Article

The Pursuit of Full Spectrum Dominance: The Archives of the NSA

Johan Lau Munkholm

University of Copenhagen, Denmark
jomu@hum.ku.dk

Abstract

This article explores the archives of the National Security Agency (NSA) and the inherent logic vested in the agency's management of them. By drawing on Derrida's conception of the archive and the compulsion to administer and complete it, this article suggests that the data collection practices, as well as the rhetoric, of the NSA indicate a specific logic of gathering and organizing data that presents a fantasy of perfect surveillance and pre-emptive intervention that stretches into the future to cancel emergent threats. To contextualize an understanding of the archival practices of the NSA within a wider conquest for complete security and US hegemony, this article outlines the US Department of Defense's vision for *full spectrum dominance*, stressing that a show of force is exercised according to a logic of appropriate response that ranges from soft to hard power. As an organization that produces knowledge and risk factors based on data collection, the NSA is considered a central actor for understanding the US security regime's increasing propensity for data-based surveillance that is fundamentally structured around the data center: a specific kind of archive.

Introduction

On May 30, 2000, the US Department of Defense (DoD) released the document "Joint Vision 2020" in which it established guidelines for the continuing transformation of the US Armed Forces. The DoD envisioned this transformation to be completed by 2020, by which time the military would have to be fully capable of responding to a new environment of threats already in the process of unfolding. The document emphasizes the threat posed by asymmetric warfare adopted by military adversaries that exploit the weaknesses of a stronger foe while circumventing its strengths in an environment of operational uncertainty (Ryan 2014). Under the category of asymmetric warfare, future enemies are understood to be dynamic, unpredictable, and always looking for the next creative fix to pierce the defenses of the US military on foreign and domestic territory. In a sense, the DoD was already keenly aware of the risk of an attack like the one perpetrated on September 11 the following year. The threat of a potential terrorist attack was on the agenda before 2001 and so the attacks on the World Trade Center all but confirmed the necessity of ramping up efforts to deal with a flexible and unpredictable enemy: 9/11 escalated the need to address the future challenges presented in "Joint Vision 2020." For the DoD, the solution to the threat of asymmetric warfare lies in achieving *full spectrum dominance*, which is "the ability of United States forces, operating unilaterally or in combination with multinational and interagency partners, to defeat *any* adversary and control *any* situation across the full range of military operations" (US Department of Defense 2000: 6; italics added). A central condition for achieving full spectrum dominance is the competitive advantage gained by information superiority that allows the US military to act in due time. Although the "Joint Vision 2020" document is skeptical as to the prospect of "perfect information" (US Department of Defense 2000: 9), the possibility of predicting and pre-empting future occurrences has not yet been extinguished in the US intelligence industry. Instead, with the increasing technological sophistication of data collection, processing,

and interpretation, the capability to preempt future threats before they occur is seemingly within the scope of the US intelligence community.

This article is an exploration of a fantasy of prediction held within the US security apparatus that manifests itself in a belief in the ability of big data to procure military dominance on a scale that moves beyond the present and into the future. This fantasy is produced parallel to the DoD's key objective of full spectrum dominance. By considering the military regulation that occurs according to the logic of a spectrum for possible intervention, we are able to discern the contours of perpetual war and the embeddedness of soft and hard power emphasizing the immanence of surveillance techniques and extra-judicial violence. Achieving the overarching goal of full spectrum dominance rests on the ability to utilize data appropriately to gain "information superiority" (US Department of Defense 2000). At the forefront of producing information superiority is the National Security Agency (NSA), which is an exemplary employer of big data analytics used to strengthen the US security apparatus' ability to predict and intervene preemptively on threats not yet fully formed by connecting and examining the data patterns that enable appropriate situational awareness. Acquisition of the necessary data is enabled by an extensive "physical and logistical infrastructure" (Andrejevic and Gates 2014: 188) whose flows of data the NSA is attempting to capture and direct to its data centers to intensify the agency and its partners' powers to monitor and control future threats.

As such, the privileged site for gaining information superiority is the data center, which functions as a specific kind of archive. This archive's mode of operation will be explored on a theoretical and practical level to assess not only the abilities it potentially provides the US surveillance and military regime but also the compulsions and temporal fantasies that are inherently ingrained in the way that the NSA manages its archives. Archival theory, inspired by Jacques Derrida's seminal lecture *Archive Fever* (1995), will inform an approach to assessing the logic that shapes the compulsive quest of the NSA to collect, archive, and process vast quantities of data. The aim here is not to seamlessly apply Derrida's slippery concepts to the practices of the NSA, as this would imply a misunderstanding of the processual and unfinished nature of the notion of the archive. To directly superimpose Derrida's notion onto an actual place where collected items are stored, cataloged, and categorized would be problematic since Derrida's musings are not simply descriptions of the actual archive. Rather, they are meditations on the etymology of the word "archive" and its association with an unending and reciprocal process of forgetting and remembering in the structure of Freudian thought that is absorbed in the injunction and beginning of the law. The aim is, instead, to indicate that certain impulses regarding temporal and ontological construction repeat themselves and mutate in different logics of (state) dominance expressed in governmental organizing of time and the real through expressions of power.

First, to approach and apprehend the surveillance practices structured around the data archive and the further objectives of the NSA as an actor within the US security apparatus, it is necessary to conceptually unfold full spectrum dominance as logic of global governance. Full spectrum dominance is pursued to sustain an arduous quest for US hegemony, to secure the continuous profitability of the global markets whose efficiency is based on the safety of multinational corporations to conduct business unhindered by unstable conditions (Murakami Wood 2017: 366), and to open new markets for neoliberalist enterprise (Harvey 2005: 6). First, I unfold full spectrum dominance to present the overriding logic of military dominance that the NSA operates within. Second, I offer an analysis of the NSA's logic of operation and military assistance, for which Derrida offers a conceptual vantage point for comprehending the collection practices of the NSA. This will require an exposition of Derrida's (1995) lecture before we can return to the NSA's specific data operations.

