political mattering. However, as Derrida notes, the process of "archivization produces as much as it records,"[2] and the question of *how* particular understandings of the structure of enmity get inscribed and produced in these archival regimes and manipulations is the focus of this chapter.

As one historical example, consider the United States Air Force's (USAF) establishment post-World War II of a Directorate of Targets, which was responsible for compiling what eventually came to be

[1] Elaine Scarry, *The Body in Pain: The Making and Unmaking of the World* (Oxford: Oxford University Press, 1985).

[2] Jacques Derrida, *Archive Fever: A Freudian Impression* (Chicago: University of Chicago Press, 1995), 17.

known as "The Bombing Encyclopedia of the World" (BEW).[3] This was an archive constructed at a global scale containing records of thousands of military installations, industrial plants, and other elements of vital infrastructural systems—electricity, petroleum, transportation, water, steel, etc.—"the destruction of which would cut across […] the enemy's ability to defend himself."[4] Although initially focused upon the Soviet Bloc, the project rapidly expanded throughout the 1950s to cover Western Europe, the Far East, and beyond. By 1959, seventy-eight thousand potential bombing targets had been produced, rendering large parts of the world through a particular military grid of intelligibility.

While images from aerial reconnaissance became crucial as the project developed, the key initial source of data for the BEW in its early years was human intelligence obtained via Project Wringer.[5] This was a vast program of mass debriefing and interrogation of over three hundred thousand human subjects, mostly German and Japanese ex-servicemen, returning from postwar detention and forced labor in the Soviet Union. Elliott Child details how millions of oral accounts and memory sketches of installations and plants were systematically obtained from these "human sources" and fed back to USAF target compilers in Washington, where, guided by rationalized and productivist principles of industrial managerialism, the accounts were "stripped of subjectivity" and bureaucratically transformed, disarticulated, and recombined to form abstract and codified targeting records.[6]

Importantly for the purposes of the current discussion, the material form in which individual records were initially stored was punched cards that could be read by early Univac computers built specifically for the Department of Defense. Subsequently the records were encoded in a standardized format, the Consolidated Target Intelligence File, on magnetic tapes that allowed more rapid automatic machine processing.[7] Each record in the archive had multiple data fields, detailing the

---

[3] Stephen Collier and Andrew Lakoff, "The Bombing Encyclopedia of the World," *Limn*, no. 6. (2016), http://limn.it/the-bombing-encyclopedia-of-the-world/; Derek Gregory, "Bombing Encyclopedia of the World," August 3, 2012, https://geographicalimaginations.com/2012/08/03/bombing-encyclopedia-of-the-world/.

[4] James Lowe (1946, 7), cited in Collier and Lakoff, "The Bombing Encyclopedia of the World". Lowe, James T. "Intelligence in the Selection of Strategic Target Systems." lecture, Air War College, Maxwell Air Force Base, Alabama. (1946) Documents M-U 38043 L913i. Muir S. Fairchild Research Information Center, Air University.

[5] Elliott Child, "Through the Wringer: Mass Interrogation and United States Air Force Targeting Intelligence in the Early Cold War," *Political Geography*, no. 75 (2019), https://doi.org/10.1016/j.polgeo.2019.102052.

[6] Child, "Through the Wringer."

[7] Gregory, "Bombing Encyclopedia of the World."

geolocation, industrial outputs and capabilities, and various other aspects of the site. As these records were not organized by a single, rigid system of classification, they could be queried on machine runs that would generate targeting reports according to various strategic criteria such as all the sites within a specific area that might contribute to particular production cycles, e.g. of fighter planes.[8]

This, then, was an open-ended archiving of the vital infrastructures and productive capacities of modern military-industrial economies and societies, where the specific information architecture facilitated the flexible generation of myriad targeting reports detailing multiple material flows, interdependencies, and critical vulnerabilities. The archive thus encoded a particular martial epistemology and enabled the production of new knowledge about various ways in which the military capabilities of enemy societies might be constituted and could be vulnerable to attack.[9] It marked an important moment in twentieth-century war-fighting in which a particular type of database storage and querying system emerged as a key technocultural form for the flexible planning of military violence, as well as offering an early instantiation of a totalizing ambition to disclose the entire world's existent and emergent structures of enmity.[10]

It is the construction of such *archives of enmity* through the organization of "military information regimes," defined by McCoy as "sophisticated systems for collecting, codifying and operationalizing voluminous amounts of data about whole societies,"[11] and in particular the development of new

[8] Collier and Lakoff, "The Bombing Encyclopedia of the World."

[9] Collier and Lakoff, "The Bombing Encyclopedia of the World."

[10] Collier and Lakoff argue that this Cold War analysis of enemy societies was also turned inward in the second half of the twentieth century, leading to a new reflexive self-understanding and governance of domestic urban and infrastructural planning according to principles of "vital systems security." The enemy city targeted thus became the homeland city dispersed and suburbanized in preventive anticipation of attack. Stephen Collier and Andrew Lakoff, "Vital Systems Security: Reflexive Biopolitics and the Government of Emergency," *Theory Culture and Society* 32, no. 2 (2015): 19–51.

[11] Alfred McCoy, "Imperial Illusions: Information Infrastructure and the Future of US Global Power," in *Endless Empire: Spain's Retreat, Europe's Eclipse, America's Decline*, ed. Alfred McCoy, Josep Fradera, and Stephen Jacobson (Madison: University of Wisconsin Press, 2012), 361–62. McCoy proposes an overarching schema of three main "military information regimes"—manual, computerized, and robotic—that have characterized US conventional and counterinsurgency/pacification war-fighting over the last century, all designed to reduce complex societies to "serviceable data": "Despite an enormous expansion into a global system during World War II, Washington's data management remained, until the 1950s, largely manual with typewritten files, numeric codification, and limited mechanical assistance for transmission and tabulation. From the 1960s onward, however, a computerized information infrastructure emerged

computational and database technologies, that is the focus of attention here. What distinct understandings of enmity, what "ontology of the enemy,"[12] gets inscribed and produced through such archival developments? While war is undoubtedly a crucible of technological innovation,[13] it is beyond the scope of this chapter to provide a comprehensive genealogy of the ways in which changes in war-fighting and transformed understandings of enmity have coevolved with historical transformations in computational and data-processing technologies.[14] Rather, I will predominantly focus here upon exploring the advent of specific forms of data-driven warfare that are associated particularly with recent developments in ubiquitous sensing and immanent archiving, evolutions in "post-relational" database architectures and analytics, and certain doctrinal and operational shifts away from conventional large-scale warfare against nation-state adversaries and regular formations, and toward forms of discontinuous and open-ended military violence directed across the globe against networked and individual antagonists.[15]

---

during the Vietnam War with automated data processing and electronic communications. After a decade of combat in Iraq and Afghanistan, the Pentagon was, by 2010, at the edge of a robotic information regime that will fuse aerospace, cyberwarfare, and biometrics into a worldwide surveillance and strike network of unprecedented power" (362).