Full Spectrum Dominance

According to the logic of full spectrum dominance, the application of security measures ebbs and flows. Governmental regulation is practiced discreetly to avoid manifest repressions through force, but violent intervention is always a possibility. Security regulation takes place on a flexible continuum that can be scrutinized to assess a variety of strategies and techniques of power utilized on a quest for dominance. The

ideal capability gained by full spectrum dominance is to respond to *any* situation or adversary, which emphasizes the contingent environmental conditions of its domain of intervention and the global extent of its potential reach. Full spectrum dominance is thus in a permanent state of potential expansion, as it is a force continuously capable of responding to a global and ubiquitous environment of threats.

To unfold its potential to respond to any situation and adversary, full spectrum dominance can be conceptualized as a scale that designates an appropriate response to a possible threat at a given time that ranges from *soft* to *hard* force. As Brian Massumi (2015: 69) writes, soft force, or power, can be understood as the way “you act militarily in waiting, when you are not tangibly acting.” Soft force pertains to information superiority that defines “the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary’s ability to do the same” (US Department of Defense 2000: 8). Soft power is a ceaseless inscription on the conditions in which frictional warfare could emerge. In the military sphere, examples of soft power are surveillance techniques and info wars (Massumi 2015: 225) as well as more unobtrusive measures, summed up as “the ability to obtain preferred outcomes through attraction” by shaping preferences and desires of a foreign population through “public diplomacy, media campaigns, development aid and disaster relief” (Nye 2009: 160–162). By designating soft power as an expectant position awaiting frictional action, a spectrum ranging from soft to hard power is necessarily a continuum where an exercise of soft force perpetually contains a potential intensification: “war is no longer punctual, like a battle. It’s on a low boil all the time” (Massumi 2015: 69). By thinking of full spectrum dominance as an objective that integrates divergent interventionist practices, a certain relativity is emphasized: a relativity between governmentality, that is, between the anonymous and discreet governing of populations through micropolitics or environmental regulation in the so-called civil sphere (Foucault 2008) and the proactive and violent force expressed by the military sphere of exceptional sovereign power. In full spectrum dominance, logically, these two spheres are not binary; rather, they are subjected to different regimes of response within the same logic of power. Here, soft force “immaterializes violence” (Massumi 2015: 82). In the face of indiscriminate threat, “[the] overall environment of life now appears as a complex, systemic threat environment, composed of subsystems that are not only complex in their own right but are completely interconnected” (Massumi 2015: 29).

From this perspective, military regulation is always in action on a low intensity (Hippler 2017: 369), and, in a borderless war, regulation is enacted on a global level. When any dimension of global space is a target for asserting full spectrum dominance, national borders lose their sovereign prerogative as checks for hegemonic exertions of power. This does not mean that national borders have become obsolete, far from it, merely that territorial sovereignty is contingent and is readily undermined if a state is deemed to pursue weapons of mass destruction or aid and harbor terrorists (Elden 2009: 163). In the global order, the validity of borders is relative to the specific nation claiming sovereignty and its power to do so; if someone, or something, is deemed threatening to hegemonic interest, borders, and the rights they procure to citizens, borders lose authority and the sovereignty of state territory is undermined (Douglas 2009: 40).¹ Inside the national territory itself, border practices are likewise being established, creating zones with varying degrees of surveillance and policing (Graham 2010). We are perpetually in a state of war because, from a certain paranoid perspective of governance, threats are everywhere. This is a fundamental premise of the war on terror. Donald Rumsfeld (2002) all but confirms this reality: “First, wars in the twenty-first century will increasingly require all elements of national power: economic, diplomatic, financial, law enforcement, intelligence, and both overt and covert military operations. Clausewitz said, ‘War is the continuation of politics by other means.’ In this century, more of those means may not be military.” Here, Rumsfeld underlines the fact that clandestine responses to the ubiquitous nature of threats always have the potential

¹ The two-dimensionality of a flat and looped national territory cartographically drawn is, for instance, undermined by the volumetric and three-dimensional dominance perpetrated by the advent of unmanned aerial vehicles (UAVs) like the predator drone, which is simultaneously capable of ubiquitous aerial surveillance and violent intervention (Chamayou 2015a: 54). The drone is an ideal integration of both soft and hard force capabilities.

to become a spectacular show of force in the name of war: soft power can always intensify and cross over into hard power.