[12] In an analysis of Norbert Weiner's development of cybernetic defense systems, Galison argues that the way the enemy figure was understood and inscribed within such human/machine assemblages differed from the racialized figure of the enemy "other" that existed in public discourses. Peter Galison, "The Ontology of the Enemy: Norbert Wiener and the Cybernetic Vision," *Critical Inquiry* 21, no. 1 (1994): 228–66.

[13] While cautioning against simplistic narratives that stress either the overwhelming determining force of the exigencies of war-fighting upon technical change, or the uniquely transformative effects of particular technologies upon the conditions of war, Bousquet nonetheless notes that "armed conflict is undoubtedly a particularly potent accelerant for technological evolution, concentrating minds and resources and subject to an intense dynamic of action–reaction between belligerents that singularly spurs innovation." Antoine Bousquet, "A Revolution in Military Affairs? Changing Technologies and Changing Practices of Warfare," in *Technology and World Politics: An Introduction*, ed. Daniel McCarthy (Abingdon: Routledge, 2018), 173.

[14] For studies which might contribute to such an undertaking, see e.g. Josef Ansorge, *Identify and Sort: How Digital Power Changed World Politics* (Oxford: Oxford University Press, 2016); Oliver Belcher, "The Afterlives of Counterinsurgency: Postcolonialism, Military Social Science, and Afghanistan 2006–2012" (PhD diss., University of British Columbia, 2013); Oliver Belcher, "Sensing, Territory, Population: Computation, Embodied Sensors, and Hamlet Control in the Vietnam War," *Security Dialogue* 50, no. 5 (2019): 416–36; Antoine Bousquet, "Cyberneticizing the American War Machine: Science and Computers in the Cold War," *Cold War History* 8, no. 1 (2008): 77–102; Paul Edwards, *The Closed World: Computers and the Politics of Discourse in Cold War America* (Cambridge, MA: MIT Press, 1996); James Gibson, *The Perfect War: Technowar in Vietnam* (New York: Avalon, 2000); Katherine Hayles, *How We Became Posthuman* (Chicago: University of Chicago Press, 1999); McCoy, "Imperial Illusions"; Ian Shaw, *Predator Empire: Drone Warfare and Full Spectrum Dominance* (Minneapolis: University of Minnesota Press, 2016).

[15] Frédéric Gros, *States of Violence: An Essay on the End of War* (Chicago: University of Chicago Press, 2010); Derek

Immanent Archiving and Emergent Enmity

The contemporary moment is one marked by increasingly ubiquitous, networked, and automated forms of "data" production, with ever more interactions and practices of quotidian life—communication, consumption, finance, travel, leisure, social networking, online identity curation, interfacing with the "Internet of Things," simply moving while carrying a cell phone—generating immanent data trails that are recorded as a matter of course across permanently updating and reconfigurable archives that stretch the very definition of the word.[16] Much of embodied existence is thus now productive of "data exhaust" or "ontic exhaust,"[17] with being-archived increasingly an ontological condition of contemporary living, producing an oceanic cacophony of data.[18]

It is worth noting here that many of the technologies, protocols, and logics that are central to this datafication of everyday life have been significantly shaped by defense funding and military aspirations. For example, the genealogy of Internet protocols such as TCP/IP is fundamentally entangled with military desires for resilient networking,[19] and the development of location-based services and targeting is fundamentally dependent upon GPS technology originally designed for the navigation of weapons systems.[20] Martial desires have thus long been intertwined with the wider parameters of everyday technocultural becoming, enframing human life in complex recursive processes of technogenesis,[21] with "civilianized" technologies becoming central to the way that the contemporary (post)human subject has increasingly become constituted as an informational entity or node, as a signal transmitter in military terms.

These and related developments have been variously theorized in terms of "surveillance

---

Gregory, "The Everywhere War," *Geographical Journal* 177, no. 3 (2011): 238–50; Glenn Voelz, "The Individualization of American Warfare," *Parameters* 45, no. 1 (2015): 99–111.

[16] Holger Potzsch, "Archives and Identity in the Context of Social Media and Algorithmic Analytics: Towards an Understanding of iArchive and Predictive Retention," *New Media & Society* 20, no. 9 (2018): 3304–22.

[17] Mark Jarzombek, *Digital Stockholm Syndrome in the Post-Ontological Age* (Minneapolis: University of Minnesota Press, 2016).

[18] Ed Finn, *What Algorithms Want: Imagination in the Age of Computing* (Cambridge, MA: MIT Press, 2017).

[19] Janet Abbate, *Inventing the Internet* (Cambridge, MA: MIT Press, 1999).

[20] Caren Kaplan, "Precision Targets: GPS and the Militarization of Everyday Life," *Canadian Journal of Communication* 38, no. 3 (2013): 397–420.

[21] Hayles, *How We Became Posthuman*.

capitalism,"[22] "data colonialism,"[23] the "sensor society,"[24] and the rise of "big data."[25] The emergence of big data is said to be changing the overall ways in which sense-making might occur, ushering in a paradigm shift in how knowledge of the world may be generated, and with it transformations in the ways in which life may be governed through such data.[26] Kitchin argues that "big data analytics enable an entirely new epistemological approach for making sense of the world; rather than testing a theory by analyzing relevant data, new data analytics seek to gain insights 'born from the data.'"[27] For Andersen, the data deluge is ushering in an "end of theory" whereby pattern recognition and correlation outstrip the understandings offered by models of causality, intentionality, or ideology: "Out with every theory of human behavior, from linguistics to sociology. Forget taxonomy, ontology and psychology. Who knows why people do what they do? The point is they do it, and we can track and measure it with unprecedented fidelity. With enough data, the numbers speak for themselves."[28]

Further, unlike "modernist" processes of knowledge production, immanent data collection that happens as a by-product of daily life is more speculative and occurs without necessarily anticipating the uses to which it may be put, without a clear question or purpose in mind.[29] Andrejevic and Burdon thus note that "function creep is not ancillary to the data collection process but is built into it, the function *is* the creep,"[30] and as such commercial and military information regimes often overlap and

---

[22] Shoshana. Zuboff, *The Age of Surveillance Capitalism* (London: Profile Books, 2019).

[23] Nick Couldry and Ulises Mejias, "Data Colonialism: Rethinking Big Data's Relation to the Contemporary Subject," *Television & New Media* 20, no. 4 (2019): 336–49. Couldry and Mejias predominantly emphasize how colonial and capitalist logics of extraction, accumulation, and commodification, rather than e.g. securitization, underpin contemporary "data" production. They argue that increasingly, the very texture of social life itself is being reconfigured as a potential resource for expropriation, whereby "digital platforms […] *produce* a new type of 'social' for capital: that is, the social in a form that can be continuously tracked, captured, sorted and counted for value as 'data'" (341).

[24] Mark Andrejevic and Mark Burdon, "Defining the Sensor Society," *Television & New Media* 16, no. 1 (2015): 19–36.

[25] David Lyon, "Surveillance, Snowden, and Big Data: Capacities, Consequences, Critique," *Big Data & Society* 1, no. 2 (2014): 1–13; Rob Kitchin, "Big Data, New Epistemologies and Paradigm Shifts," *Big Data & Society* 1, no. 1 (2014): 1–12.

[26] David Chandler, "A World without Causation: Big Data and the Coming of Age of Posthumanism," *Millennium* 43, no. 3 (2015): 833–51.

[27] Kitchin, "Big Data, New Epistemologies and Paradigm Shifts," 2.

[28] Chris Andersen, "The End of Theory: The Data Deluge Makes the Scientific Method Obsolete," *Wired*, no. 16 (2008): para. 7, http://archive.wired.com/science/discoveries/magazine/16-07/pb_theory.

[29] Chandler, "A World without Causation."

[30] Andrejevic and Burdon, "Defining the Sensor Society," 32.

inform one another in deeply symbiotic relationships. Indeed, recent histories have detailed longstanding dual-use hybridity and the continuing inseparability of military interests from the shaping of the structures of innovation, regulatory frameworks, practices, and values of the commercial data-tech giants of Silicon Valley.[31]

This epistemological approach is transforming numerous domains of social life, but particularly the realm of security broadly conceived, and notably in a context in which it was argued that the 9/11 attacks could have been predicted if only the US security agencies had somehow been able to "connect up the dots" in already existent data,[32] to see the patterns of emergent enmity prior to the event, rather than in post hoc reconstruction. Haunted by this question of "how did we miss it?" the US security state has increasingly been concerned with how to unlock the potential that was felt to exist in the broad dataverse, to recombine or manipulate or reterritorialize it in ways that might be specifically revelatory for security and military concerns. With data seen as a potential reservoir of previously untapped insights, the possibility of preemptively tracing the latent "threatprint,"[33] the emergent signature of insecurity or enmity, within and across various data archives has assumed new salience.

The idea that new knowledge production might occur through big data analytics, operating at speeds and scales exceeding human perception and cognition,[34] has thus increasingly become a significant

[31] John Foster and Robert McChesney, "Surveillance Capitalism: Monopoly-Finance Capital, the Military-Industrial Complex, and the Digital Age," *Monthly Review* 66, no. 3 (2014), https://doi.org/10.14452/MR-066-03-2014-07_1; Yasha Levine, *Surveillance Valley: The Secret Military History of the Internet* (London: Icon Books, 2019); Margaret O'Mara, *The Code: Silicon Valley and the Remaking of America* (London: Penguin, 2019). Levine's analysis of the "military-digital complex" thus argues that "the Internet was hardwired to be a surveillance tool from the start. No matter what we use the network for today […] it always had a dual-use nature rooted in intelligence gathering and war" (2). Foster and McChesney conclude their analysis of the history and political economy of surveillance capitalism by arguing that "the digital revolution must be demilitarized and subjected to democratic values and governance, with all that entails."

[32] United States Joint Inquiry, "Report of the Joint Inquiry into the Terrorist Attacks of September 11, 2001," Washington DC: House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence, 2003.

[33] Alexandra Hall and Jonathan Mendel, "Threatprints, Threads and Triggers: Imaginaries of Risk in the 'War on Terror,'" *Journal of Cultural Economy* 5, no. 1 (2012): 9–27.

[34] Louise Amoore, "Cloud Geographies: Computing, Data, Sovereignty," *Progress in Human Geography* 42, no. 1 (2016): 4–24.

new *doxa* of the security professions,[35] with intelligence agencies and analytic labor being restructured for an age of "digital warfare."[36] There has been massive investment in an amalgam of practices including interoperable data exchange and database interconnectivity, new forms of social network analysis, risk profiling and predictive analytics, machine learning and artificial intelligence, advanced data visualization, and so on. Such practices are transforming intelligence work, policing, homeland security, counterterrorist practice, and counterinsurgency warfare.[37]

With the rise of automated and ubiquitous forms of mass data collection across entire populations, one key epistemological principle of the big data paradigm is that the very heterogeneity of the mass is reconceptualized not as an obfuscatory haystack, but as an asset whose very complexity can reveal new patterns and connections.[38] The economy of knowledge, then, is to *archive it all*,[39] in order that heterogeneous plural normalities and the anomalous, the haystack and the needle, might emerge together.[40] Indeed, the bigger the data, the more self-correcting it is understood to be. The logic here, then, is not simply the traditional disciplinary idea that particular suspect communities might become subject to more targeted surveillance, but that the mass archiving of the lifeworlds of entire populations might lead to the emergence of new forms of knowledge and targets, might surface currently unknown unknowns: "The population-level portrait allows particular targets to emerge, and once they do, their activities can be situated in the context of an ever-expanding network of behaviors

---

[35] Claudia Aradau, "The Signature of Security: Big Data, Anticipation, Surveillance," *Radical Philosophy*, 191 (May–June 2015): 21–28.

[36] David Rohde, "Digitizing the CIA: John Brennan's Attempt to Lead America's Spies into the Age of Cyberwar," *Reuters*, November 2, 2016, https://www.reuters.com/investigates/special-report/usa-cia-brennan/.

[37] See *inter alia* Louise Amoore, "Algorithmic War: Everyday Geographies of the War on Terror," *Antipode* 41, no. 1 (2009): 49–69; Louise Amoore, *The Politics of Possibility: Risk and Security Beyond Probability* (Durham, NC: Duke University Press, 2013); Eli Berman, Joseph Felter, and Jacob Shapiro, *Small Wars, Big Data: The Information Revolution in Modern Conflict* (Princeton, NJ: Princeton University Press, 2018); Roberto Gonzales, "Seeing into Hearts and Minds: 'Big Data,' Algorithms, and Computational Counterinsurgency," *Anthropology Today* 31, no. 4 (2015): 13–18.

[38] Aradau, "The Signature of Security"; Charlotte Heath-Kelly, "Algorithmic Autoimmunity in the NHS: Radicalisation and the Clinic," *Security Dialogue* 48, no. 1 (2017): 29–45.

[39] As encapsulated in DARPA's "Total Information Awareness" program (see e.g. Lyon, "Surveillance, Snowden, and Big Data") and the National Security Agency's (NSA) characterization of its own data collection posture as "Sniff it all, know it all, collect it all, process it all, exploit it all." Jon Queally, "NSA Global Spy Stations Revealed: 'Sniff It All, Collect It All, Know It All, Process It All, Exploit It All,'" *Common Dreams*, March 7, 2015.

[40] Aradau, "The Signature of Security."

and the patterns these generate."[41]

While patterns of suspicious activity may be sought in individual and discrete archives of e.g. travel data, financial transactions, or communicative metadata, in addition databases and archives, unmoored from their commercial purposes, are also fused together via new combinatorics to generate a multidimensional higher-level feature space that offers new possibilities for inquiry and intervention.[42] Vast computational power and new-generation database designs and query languages mean that the rapid, dynamic, and generative interrogation of massive open-ended, semi-structured, and scalable data sets is now possible. With the definition of a few rules or boundary conditions, algorithms may rapidly search such a problem space for data patterns and anomalies. A one-way airfare between particular locations, a pattern of chatter on social media, a GPS trace along a particular route, or a large transaction between particular accounts may all be meaningless and absolutely inauspicious in isolation, part of the curves of many everyday normalities.[43] But if associatively traced and linked across a higher-level feature space, then the network mapped and the traces conjoined may be calculated and recognized as the potential surfacing of threat or enmity. As Amoore and de Goede note, "the deviant other, then, is identified not so much through her individual aberration from a norm, but through an assembly of transactions or associations seen as signifying suspicious activity."[44]

The threatprint of the enemy-to-come is thus now understood in terms of this complex ontology of *association* across a multidimensional feature space, the relations between elements more significant than the individual elements per se. The inductive and iterative generation of new security derivatives[45] assembled from the myriad relationships between heterogeneous sources of data widens the analytic field and creates new potentialities for investigation and possible intervention, surfacing patterns for the attention of the analyst. For Pasquinelli, this "introduction of the topological

---

[41] Andrejevic and Burdon, "Defining the Sensor Society," 23.