Hard Power

Hard power is when the low boil becomes a sputter. It is characterized by force-against-force, a spectacle of violence, or a strategic use of “shock and awe” (Ullman and Wade 1996), which changes the field of emergence by “addressing potential action” (Massumi 2015: 77). This means that a form of negotiation with combatant perception is still taking place at the hard end of the spectrum of force. Hard force reaches its *limit case* on the spectrum when annihilation takes precedence over perception-attack. As Eyal Weizman (2011: 200) explains: “However bad military attacks may appear to be, they could always get worse. When this gap between the possible and the actual application of forces closes, war is no longer a language, and violence is stripped of semiotics and simply aims to make the enemy disappear as a subject.” The limit case of the force spectrum is thus total annihilation, typically identified as all-out nuclear war, which, as Derrida (1984) reminds us, is a non-event without a referent outside itself since it has never actually taken place in history and, if it does, no one will be alive to redistribute the experience in writing. Given the abyss-like quality of the limit case, full spectrum dominance is immanently an exercise of force that works within certain limits of response to a given, or possible, threat on a variety of fronts through a series of techniques. Central to the justification for expanding the reach of the national security apparatus is the notion that we have entered an age of uncertainty. But, as Louise Amoore (2013: 7) writes, “What matters is not so much a question of whether or how the world is more dangerous, more uncertain, or less safe but how specific representations of risk, uncertainty, danger, and security are distinctively writing the contours of that world.” The increasingly sophisticated technologies for representing risk and uncertainty produce, in effect, reality as an aleatory environment of risk (Amoore and de Goede 2005: 168). This indicates the importance of the data archive to coordinate the representation of risk leading to an intervention. The refined technologies for establishing risk are part and parcel to justifying and expanding the security and surveillance apparatus that can manage the heightened threat levels pre-emptively: the full spectrum of force must defend against “the unknown, the uncertain, the unseen, and the unexpected” (Rumsfeld 2002). Pre-emption is precipitated on subverting the unpredictable. As Mark B.N. Hansen (2015: 106) has observed, Rumsfeld’s invocation of radical uncertainty, best represented in Rumsfeld’s famous epistemological category *unknown unknowns*, does not exist: “There is no unknown unknown in material reality: the unknown unknown is an ideological mystification of a geopolitical phenomenon, terrorism, that gains whatever traction it has from its capacity to pose extreme difficulties for extant epistemologies.” Suggesting that the world is radically unpredictable validates the need for extending the range of the dominance of the US military.

Full spectrum dominance is a militarily embedded form of governance engaged with a distribution of appropriate responses to emerging and aleatory threats. In other words, full spectrum dominance is an economy of force that works on the conditions of continual variation. The correct calculation leads to an appropriate show of force: a proper utilization of resources. A destructive approach, ultimately exemplified by the limit case, is by no means the ideal. Rather, it is the point when the environment of emergent threats intensifies and potentially becomes impossible to regulate, passing into chaos. Cost accounting for exertions of dominance is essential. The ideal hegemonic rule implied by full spectrum dominance is the ability to control and respond to a global environment. It is, however, an ideal that seems increasingly unlikely to materialize. Numerous geopolitical conditions limit the realistic actualization of full spectrum dominance. For example, the continuous ascendancy of China on the geopolitical stage contests the idea of the unimpeded military dominance of a single actor. This reality is not lost on the DoD. In its National Defense Strategy of 2018, China is named the main competitor to US supremacy (US Department of Defense 2018), which is reiterated by the current US Secretary of Defense Mark T. Esper at a talk at Goldman Sachs (2019): “We identify them as our number one competitor; we are their adversary. So everything they are doing right now is aimed toward pushing us out of the region... I just think China’s heading in the wrong direction; and so what we’ve been saying is we need to—we need to compete with them, and we need to try and pull them back—back into the international world order.”

Doubtless, the international order Esper is referring to is the liberal one designed after the Second World War under the leadership of the US. As Chinese GDP dwarfs the US's and the Central Government of the People's Republic of China is investing heavily in sophisticated military technology and global infrastructure projects, under the Rust and Belt Initiative, to further secure its borders and extend the reach of Chinese influence and potential military intervention, there is no indication that the Chinese government would submit to a world order imposed by the US. As a consequence of the rise of China as an ambitious global power, the US military primacy in the Indo-Pacific region is deteriorating (Townshend, Thomas-Noone, and Steward 2019), which logically impedes the global supremacy and reach immanent in full spectrum dominance. As doubtful as it may be that the US military can achieve full spectrum dominance within the current geopolitical division of power, it remains an overriding logic that orders succeeding modes of military and surveillance practices within a general environment of supposed threats. For the purposes of managing emergent threats, such as terror attacks, big data technologies have bolstered the fantasies of measured risk management, prediction, and temporal control (Amoore and de Goede 2005; Aradau and Blanke 2017), founding a fundamental attention to the global flow of data.

Bumblehive

In 2014, the US government completed the Utah Data Center, code-named “Bumblehive,” that serves as a data storage facility for the US Intelligence Community led by the NSA. The structure takes up 1–1.5 million square feet (90,000–140,000 m²); costs \$1.5 billion plus another estimated \$2 billion for hardware, software, and maintenance; and requires sixty-five megawatts of electricity and uses 1.7 million gallons of water daily for its chiller plant (Miller 2013). The Utah Data Center is an immense physical structure that draws on finite natural resources to work efficiently, particularly water.² The imposing material existence of the data center is a prerequisite for the omnipresent extent of its network. The pervasive surveillant assemblage is dependent on digitalized networks that render information readable and interactive as well as an intensification of computational efficiency in storing capabilities and processing power. The inconspicuous delivery-infrastructure that feeds the expanding collections of data is cloud computing, which traffics centripetal data circuits through bifurcated fiberoptic networks towards the centralized data storing facilities of corporate cloud service providers (Hu 2015: 7). The ubiquity of cloud computing, transmitted through a global network of interfaces, accentuates the reality of the control societies in which disciplinary environments of enclosure (Foucault 1995) open into a smooth and limitless milieu of biopolitical pervasive regulation of individual behavior through computational communication, tracking, and checkpoint technology (Haggerty and Ericson 2000). The subsistence of the control society is, however, mediated by identifiable and energy-hungry data archives: the modulatory power of the “corporation” in societies of control, announced by Gilles Deleuze (1992), is *presupposed* by the data factory. The apparent decentralization of power into digital networks is coordinated by the centralizing force of the cloud. As Tung-Hui Hu (2015: 79) states: “for the cloud to appear decentralized, its data must first be centralized.” It is the data archive that renders visible the deconstruction of the real and the mediated network occurring in societies of control that enables “dataveillance: a form of continuous surveillance through the use of (meta)data” (van Dijck 2014: 198). The power to monitor, track, and regulate emanates from these centralizing archives that house endless rows of servers collecting private and public information in concurrence with NSA's *raison d'être*: “collect it all” (Chamayou 2015b; van der Velden 2015). In a swarm of collected data, data mining becomes a significant tool in coordinating appropriate interventions in pursuit of full spectrum dominance. In other words, the eventual material expressions of hard power, for instance manifested in a drone strike, are increasingly guided by information gathered and derived through discreet digital networks. The suspension of the law inherent to the exceptional decision expressed in hard power is therefore integrated into the algorithmic calculations in the data center to assert exceptional dominance if deemed necessary (Agamben 2005: 84). Infusing the data archive with this toponomological principle