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

[43] Louise Amoore, "Data Derivatives: On the Emergence of a Security Risk Calculus for Our Times," *Theory, Culture and Society* 28, no. 6 (2011): 24–43.

[44] Louise Amoore and Marieke de Goede, "Transactions after 9/11: The Banal Face of the Preemptive Strike," *Transactions of the Institute of British Geographers* 33, no. 2 (2008): 178.

[45] Amoore, "Data Derivatives." Amoore notes that derivatives, e.g. in finance, are a speculative mode of data derived from, but also necessarily different than and hence partially indifferent to, the individual values or singularities of the underlying phenomena or data fields.

perspective to large datasets is the birth of a new symbolic form that is comparable to the birth of modern perspective using techniques of optical projection from astronomy."[46] Furthermore, enmity is increasingly understood in terms of the *anomalous*,[47] whereby "an anomaly can be detected only against the ground of a pattern regularity."[48] And recursive algorithms may continuously find, learn, and apply new rules from data contingencies and variations, generate new derivatives of derivatives, while patterns that are not anomalous are continuously folded back into the calculation of normalities. In this way, algorithms and thresholds may constantly modulate, change, and evolve. In cases of deep machine learning, the ultimate rationale for the emergence of outcomes may thus become increasingly opaque and inscrutable even to the analysts deploying it.

Patterns of Life and Predatory War

Drawing partly upon such principles, the twenty-first century battlespaces of the "everywhere war"[49] have become laboratories for experimentation in the archival and analytic underpinnings of military violence. The US wars in Iraq and Afghanistan in particular involved the transformation and accelerated tempo of special forces-led operational intelligence cycles, the society-wide "reality-mining" of myriad data sources for programs of "computational counterinsurgency,"[50] and an analytic

---

[46] Matteo Pasquinelli, "Arcana Mathematica Imperii: The Evolution of Western Computational Norms," in *Former West: Art and the Contemporary after 1989*, ed. Maria Hlavajova and Simon Sheikh. (Cambridge, MA: MIT Press, 2017), 290.

[47] Claudia Aradau and Tobias Blanke, "Governing Others: Anomaly and the Algorithmic Subject of Security," *European Journal of International Security*, no. 1 (February 2018): 1–21.

[48] Matteo Pasquinelli, "Anomaly Detection: The Mathematization of the Abnormal in the Metadata Society," 2015, http://matteopasquinelli.com/anomaly-detection/.

[49] Gregory, "The Everywhere War."

[50] Belcher's analysis of computational counterinsurgency details how the US occupation accumulated massive amounts of disparate data on Afghan society through traditional means such as informants and police reports, significant activities reports from patrols, biometric technologies deployed at checkpoints, cell phone data, and even metrics supposedly indicating local "confidence and security" such as commodity prices in markets. Military projects such as Nexus 7 then subjected this disparate data to "dynamic network analysis" in order to produce models, predictions, and visualizations thought to reveal the structural patterns, rhythms, and movements of insurgency through the Afghan population, with the results used to orient the deployment of further military resources. As Belcher notes, the fundamental working assumption of this program was an underlying vision of the "networked enemy," an ontology of enmity that was further naturalized in these programs of computational counterinsurgency. Belcher, "The Afterlives of Counterinsurgency." See also Gonzales, "Seeing into Hearts and Minds"; Sharon Weinberger, *The Imagineers of War: The Untold Story of Darpa, the Pentagon Agency That Changed the World* (New York: Alfred A. Knopf, 2017).

preoccupation with disclosing networked forms and patterns of enmity within the wider population rather than understanding social and political concerns at the local level.[51] Furthermore, beyond these specific wars of occupation, rolling programs of punctuated military violence, particularly in the form of targeted drone strikes, have also been carried out by the United States Joint Special Operations Command and the Central Intelligence Agency (CIA) under the sign of counterterrorism across many other territories including Pakistan's Federally Administered Tribal Areas (FATA), Yemen, and Somalia, as will be discussed below.

While the drone strike is the signature motif of this form of "predatory war,"[52] it is important to initially emphasize that the drone itself is merely one element in a whole archival apparatus of sensors, databases, and algorithms, and that "cut off from its back end, from its satellite links and its data processors, its intelligence analysts and its controller, the drone is as useless as an eyeball disconnected from the brain."[53] Predatory war exemplifies both the individuation of warfare and the dissolution of the spatiotemporal and normative constraints of the conventional battlefield.[54] As Gregory and Chamayou note,[55] the locus of violence for drone strikes is defined by the presence of the individualized enemy, with "the target contracted to the individual human body even as the field of military violence expands to encompass the globe."[56]

One aspect of predatory war that deserves particular attention here is the procedure for the disclosure, the anticipatory surfacing, of particular targets - so-called "signature strikes" - who may never be known or identified, but who emerge on the basis of activity rather than identity from a "vast and

---

[51] Belcher, "The Afterlives of Counterinsurgency"; Gregoire Chamayou, "Oceanic Enemy: A Brief Philosophical History of the NSA," *Radical Philosophy*, 191 (May–June 2015): 2–12; Matthew Ford, "Finding the Target, Fixing the Method: Methodological Tensions in Insurgent Identification," *Studies in Conflict and Terrorism* 35, no. 2 (2012): 113–34.

[52] Kevin McSorley, "Predatory War, Drones and Torture: Remapping the Body in Pain," *Body and Society* 25, no. 3 (2019): 75–99.

[53] Mark Bowden, "The Killing Machines: How to Think about Drones," *The Atlantic*, August 14, 2013, para 12, http://www.theatlantic.com/magazine/archive/2013/09/the-killing-machineshow-to-think-about-drones/309434/.

[54] Antoine Bousquet, *The Eye of War: Military Perception from the Telescope to the Drone* (Minneapolis: University of Minnesota Press, 2019); Voelz, "The Individualization of American Warfare"; Kyle Grayson, "Six Theses on Targeted Killing," *Politics* 32, no. 2 (2012): 120–28; Gros, *States of Violence*.

[55] Derek Gregory, "Lines of Descent," in *From Above: War, Violence and Verticality*, ed. Peter Adey, Mark Whitehead, and Alison Williams (Oxford: Oxford University Press, 2013), 41–70; Gregoire Chamayou, *Drone Theory* (London: Penguin, 2015).

[56] Derek Gregory, "Drone Geographies," *Radical Philosophy*, no. 183 (2014): 14.

continually evolving database, known as the disposition matrix."[57] This archive does not just amass information on certain individuals, but rather records comprehensive data across a whole population, across the entire "life of the populace described as pre-insurgent,"[58] with blanket surveillance and targeted killing going hand in hand. As Shaw notes, "in order to individualize, the security state must first totalize."[59]

The disposition matrix draws on multiple sensors and sources in the generation of its open-ended kill lists, principally the many billions of elements of communicative metadata that the United States National Security Agency (NSA) routinely harvests daily, alongside further signals intelligence collected from drones acting as virtual base towers. Many US military drones capture all the available wireless data traffic in the areas through which they fly,[60] and the felt value of communicative metadata in particular is such that NSA General Counsel Stewart Baker has argued that "it absolutely tells you everything about somebody's life […]. If you have enough metadata, you don't really need content."[61] This data is supplemented by human intelligence from agents and informants, and visual surveillance imagery from drone feeds.[62]

From the combinatoric manipulation of all these various anonymous and "dividualized" traces of communication, geolocation, and activity, an archive of overall "patterns of life" in a digitally enclosed battlespace can be derived (indicating bodily movements and rhythms in space and time, gatherings of bodies, networks of speech and chatter, durational intensities of social connectivity, etc.). The interrogation of this multidimensional data topography is then conducted via algorithmic inquiry, including forms of social network analysis, time series analysis, and rhythmanalysis, with

---

[57] Greg Miller, "Plan for Hunting Terrorists Signals US Intends to Keep Adding Names to Kill Lists," *Washington Post*, October 23, 2012.

[58] Neal Curtis, "The Explication of the Social: Algorithms, Drones and (Counter-)terror," *Journal of Sociology* 52, no. 3 (2016): 528.

[59] Ian. Shaw, "The Urbanization of Drone Warfare," *Geographica Helvetica*, no. 71 (2016): 25.

[60] Andrejevic and Burdon, "Defining the Sensor Society."

[61] Stewart Baker cited in David Cole, "We Kill People Because of Metadata," *New York Review of Books*, May 10, 2014. Indeed, General Michael Hayden, former director of the NSA and the CIA, has similarly attested that "we kill people based on metadata," cited in Cole, "We Kill People Because of Metadata."

[62] Derek Gregory, "The Territory of the Screen," *Mediatropes* 6, no. 2 (2016): 126–47; Jutta Weber, "Keep Adding: On Kill Lists, Drone Warfare and the Politics of Databases," *Environment and Planning D: Society and Space* 34, no. 1 (2016): 107–25.

the hermeneutic goal of identifying anomalous patterns of suspicion linked to particular networked nodes and "bodies out of place."[63] The process by which "an archive of lives […] will constitute a death warrant"[64] is thus one where anonymous and anomalous "data bodies" are fundamentally derived from digital traces of *activity*, as opposed to forms of individual *identity* anchored in e.g. biometric data. Via "cross-sensor cueing,"[65] such emergent targets may also become subject to further granular and more intense visual surveillance, including full-motion video feeds that may be watched by drone personnel or become subject to further machinic vision and interrogation,[66] and which ultimately inform the triggering of strikes.

As Nordin and Oberg note, one of the dangers of such a process of producing targets is that it is theoretically endless: "There will always be more targets than it is possible to destroy."[67] The logic of big data is ultimately one of continuous recommendation on the basis of noting similarities between patterns. Indeed, Paul Pillar, former director of the CIA's counterterrorism center, has stated that "we are looking at something that is potentially infinite."[68] For Jaffer, relatedly, the institutional danger is that, once established, "the legal and bureaucratic infrastructure required to sustain this practice […] will demand a [further] targeted-killing campaign."[69] Further, the likelihood of identifying false positives is heightened by such an archival reliance on metadata, where the meaning of communication or the qualitative context of association is abstracted.[70]

Moreover, the total archiving of an entire population inevitably introduces wider transformations of

---

[63] Lauren Wilcox, "Drone Warfare and the Making of Bodies out of Place," *Critical Studies on Security* 3, no. 1 (2015): 127–31.

[64] Chamayou, *Drone Theory*, 49.

[65] Pratap Chatterjee and Christian Stork, "Drone, Inc.: Marketing the Illusion of Precision Killing," *Corpwatch*, 2017, http://www.corpwatch.org/droneinc.

[66] United States Department of Defense, "Project Maven to Deploy Computer Algorithms to Wars," 2017, https://www.defense.gov/News/Article/Article/1254719/project-maven-to-deploy-computer-algorithms-to-war-zone-by-years-end/.

[67] Astrid Nordin and Dan Oberg, "Targeting the Ontology of War: From Clausewitz to Baudrillard," *Millennium* 43, no. 2 (2015): 401.

[68] Paul Pillar cited in Miller, "Plan for Hunting Terrorists."

[69] Jameel Jaffer, *The Drone Memos* (New York: New Press, 2016), 7.

[70] For example, the prominent Al Jazeera journalist Ahmad Muaffaq Zaidan was identified as a member of Al Qaeda by the NSA SKYNET program on the basis of communicative metadata generated in the course of his investigative work on the group (for further examples, see Chamayou, *Drone Theory*, 49–51).

the social for all those living under drones, ruptures that are regularly elided in narratives of precision targeting. As Curtis notes, "the implicit aspects of the social that the drone apparatus targets are that a person speaks and acts, moves and comes together with others […]. Drones make this very being-with explicit and problematic, if not dangerous and lethal."[71] Indeed, testimonies of the lives of those wider populations in territories such as FATA reveal widespread experiences and feelings of danger, exposure, paranoia, incomprehension, and helplessness.[72] Many mundane social interactions are felt to be newly precarious lest they attract the drones, with a consequent and profound undermining of all of the normal routines of everyday living, a stable interaction order, and any sense of ontological security and trust in the world.[73]

As Scarry notes, such a radical inversion and contraction of everything that is traditionally experienced as safe and benign, the unmaking of the victim's world, describes the very phenomenology and methodology of torture. However, in predatory war, this profound reversal and negation is scaled up from the site of the individual torture room to the assay and enclosure of the entire population and social lifeworld. As myriad everyday sayings and doings, moving and being-with others become targeted by the drone apparatus, the entire social environment is both unmade and weaponized, "the appropriation of the world into the torturer's arsenal of weapons."[74] For those already highly vulnerable populations who are subject to the intense necropolitical assay of predatory war, the phenomenology of their embodied experiences is thus not just of targeted killing, nor even of more widespread death, injury, grief, and destruction, although it is all of those. Rather, it is the very unmaking of their world, a profoundly asymmetric unmaking that increasingly approaches the underlying structure of mass torture, whereby an entire population may be "kept in a state of radical embodiment by its awareness that it is at any moment deeply woundable."[75]

---

[71] Curtis, "The Explication of the Social," 531.

[72] James Cavallaro, Stephan Sonnenberg, and Sarah Knuckey, "Living under Drones: Death, Injury and Trauma to Civilians from US Drone Practices in Pakistan," Stanford: International Human Rights and Conflict Resolution Clinic, Stanford Law School, 2012, https://law.stanford.edu/projects/living-under-drones/.

[73] McSorley, "Predatory War, Drones and Torture"

[74] Scarry, *The Body in Pain*, 45.