² The Utah Data Center is the NSA's central and biggest data center. It is not, however, the NSA's only center for storing and processing data. The NSA has data centers in Georgia, Texas, Colorado, and Hawaii as well as at its headquarters in Fort Meade, Maryland. In combination, these data centers serve as a “colossal network of backup hard drives ensuring that failure at one facility is easily recovered from another” (Hogan 2015: 3).

prompts a Derrida-inspired “archivological” investigation of the state-founded archive that propagates new governmental perceptive abilities and temporal regulation inconceivable without the machine vision of computation. Fantasies of temporal dominance are thus structured by the archival capabilities of the data center, which warrants a consideration of governmental surveillance potentiated by technological data capture that starts with the archive.

The Archive

The significance of the polysemantic word *archive* resonates with our present understanding of the data center. “Archive” is derived from the Greek *arkhé*, which concurrently denotes the *commencement* from which “physical, historical, or ontological principles” begin “according to nature or history” and the principle of the *commandment*, designating the archive as the authoritative site of the force of law that commands and structures the social order at the behest of the ruler (Derrida 1995: 9). By merging these two principles together, the name “archive” imbues the archival site with a toponomological principle from which the law begins *and* commands in a sequential series of ordering principles that structure reality and history. Because the archive is continuously being archived, there is no single principle of original commencement nor a potentially final expression of commandment in the archive. In addition, “archive” receives its meaning from the Greek *arkheion*: “initially a house, a domicile, an address, the residence of the superior magistrates, the *archons*, those who commanded” (Derrida 1995: 9). In the domicile of the *archons*, who hold the hermeneutic and political power to interpret, represent, and protect the law, the archive “takes place” (Derrida 1995: 10). From the domicile of the ruler, the power of the law emanates and the structure of history is endlessly organized. The archive resides in the home of the ruler in a state of restlessness, brought on by the *archontic* desire for *consignation* that “aims to coordinate a single corpus, in a system of synchrony in which all the elements articulate the unity of an ideal configuration” (Derrida 1995: 10). The principle of consignation describes the aim of establishing a cohesive institutional archive void of heterogeneity threatening the non-ambiguity of the archive. The archontic desire for ideal consignation is a desire to produce *one* archive that *speaks* in all objectivity, with one present “voice” presenting its content in a singular cohesion that allows for a conclusive interpretation of the historical archive and precludes potential innovations vested in its re-interpretation: a complete archive (Andrejevic and Gates 2014: 187). Making the archive total is the condition for acquiring absolute knowledge. It indicates that the NSA has been and is engaged in a relatively clandestine continuation of the not-so subtlety named Total Information Awareness program of Admiral Poindexter, initiated, and subsequently discontinued after public criticism, in 2003 (Bauman et al. 2014). Total awareness is a condition for the ability to predict future occurrences and achieving full spectrum dominance.

“Archive” does not merely designate a place but a structuring logic. The ideal consignation does not just encompass archival history. Rather, “the technical structure of the *archiving* archive also determines the structure of the *archivable* content even in its very coming into existence and in its relationship to the future. The archivization produces as much as it records the event” (Derrida 1995: 17). The process of archivization has as much to do with the future as the past, since the specific mode of nomological and topological assignment in a present moment determines the guiding relation between past and future. In this sense, the future is determined by the technical organization and quality of the archive, which coincidentally means that we cannot know what the archive is before it shows its meaning in the future. This is important, as it highlights the productivity of the archive. The archive is an active institution in forming the relation between present and future: what it is possible to know about the future based on an ongoing interplay between archive and the “outside” of the archive. The archive transforms its content according to a structuring logic and is, in turn, transformed by that very content; the archive does not unilaterally condition the quality of the archivable representations of phenomena (“the outside” of the archive)—the inside and outside reciprocally condition an ongoing exchange between archive and external phenomena without ever converging in ideal consignation. The ongoing exchange marks a technique of repetition that leaves an *impression* in the archive in which a loss in the inscriptive transfer is inevitable: a disjuncting gap opens between the original and its representation whose inexplicability drives a passionate search for the original

presenting itself completely. This drive forces a feverish return “to the most archaic place of absolute commencement” (Derrida 1995: 57).³ The search for the original, imposed by the refusal of loss, repeats the need for the archive that conditions forgetting; the compulsion that drives the search is what Derrida calls “archive fever,” which is an intangible and destructive force. Archive fever is an ailment, or a passion, inherent to the disjointing forces of archivization that continuously both destructs and archives the archive. For Derrida, the archiviolithic force “incites forgetfulness, amnesia, the annihilation of memory” and erodes anamnesis: spontaneous and lived memories of experience (Derrida 1995: 14). The archiviolithic force presupposes and amplifies the desire to archive and to remember in the future by means of supplemental or mnemotechnical methods for memorizing. The drive to repetitively archive is compelled by an unnameable and aggressive drive of forgetting; archive fever is a destructive drive that avoids extinction because it is repeated forward in every loss inherent to the archival translation from anamnesis to hypomnesia. Archive fever designates the reciprocally dependent forces of anamnestic loss and archiving. As such, the archive implies an indefinite process of archivization that refuses a finite concept ascribed to it. Instead, the archive changes with external substrates. In short, archiving can never be totally completed but must be endlessly repeated: more data are always necessary.

When computational information becomes the substrate of the archive, the notion of the archive occurs around the data center. The data center is restructuring our “inherited concept of the archive,” which is less like a concept and more like a “notion” or an “impression” awaiting development in the future (Derrida 1995: 24). The data center reciprocally transforms the archivable information into a new perceptive condition—as Derrida (1995: 18) notes, “what is no longer archived in the same way is no longer lived in the same way.” The data center changes reality and conceptions of time according to its mode of archiving. The critical change is not so much dependent on the ambition of total knowledge through consignment that gives an unmediated and comprehensive depiction of the real. This motivation is far from new, illustrated by ambitious projects of information collection and classification embodied in the Alexandrian Library, the encyclopedic projects of the Enlightenment, and Paul Otlet and Henri La Fontaine’s Mundaneum, not to mention various attempts at all-encompassing spying on potential dissidents by intelligence agencies like the Stasi police in the former DDR whose combined archived files extend over 111 kilometers. What is new is the archival technology and the ability to process the substrate, namely digital data, *allegedly* independently of any human system of classification or cataloguing, thereby overcoming the biases and limitations of human interpretation and revitalizing the fantasy of total knowledge. The NSA’s database functions like an archive insofar as it is a space for storing, categorizing, and tagging information, but it processes content unlike any other archive before it. As such, it changes ontological assumptions about reality and temporality accordingly. As Benjamin Bratton (2015: 353) remarks, “a database is just a particularly active kind of archive, one for which information that is drawn from the world more easily becomes an instrument for working reflexively back on it.” For the US military, the information drawn from the world is archivally organized to give the kind of situational and temporal awareness that facilitates full spectrum dominance. In other words, it is the new technological capabilities of the archive that afford the quest for full spectrum dominance. The data archive organizes a vision of the future by structuring the past and present in novel and unpredictable patterns. How does this work?

Archival Tools

Edward Snowden’s comprehensive leak from 2013 confronted the public with NSA-surveillance programs such as BLARNEY, FAIRVIEW, OAKSTAR, STORMBREW, PRISM, and XKEYSCORE (XKS).⁴ These

³ In Freudian psychoanalysis, a theory of the (psychic) archive, the destructive character of the transfer from the outside to the inside of the psyche relates to the problem of repression inherent to the forgetting of the entirety of the injunctive or traumatic impression of the past. Psychoanalysis is a continuous, yet futile, attempt at illuminating the character of this original impression to exorcise its repetitive influence. For Derrida (1995: 25), this is the lasting mark Freud has impressed upon historiography, which repeats the dream of reviving what is lost in the archive and thereby confirms the archive’s force mobilized by forgetting. See Steedman (1998).

⁴ For a more comprehensive list of programs, see van der Velden (2015).

programs comprise some of the operative software tools that the NSA uses to gather and store copious amounts of data. They are, in effect, archive management tools. In NSA parlance, BLARNEY, FAIRVIEW, OAKSTAR, and STORMBREW are tools for “upstream” collection that intercept web and telephone traffic from the principal routes between major and globally interconnected computer networks and core routers on the Internet—i.e., tools that tap into the fiberoptic lines that compose the backbone of the Internet. Upstream collection is conducted in collaboration with a variety of telecommunications and network service providers like Verizon, AT&T, and Cisco that are ordered by the US Foreign Intelligence Surveillance Court (FISA) to facilitate the NSA and its subcontractors in collecting raw communication data in bulk from their networks. As reported by *The Intercept*, the NSA’s infrastructure for data capture is intimately integrated with AT&T’s through eight AT&T data centers located in major cities across the US that give the NSA direct access to AT&T’s networks that are frequently used by telecommunication operators who “peer” with the service provider to route data efficiently (Gallagher and Moltke 2018). The integration of further network nodes into its assemblage for data capture intensifies the efficiency with which the NSA appropriates data.

Authorized by the FISA court, PRISM is utilized to do front-door collection of data directly from the servers of major Internet companies like Facebook, Apple, Google, and Microsoft, whose cloud platforms are unremittingly fed user-generated data then made available to the NSA through PRISM. XKS is another powerful collecting tool that processes phone numbers, email addresses, log-ins, and other online user activity from online sessions and transfers it to a database that can be accessed by NSA employees through an XKS search-engine for monitoring traffic on different cloud-based social media networks. XKS effectively offers an archive interface that assists users of the NSA’s proprietary cloud platform to access queried data. The NSA’s ongoing preoccupation with data is reflected in the agency’s 2014 publication of *The Next Wave*, a public NSA-journal dedicated to emerging technologies that focuses specifically on big data. For Mark E. Segal (2014: 2), chief of the Computer and Information Sciences Research Group at the NSA, “Big Data offers the promise of being able to detect trends in large data sets in ways that were not possible with older technologies.” Specifically, he says, “Big Data capabilities can enhance national security by allowing our military to gain better situational awareness before and during battle. Big Data capabilities may also be used to analyze potential actions by a country or terrorist organization hostile to the United States and prevent those actions from taking place” (Segal 2014: 2). Segal confirms that the promising aspect of big data is that it offers augmented pre-emptive capabilities and situational military awareness by enhancing perceptive abilities through computation and producing patterns of future emergences in the present.