[75] Scarry, *The Body in Pain*, 80. As Metin Basoglu relatedly notes, "the overlap between features of drone warfare and torture is so striking that it deserves attention from both moral and legal perspectives […]. Inflicting severe and prolonged mental suffering on people essentially trapped in an 'inescapable shock' situation is no less morally abhorrent than torture and, at least from a behavioural science perspective, may well amount to mass torture." Metin Basoglu, "Drone Strikes

Conclusion

In this chapter, I have pointed to the production and naturalization of various ontologies of enmity through archival procedures underpinned by historical transformations in military information regimes and associated shifts in computational power and database architectures. Given that war is a constantly shape-shifting, but enduringly injurious, transhistorical, and transcultural social institution, this is clearly a very partial genealogy of the archive as a technology of epistemic and military violence,[76] one that invites further complication. By way of conclusion, I wish to highlight just a few of the issues that are provoked particularly by immanent digital archiving and the associated rise of forms of predatory war.

Firstly, and quite apart from the crucial ethico-political issues and violences that accompany such developments, it is important to note that many historical precursors and ambitious experiments in forms of total information awareness, granular targeting, and datafied warfare have been characterized by significant overreach, blowback, and failure to disrupt adaptive enemy capacity in the ways envisaged. For example, during the Vietnam War the establishment of the "electronic battlefield" to try to stop the north–south flow of enemy combatants and trucks along a key jungle supply route, the so-called Ho Chi Minh Trail in southeastern Laos, ended up being a costly fiasco.[77] Programs of reality-mining and computational counterinsurgency such as Nexus 7 in Afghanistan were unproven at best in their abilities to predict insurgent behavior.[78] Indeed, as Chamayou notes, the prosecution of the entire global war on terror has only exacerbated the incidence of terrorism

---

or Mass Torture? A Learning Theory Analysis," Metin Basoglu, November 11, 2012, https://metinbasoglu.wordpress.com/2012/11/25/drone-warfare-or-mass-torture-a-learning-theory-analysis/.

[76] Spivak uses the term "epistemic violence" when discussing the silencing and othering of marginalized groups and the privileging of colonial epistemic practices over local forms of knowledge. Gayatri Spivak, "Can the Subaltern Speak?" in *Marxism and the Interpretation of Culture*, ed. Cary Nelson and Lawrence Grossberg (Champaign: University of Illinois Press, 1988), 271–313. In an analysis of the computerized Hamlet Evaluation System deployed by the US in the Vietnam War, Belcher argues that "acts of translating the rich texture of hamlet and village life into an objectified information format constituted a unique form of 'epistemic violence,' rooted not so much in the narrative subjection of the 'Other,' but in the pure abstraction of life into a digitally stored data trace." Belcher, "Sensing, Territory, Population," 420.

[77] Gibson, *The Perfect War*; Bernard Nalty, *The War against Trucks: Aerial Interdiction in Southern Laos 1968–1972* (Washington, DC: US Air Force History and Museums Program, 2005).

[78] Belcher, "The Afterlives of Counterinsurgency"; Gonzales, "Seeing into Hearts and Minds"; Weinberger, *The Imagineers of War*.

worldwide, with the underlying premise of the existence of reliable individualized signatures of enmity yet to be found to hold up.[79] History thus suggests that caution is advisable when assessing the martial significance of any such developments, beyond noting the recurring attraction to militaries of technical systems and abstractions that promise to "project power without projecting vulnerability."[80] This hubristic compulsion also underpins the digital archive fever of contemporary martial power.[81]

That said, the promise of immanent archiving and big data analytics has clearly been inspiring renewed devotional and even magical thinking in military circles in recent years, with the notion of the algorithm in particular taking on its own performative force, becoming "an evocative shorthand for the power and potential of objective calculative systems that can think more accurately than humans."[82] "Algorithmic warfare" is a sign under which increasing quantities of resources, research, and development are being mobilized worldwide,[83] with the big data paradigm only strengthened by its hermetically sealed understanding of error and failure as that which gets enfolded back into the iterative refinement of its discriminatory powers.[84] As Kindervarter notes, visions of total access, infinite searchability, and digital omniscience have thus decisively entered the contemporary martial imagination.[85] The future trajectories of brutal developments such as predatory war thus remain troublingly unclear. While, as noted, previous martial experiments in total information awareness have often ultimately offered only ephemeral advantages and illusions of control, current archival assemblages in the laboratories of the imperial peripheries may nonetheless be harbingers of a much

---

[79] Chamayou, "Oceanic Enemy."

[80] Lieutenant General David Deptula, United States Air Force, cited in Chamayou, *Drone Theory*, 12.

[81] Relatedly, the broad US doctrine of low personnel, high-tech networked warfare characterized as the Revolution in Military Affairs (RMA) failed to survive the initial realities on the ground in the US occupations of the early twenty-first century. However, as Black notes, whatever objective assessment one might make of its military successes or failings, its very existence was revelatory of a wider set of Western cultural and political assumptions: "The RMA acts as a nexus for a range of developments and beliefs, including an unwillingness to accept conscription, a very low threshold for casualties, an assertion of Western superiority, and the ideology of machinism." Jeremy Black, *New Century War: Past, Present, Future* (London: Continuum, 2003), 97.

[82] David Beer, "The Social Power of Algorithms," *Information, Communication & Society* 20, no. 1 (2017): 11.

[83] United States Department of Defense, "Project Maven to Deploy Computer Algorithms to Wars"; Hague Center for Strategic Studies, "Artificial Intelligence and the Future of Defense," 2017, https://hcss.nl/report/artificial-intelligence-and-future-defense.

[84] Aradau, "The Signature of Security."

[85] Katharine Kindervarter, "The Emergence of Lethal Surveillance," *Security Dialogue* 47, no. 3 (2016): 223–38.

wider "great war of enclosure,"[86] one that increasingly turns its attention back toward the homeland, to "domestic societies conceived as battlespaces *in potentia*,"[87] and to producing the enemy within.

Finally, it remains crucial to study not only how such datafied targeting occurs, its archival infrastructure and algorithmic rendering of particular patterns of life and enmity, but also to explore how the knowledge of being permanently subject to this regime of intense necropolitical assay is understood and experienced by those who actually live with its torturous uncertainties, with the very unmaking of their social world. There are clearly numerous significant ethico-political issues that accompany the rise of predatory war—its lack of algorithmic transparency and the militarized culture of secrecy, its logic of endless expansion, its redistribution of the sovereign decision across recursive loops of automation, its adaptive driving of its actual adversaries further into civilian "hypercamouflage,"[88] even its cybernetic reconfigurations of its own operators' subjectivities. However, perhaps the most acute, particularly for those currently living under the drone apparatus, is its potential for apophenia, for "seeing patterns where none actually exist, simply because massive quantities of data can offer connections that radiate in all directions."[89] While from one point of view this may seem like a technical issue—the procedural collateral of radically opening up a search space—for those who are currently subject to predatory war, it is a matter of life and death.

Bibliography

Abbate, Janet. *Inventing the Internet*. Cambridge, MA: MIT Press, 1999.

Amoore, Louise. "Algorithmic War: Everyday Geographies of the War on Terror." *Antipode* 41, no. 1 (2009): 49–69.

Amoore, Louise. "Cloud Geographies: Computing, Data, Sovereignty." *Progress in Human Geography* 42, no. 1 (2016): 4–24.

Amoore, Louise. "Data Derivatives: On the Emergence of a Security Risk Calculus for Our Times." *Theory, Culture and Society* 28, no. 6 (2011): 24–43.

[86] Shaw, *Predator Empire.*

[87] Bousquet, *The Eye of War*, 193.

[88] Reza Negarestani, "The Militarization of Peace: Absence of Terror or Terror of Absence?" in *Collapse I*, ed. Robin Mackay (Oxford: Urbanomic, 2007), 53–92.

[89] danah boyd and Kate Crawford, "Critical Questions for Big Data," *Information, Communication & Society* 15, no. 5 (2012): 668.

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

Amoore, Louise., and Marieke. de Goede. "Transactions after 9/11: The Banal Face of the Preemptive Strike." *Transactions of the Institute of British Geographers* 33, no. 2 (2008): 173–85.

Andersen, Chris. "The End of Theory: The Data Deluge Makes the Scientific Method Obsolete." *Wired*, no. 16 (2008). http://archive.wired.com/science/discoveries/magazine/16-07/pb_theory.

Andrejevic, Mark, and Mark Burdon. "Defining the Sensor Society." *Television & New Media* 16, no. 1 (2015): 19–36.

Ansorge, Josef. *Identify and Sort: How Digital Power Changed World Politics*. Oxford: Oxford University Press, 2016.

Aradau, Claudia. "The Signature of Security: Big Data, Anticipation, Surveillance." *Radical Philosophy*, no. 191 (May–June 2015): 21–28.

Aradau, Claudia., and Tobias Blanke. "Governing Others: Anomaly and the Algorithmic Subject of Security." *European Journal of International Security*, no. 1 (February 2018): 1–21.

Basoglu, Metin. "Drone Strikes or Mass Torture? A Learning Theory Analysis." November 11, 2012. https://metinbasoglu.wordpress.com/2012/11/25/drone-warfare-or-mass-torture-a-learning-theory-analysis/.

Beer, David. "The Social Power of Algorithms." *Information, Communication & Society* 20, no. 1 (2017): 1–13.

Belcher, Oliver. "The Afterlives of Counterinsurgency: Postcolonialism, Military Social Science, and Afghanistan 2006–2012." PhD diss., University of British Columbia, 2013.

Belcher, Oliver. "Sensing, Territory, Population: Computation, Embodied Sensors, and Hamlet Control in the Vietnam War." *Security Dialogue* 50, no. 5 (2019): 416–36.

Berman, Eli., Joseph Felter, and Jacob Shapiro. *Small Wars, Big Data: The Information Revolution in Modern Conflict*. Princeton, NJ: Princeton University Press, 2018.

Black, Jeremy. *New Century War: Past, Present, Future*. London: Continuum, 2003.

Bousquet, Antoine. "Cyberneticizing the American War Machine: Science and Computers in the Cold War." *Cold War History* 8, no. 1 (2008): 77–102.

Bousquet, Antoine. *The Eye of War: Military Perception from the Telescope to the Drone*. Minneapolis: University of Minnesota Press, 2019.

Bousquet, Antoine. "A Revolution in Military Affairs? Changing Technologies and Changing Practices of Warfare." In *Technology and World Politics: An Introduction*, edited by Daniel McCarthy, 165–82. Abingdon: Routledge, 2018.

Bowden, Mark. "The Killing Machines: How to Think about Drones." *The Atlantic*, August 14, 2013. http://www.theatlantic.com/magazine/archive/2013/09/the-killing-machineshow-to-think-about-drones/309434/.

boyd, danah., and Kate Crawford. "Critical Questions for Big Data." *Information, Communication & Society* 15, no. 5 (2012): 662–79.

Cavallaro, James, Stephan Sonnenberg, and Sarah Knuckey. "Living under Drones: Death, Injury and Trauma to Civilians from US Drone Practices in Pakistan." Stanford: International Human Rights and Conflict Resolution Clinic, Stanford Law School, 2012. https://law.stanford.edu/projects/living-under-drones/.

Chamayou, Gregoire. *Drone Theory*. London: Penguin, 2015.

Chamayou, Gregoire. "Oceanic Enemy: A Brief Philosophical History of the NSA." *Radical Philosophy*, no. 191 (May–June 2015): 2–12.

Chandler, David. "A World without Causation: Big Data and the Coming of Age of Posthumanism." *Millennium* 43, no. 3 (2015): 833–51.

Chatterjee, Pratap., and Christian Stork. "Drone, Inc.: Marketing the Illusion of Precision Killing." *Corpwatch*, 2017. http://www.corpwatch.org/droneinc.

Child, Elliott. "Through the Wringer: Mass Interrogation and United States Air Force Targeting Intelligence in the Early Cold War." *Political Geography*, no. 75 (2019). https://doi.org/10.1016/j.polgeo.2019.102052.

Cole, David. "We Kill People Because of Metadata." *New York Review of Books*. May 10, 2014.

Collier, Stephen., and Andrew Lakoff. "Vital Systems Security: Reflexive Biopolitics and the Government of Emergency." *Theory, Culture and Society* 32, no. 2 (2015): 19–51.

Collier, Stephen., and Andrew Lakoff. "The Bombing Encyclopedia of the World." *Limn*, no. 6 (2016). http://limn.it/the-bombing-encyclopedia-of-the-world/.

Couldry, Nick., and Ulises Mejias. "Data Colonialism: Rethinking Big Data's Relation to the Contemporary Subject." *Television & New Media* 20, no. 4 (2019): 336–49.

Curtis, Neal. "The Explication of the Social: Algorithms, Drones and (Counter-)terror." *Journal of Sociology* 52, no. 3 (2016): 522–36.

Derrida, Jacques. *Archive Fever: A Freudian Impression*. Chicago: University of Chicago Press, 1995.

Edwards, Paul. *The Closed World: Computers and the Politics of Discourse in Cold War America*. Cambridge, MA: MIT Press, 1996.

Finn, Ed. *What Algorithms Want: Imagination in the Age of Computing*. Cambridge, MA: MIT Press, 2017.

Ford, Matthew. “Finding the Target, Fixing the Method: Methodological Tensions in Insurgent Identification.” *Studies in Conflict and Terrorism* 35, no. 2 (2012): 113–34.

Foster, John., and Robert McChesney. “Surveillance Capitalism: Monopoly-Finance Capital, the Military-Industrial Complex, and the Digital Age.” *Monthly Review* 66, no. 3 (2014). https://doi.org/10.14452/MR-066-03-2014-07_1.

Galison, Peter. “The Ontology of the Enemy: Norbert Wiener and the Cybernetic Vision.” *Critical Inquiry* 21, no. 1 (1994): 228–66.

Gibson, James. *The Perfect War: Technowar in Vietnam*. New York: Avalon, 2000.