The limited selection of NSA programs presented here are archival tools for collecting data and creating aggregated data sets large enough for big data analytics. This situates the NSA as a regime of capture that re-directs, duplicates, and repurposes data from other cloud archives in the service of an underlying logic: to collect it all, which reflects an archiviolithic drive. The NSA is a parasitic organization feeding on data that it seeks to convert to greater surveillance capabilities affording full spectrum awareness and dominance. The aim of collecting everything spurs the agency on as new threats keep appearing. A recent invocation of the rising threat of “cyberconflict” by Glenn R. Gerstell (2019), writing on behalf of the NSA, warrants the need for better technologies and systems to “capture, store and analyze” copious volumes of data that the NSA inevitably will collect. With an organization as hermetic as the NSA, it is hard to know exactly what technologies they possess. However, the need for more data and capital is constant. Now, it is important to stress that the fantasies of indiscriminate knowledge and objective awareness necessary for staying alert to any threat are born out of a shift in epistemology driven by big data. According to this epistemological shift, knowledge can be produced from correlative analytics of raw data alone, independently of any theoretical framework or selective decision-making: unmediated knowledge. The revolutionary promises of this supposed epistemological paradigm shift has been pointed out by Lisa Gitelman and Virginia Jackson (2013: 1), among many others, who quote Geoffrey Bowker (2005: 184) when stating that “raw data is an oxymoron.” This means that data are never self-evident or transparent before the fact. To suggest that conclusions can be deduced from data based on defined and trained algorithms or data sampling without any theoretical framework is unfounded (boyd and Crawford 2012; Kitchin 2014). Yet, it may work to hide

a discriminatory bias that can be lethal in the case of security systems veiled behind the glimmer of alleged objectivity. Even if the NSA are less than successful in actually thwarting terror attacks by consulting big data (McLaughlin 2015), errors and false positives produced by biased systems still have real outcomes, whether these are effectuated in terms of soft or hard power (O’Neil 2016). Nonetheless, the NSA collects lots of data.

Collect It All

At a presentation at the annual Five Eyes Conference in 2010, the “collect it all” mantra, a condensed objective stance purportedly formulated by ex-director of the NSA Keith Alexander, was presented within a looped “collection posture,” highlighting an endless routine of intelligence gathering coordinated and managed with archival technologies: “Collect it all – Process it all – Exploit it all – Partner it all – Sniff it all – Know it all” (Greenwald 2014: 97). This loop denotes a program devoted to full spectrum dominance through consignment. It indicates a constantly deferred programmatic desire to capture a continuous stream of user-data and metadata in order to constantly re-complete the archive. Consigning the NSA archive does not involve gathering data to configure the past. Rather, the NSA’s archival tools collect emergent data and store them for further analysis relevant to the future of emerging threats—the NSA’s archival practice assumes a pre-emptive posture. Data moving from *emergent* to *stored* (an impossible difference to unequivocally maintain) may congregate in patterns with emergent data in the future.

As implied by the looped collection stance, the NSA’s archival project is primed by a ceaseless aim for the exhaustive absorption of emergent data. The ambitiousness of this undertaking resembles the zeal vested in the principle of consignment: a technique of repetition that assures memorization in the future. This, in a sense, ties the NSA’s project to a certain case of archive fever that, rather than driving a search for an original inscription, instigates a vigorous search for existing traces. Thus it works to illuminate the future before it arrives, emboldened by powerful mnemotechnical tools for memorization. This drive can be described as *collection fever*, which impels the NSA to collect excessively: “As of mid-2012, the agency was processing more than twenty billion communications events (both Internet and telephone) from around the world *each day*” (Greenwald 2014: 98; emphasis in the original). For the NSA, collection fever ties to a rationale of full spectrum awareness and forensic disclosure made possible by ideal consignment—if something is missed, if proper adjudication for the traumatic and destabilizing event is not reached, then it must, as Bratton puts it in the documentary *The Sprawl (Propaganda About Propaganda)* (Metahaven 2016), “have been a function of insufficient resolution and granularity in the capture or in the disclosure itself and so the solution to this is to expand the resolution of that possibility.” If the archive does not efficiently ensure complete awareness of emerging threats, then the archival consignment requires more data—as an elated Chris Anderson (2008) once stated: “With enough data, the numbers speak for themselves.”

In a congressional hearing before the House Intelligence Committee in 2013 about the Snowden disclosures, then-director of the NSA General Keith B. Alexander repeatedly referenced the 9/11 terrorist attacks as a specter that potentially could have been exorcised if the NSA had had the surveillance-capabilities awarded to the agency post-9/11—the same tools it was now being scrutinized for utilizing excessively. In his opening statement to the committee, Alexander simultaneously evokes the specter of 9/11 and admonishes its potential reappearance, which the NSA is working to deny: “Let me start by saying that I would much rather be here today debating this point than trying to explain how we failed to prevent another 9/11. It is a testament to the ongoing team work of the Central Intelligence Agency, the Federal Bureau of Investigation, and the National Security Agency, working with our allies and industry partners, that we have been able to connect the dots and prevent more terrorist attacks” (qtd. in US House Select Intelligence Committee 2013).

The stubborn reminder of 9/11 indicates an obsession with lingering specters that, according to Derrida (1994: 45), has “a dominant influence on discourse today.” As Derrida (1994: 46) writes, “Haunting belongs to the structure of every hegemony.” Aspiring hegemonic regimes’ obsessions with reappearing specters prompts governmental work to settle the future’s refractory opening through which contingent appearances

inevitably arrive. The structure of haunting and the reappearance of the traumatizing ghost from the future justifies the NSA's drive to consign the archive in an attempt to structure temporality in accordance with a logic of full spectrum dominance that stitches the present and future together. The unpredictably new is a threatening promise but one that can be put to political use. Alexander continues his testimony:

The events of September 11, 2001 occurred, in part, because of a failure on the part of our government to connect those dots. Some of those dots were in the United States. The intelligence community was not able to connect those domestic dots, phone calls between operatives and the US and Al Qaida terrorist overseas. Following the 9/11 commission, which investigated the intelligence community's failure to detect 9/11, Congress passed the PATRIOT Act. Section 215 of that act, as it has been interpreted and implied, helps the government close that gap by enabling the detection of telephone contact between terrorists overseas and operatives within the United States. As Director Mueller emphasized last week during his testimony to the – to the Judiciary Committee, if we had had Section 215 in place prior to 9/11, we may have known that the 9/11 hijacker Mihdhar was located in San Diego and communicating with a known Al Qaida safe house in Yemen. (qtd. in US House Select Intelligence Committee 2013)

The NSA's ability to "connect the dots" is, for Alexander, integral to preventing the return of the specter of 9/11 in the future. In Alexander's testimony, he describes a scenario in the conditional perfect tense where this specter would not exist. The scenario fuels his repeated reminder to the committee that, for the NSA to "connect the dots" and clearly perceive and prevent terror attacks in advance, the agency must be in possession of the dots. This echoes another one of Alexander's aphorisms: "You need the haystack to find the needle" (qtd. in Aradau and Blanke 2017). Alexander references section 215 of the Patriot Act as the governmental authority enabling the potential ideal configuration of the archive by closing "the gap" and allowing the NSA to create a pattern of dots that indicates future trajectories of possible threatening emergences and achieving full spectrum awareness.⁵ In the constitution of an informative network of threats, any overlooked node might spell catastrophe. Consequently, the NSA's collection fever can be understood in connection to Hu's (2015: 11; italics in the original) concept *network fever*: "Network fever is the desire to connect *all* networks, indeed, the desire to connect every piece of information to another piece. And to construct a system of knowledge where everything is connected is, as psychoanalysis tells us, the sign of paranoia." The NSA's distinct case of collection fever enforces network fever (and vice versa), which is an investment in the perfect network "where everything is connected and the network is omnipresent" (Hu 2015: 18). Network fever denotes a need to connect every dot in the network, which, in turn, presupposes a fever of endless gathering of dots and nodes in a paranoid attempt to elucidate an omnipresent network of threats. As Mark Andrejevic and Kelly Gates (2014: 186) write, the attempt at representing the complete network of dots expresses the "hope of putting to use the world redoubled in digital form," creating an archive of the real that conditions the degree of efficiency of dataveillance and the ability to infer from data patterns what will happen in the future. The effort to represent the entire network is plainly expressed in the NSA's plan to map the entire internet: "TREASUREMAP."

Treasuremap

In 2014, *Der Spiegel* published NSA/Central Security Service slides that presented the TREASUREMAP initiative. TREASUREMAP is programmed to "map the entire Internet—Any device, anywhere, all the

⁵ For more on Section 215 of Title II of the Patriot Act, see Greenwald (2014). In 2015, the US Congress passed the so-called Freedom Act US, which, in effect, prolonged the Patriot Act while slightly curbing the NSA's use of Section 215 (Lyon 2015: 139). The Freedom Act was renewed on March 11, 2020 under the USA FREEDOM Reauthorization Act of 2020. Section 215, however, expired on March 15, 2020 but could very well still be renewed. It has been extended in the US Senate but re-authorization needs to be passed in the House of Representatives before the bill can be renewed. As of this writing, this has yet to happen, as the House of Representatives left Washington before it could vote on an extension.

time” according to the directorial rationale (Grothoff et al. 2014). This might be a fittingly paranoid slogan for the NSA and an epistemic condition guiding full spectrum dominance: “Bad guys are everywhere, good guys are somewhere!” (Grothoff et al. 2014). TREASUREMAP is a continuously generated “global Internet map” enabling “Cyber Situational Awareness” by mapping the “Geographical Layer,” “Physical Network Layer,” and, particularly, the “Logical Network Layer” (in the Open Systems Connection (OSI), the network layer provides an address system for routing packages from one node in the network to another) of a stacked model, enabling attentiveness to the overlying layers: the “Cyber Persona Layer” and “Persona Layer” (Bratton 2015: 441n8; Grothoff et al. 2014). Generating awareness of the entire global map via this US federal stack program is reliant on feeding the machine: the data center (Bratton 2015: 441n8). Full spectrum awareness of a vast and constantly constructed stack, mapping both benign and potentially malignant movements and deviations inferred from patterns of data, cannot be perceived or deciphered by human cognition due to an overabundance of information that constantly grows. The NSA’s captured data are centripetally and inevitably moving towards the data center where the dots are connected in complicated patterns by computational tools. To do so, consigning the archive is key. The interpretive force of the archive is privileged to algorithmic calculation capable of processing large volumes of data and tools for recognizing and visualizing data patterns, which means that the ruling privileges of the *archons* are bestowed upon a technological vision that sees correlative connections between the present and future that human perception cannot. According to Antoinette Rouvroy (2009: 8), this implies a rise in autonomic computing capable of “detection, classification and forward-looking evaluation that would gradually assist or even replace human observation,” producing new governmental rationality according to the epistemological shift towards radical uncertainty that it seeks to manage. Decisional power is increasingly vested in the operational capabilities of software emphasized by the NSA’s rationale of collecting, mapping, and knowing *everything*, which indicates a certain belief in the eventual technological ability to overcome the unpredictability of the future. The NSA’s ardor for collecting data signals an ongoing investigation into the possibilities of automation and machine learning, which will only enhance the power of software to make sovereign decisions based on data correlations, imperceptible to humans, to pre-empt undesirable future events. As Rouvroy (2009: 14) writes, “The ubiquitous threat of virtual danger acts as a powerful incentive to eradicate pre-emptively whatever, in the human being, remains uncertain, virtual, potential.” The virtual dimension of being, the unpredictable process of becoming beyond actual being, is potentially threatening, as it implies an opening for any being to appear in the future, which is a simultaneous reappearance of the traumatic unknown that repeats itself (Rouvroy 2009: 23). For Derrida (1994: 63), the spectral and traumatic reappearance of a future event cannot be exorcised, only negotiated with: the “hauntological” invocation from the past and future is perennial. Nonetheless, the genesis of totalitarianism is founded in a persistent and persevering conjuration of ghosts signaling that the haunting effects of an unpredictable environment of threat cannot simply be accepted as a premise (Derrida 1994: 131). The NSA is invested in ending the emergence of threats that come from the unknown future—whether these threats are actualizable or merely figments of autonomous data representation is of lesser importance. Rooted in an idea of tracking and mapping everything, of knowing and seeing everything through technological calculation and visualization, lies a fantasy of temporal dominance of the future—in other words: a fantasy of full spectrum awareness and dominance. In securitization, fantasies of a smooth ontology, void of specters, persevere beneath the chaos of contingent emergence, which rejects any sustained conditional notion of the unknown. The unknown, as a normalized temporal condition or an ontological premise that haunts present and future emergences, must not be accepted as the norm. Rather, the norm must be *changed* by pre-emptively intervening in the environment of emergence to control what comes next.