Gonzales, Roberto. “Seeing into Hearts and Minds: ‘Big Data,’ Algorithms, and Computational Counterinsurgency.” *Anthropology Today* 31, no. 4 (2015): 13–18.

Grayson, Kyle. “Six Theses on Targeted Killing.” *Politics* 32, no. 2 (2012): 120–28.

Gregory, Derek. “Bombing Encyclopedia of the World.” August 3, 2012. https://geographicalimaginations.com/2012/08/03/bombing-encyclopedia-of-the-world/.

Gregory, Derek. “Drone Geographies.” *Radical Philosophy*, no. 183 (2014): 7–19.

Gregory, Derek. “The Everywhere War.” *Geographical Journal* 177, no. 3 (2011): 238–50.

Gregory, Derek. “Lines of Descent.” In *From Above: War, Violence and Verticality*, edited by Peter Adey, Mark Whitehead, and Alison Williams, 41–70. Oxford: Oxford University Press, 2013.

Gregory, Derek. “The Territory of the Screen.” *Mediatropes* 6, no. 2 (2016): 126–47.

Gros, Frédéric. *States of Violence: An Essay on the End of War*. Chicago: University of Chicago Press, 2010.

Hague Centre for Strategic Studies. *Artificial Intelligence and the Future of Defense*. 2017. https://hcss.nl/report/artificial-intelligence-and-future-defense.

Hall, Alexandra., and Jonathan Mendel. “Threatprints, Threads and Triggers: Imaginaries of Risk in the ‘War on Terror.’” *Journal of Cultural Economy* 5, no. 1 (2012): 9–27.

Hayles, Katherine. *How We Became Posthuman*. Chicago: University of Chicago Press, 1999.

Heath-Kelly, Charlotte. “Algorithmic Autoimmunity in the NHS: Radicalisation and the Clinic.” *Security Dialogue* 48, no. 1 (2017): 29–45.

Jaffer, Jameel. *The Drone Memos*. New York: New Press, 2016.

Jarzombek, Mark. *Digital Stockholm Syndrome in the Post-Ontological Age*. Minneapolis: University of Minnesota Press, 2016.

Kaplan, Caren. “Precision Targets: GPS and the Militarization of Everyday Life.” *Canadian Journal*

of Communication 38, no. 3 (2013): 397–420.

Kindervarter, Katharine. "The Emergence of Lethal Surveillance." *Security Dialogue* 47, no. 3 (2016): 223–38.

Kitchin, Rob. "Big Data, New Epistemologies and Paradigm Shifts." *Big Data & Society* 1, no. 1 (2014): 1–12.

Levine, Yesha. *Surveillance Valley: The Secret Military History of the Internet*. London: Icon Books, 2019.

Lowe, James. "Intelligence in the Selection of Strategic Target Systems." lecture, Air War College, Maxwell Air Force Base, Alabama. (1946) Documents M-U 38043 L913i. Muir S. Fairchild Research Information Center, Air University.

Lyon, David. "Surveillance, Snowden, and Big Data: Capacities, Consequences, Critique." *Big Data & Society* 1, no. 2 (2014): 1–13.

McCoy, Alfred. "Imperial Illusions: Information Infrastructure and the Future of US Global Power." In *Endless Empire: Spain's Retreat, Europe's Eclipse, America's Decline*, edited by Alfred McCoy, Josep Fradera, and Stephen Jacobson, 360–86. Madison: University of Wisconsin Press, 2012.

McSorley, Kevin. "Predatory War, Drones and Torture: Remapping the Body in Pain." *Body and Society* 25, no. 3 (2019): 75–99.

Miller, Greg. "Plan for Hunting Terrorists' Signals US Intends to Keep Adding Names to Kill Lists." *Washington Post*, October 23, 2012.

Nalty, Bernard. *The War against Trucks: Aerial Interdiction in Southern Laos 1968–1972*. Washington, DC: US Air Force History and Museums Program, 2005.

Negarestani, Reza "The Militarization of Peace: Absence of Terror or Terror of Absence?" In *Collapse I*, edited by R. Mackay, 53–92. Oxford: Urbanomic, 2007.

Nordin, Astrid., and Dan Oberg. "Targeting the Ontology of War: From Clausewitz to Baudrillard." *Millennium* 43, no. 2 (2015): 392–41.

O'Mara, Margaret. *The Code: Silicon Valley and the Remaking of America*. London: Penguin, 2019.

Pasquinelli, Matteo. "Anomaly Detection: The Mathematization of the Abnormal in the Metadata Society." 2015. http://matteopasquinelli.com/anomaly-detection/.

Pasquinelli, Matteo. "Arcana Mathematica Imperii: The Evolution of Western Computational Norms." In *Former West: Art and the Contemporary after* 1989, edited by Maria Hlavajova and Simon Sheikh, 281–294. Cambridge, MA: MIT Press, 2017.

Potzsch, Holger. "Archives and Identity in the Context of Social Media and Algorithmic Analytics: Towards an Understanding of iArchive and Predictive Retention." *New Media & Society* 20, no. 9 (2018): 3304–22.

Queally, Jon. “NSA Global Spy Stations Revealed: ‘Sniff It All, Collect It All, Know It All, Process It All, Exploit It All.’” *Common Dreams*, March 7, 2015.

Rohde, David. “Digitizing the CIA: John Brennan’s Attempt to Lead America’s Spies into the Age of Cyberwar.” *Reuters*, November 2, 2016. https://www.reuters.com/investigates/special-report/usa-cia-brennan/.

Scarry, Elaine. *The Body in Pain: The Making and Unmaking of the World*. Oxford: Oxford University Press, 1985.

Shaw, Ian. *Predator Empire: Drone Warfare and Full Spectrum Dominance*. Minneapolis: University of Minnesota Press, 2016.

Shaw, Ian. “The Urbanization of Drone Warfare.” *Geographica Helvetica*, no. 71 (2016): 19–28.

Spivak, Gayatri. “Can the Subaltern Speak?” In *Marxism and the Interpretation of Culture*, edited by Cary Nelson and Lawrence Grossberg, 271–313. Champaign: University of Illinois Press, 1988.

United States Department of Defense. “Project Maven to Deploy Computer Algorithms to Wars.” 2017. https://www.defense.gov/News/Article/Article/1254719/project-maven-to-deploy-computer-algorithms-to-war-zone-by-years-end/.

United States Joint Inquiry. “Report of the Joint Inquiry into the Terrorist Attacks of September 11, 2001.” Washington, DC: House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence, 2003.

Voelz, Glenn. “The Individualization of American Warfare.” *Parameters* 45, no. 1 (2015): 99–111.

Weber, Jutta. “Keep Adding: On Kill Lists, Drone Warfare and the Politics of Databases.” *Environment and Planning D: Society and Space* 34, no. 1 (2016): 107–25.

Weinberger, Sharon. *The Imagineers of War: The Untold Story of Darpa, the Pentagon Agency That Changed the World*. New York: Alfred A Knopf, 2017.

Wilcox, Lauren. “Drone Warfare and the Making of Bodies out of Place.” *Critical Studies on Security* 3, no. 1 (2015): 127–31.

Zuboff, Shoshana. *The Age of Surveillance Capitalism*. London: Profile Books, 2019.