Conclusion

The declared aim of the US military to achieve full spectrum dominance is surely an ambitious undertaking that will likely never be accomplished. It stresses the need for a well-organized and vigilant surveillance system that directly translates observations of threatening behaviour to an appropriate and pre-emptive response that exorcises unwanted emergences. The efforts to achieve full spectrum dominance, which stretches its reach into the future, are to an increasing extent coordinated by the data archive that seeks to

capture and direct the entire flow of global data into the NSA's data centers to build a complete representation of the real. The NSA's surveillance program enlists the centripetal force of the archive in organizing a vast security apparatus, enhancing the governmental capabilities of perceptual awareness. From awareness to pre-emptive intervention, more power will be delegated to computational tools that process the library of the real to envision future threats and automatically mobilize lethal technological measures to pre-empt the specters of a contingent future. Here, it is the algorithm which deems certain patterns so deviant from a fluctuating norm that appropriate and potentially violent measures must be inserted whether soft or hard. The data archive and practices surrounding it conditions this venture into dataveillance that monitors personalized data representations for abnormal tendencies. The actual exercise of force will gradually be outsourced to progressively independent technical agents whose operations are based on an algorithmic logic creating legal aporias in terms of liability (Schuppli 2014). The indiscriminate collection practices reflected in the US federal archival project coordinated by the NSA thus enable algorithmic governance that bases decisions on the associative potential of the data double stored in proprietary data repositories—an archive inaccessible to public scrutiny. In stressing the importance of the fantasies that surround the archive, this article has indicated the inherent logic of governance working to manage any and all unpredictable emergences of the future. Attaining this capability may be a pipe dream based in a brash confidence in a new epistemological shift and big data. Nonetheless, the veneer of objectivity and technological efficiency may work to both undermine human supervision and amplify existing biases on account of imminent danger.

References

- Agamben, Giorgio. 2005. *State of Exception*. Chicago, IL: The University of Chicago Press.
- Amoore, Louise. 2013. *The Politics of Possibility: Risk and Security Beyond Probability*. Durham, NC: Duke University Press.
- Amoore, Louise, and Marieke de Goede. 2005. Governance, Risk and Dataveillance in the War on Terror. *Crime, Law & Social Change* 43: 149–173.
- Anderson, Chris. 2008. The End of Theory: The Data Deluge Makes the Scientific Method Obsolete. *The Wire*, July 23. <https://www.wired.com/2008/06/pb-theory/> [accessed September 13, 2019].
- Andrejevic, Mark, and Kelly Gates. 2014. Big Data Surveillance: Introduction. *Surveillance and Society* 12 (2): 185–196.
- Aradau, Claudia, and Tobias Blanke. 2017. Politics of Prediction: Security and the Time/Space of Governmentality in the Age of Big Data. *European Journal of Social Theory* 20 (3): 373–391.
- Bauman, Zygmunt, Didier Bigo, Paulo Esteves, Elspeth Guild, Vivienne Jabri, David Lyon, and R.B.J. Walker. 2014. After Snowden: Rethinking the Impact of Surveillance. *International Political Sociology* 8: 121–144.
- Bowker, Geoffrey C. 2005. *Memory Practices in the Sciences*. Cambridge, MA: The MIT Press.
- boyd, danah, and Kate Crawford. 2012. Critical Questions for Big Data. *Information, Communication and Society* 15 (5): 662–679.
- Bratton, Benjamin H. 2015. *The Stack: On Software and Sovereignty*. Cambridge, MA: The MIT Press.
- Chamayou, Grégoire. 2015a. *Drone Theory*. London, UK: Penguin Press.
- . 2015b. Oceanic Enemy: A Brief Philosophical History of the NSA. *Radical Philosophy* 191: 2–12.
- Deleuze, Gilles. 1992. Postscript on the Societies of Control. *October* 59: 3–7.
- Derrida, Jacques. 1984. No Apocalypse, Not Now (Full Speed Ahead, Seven Missiles, Seven Missives). *Diacritics* 14 (2): 20–31.
- . 1994. *Specters of Marx*. New York, NY: Routledge.
- . 1995. Archive Fever: A Freudian Impression. *Diacritics* 25 (2): 9–63.
- Douglas, Jeremy. 2009. Disappearing Citizenship: Surveillance and the State of Exception. *Surveillance & Society* 6 (1): 32–42.
- Elden, Stuart. 2009. *Terror and Territory: The Spatial Extent of Sovereignty*. Minneapolis, MN: The University of Minnesota Press.
- Esper, Mark T. 2019. Remarks by Secretary Esper at Goldman Sachs, New York City, New York. US Department of Defense, November 11. <https://www.defense.gov/Newsroom/Transcripts/Transcript/Article/2018541/remarks-by-secretary-esper-at-goldman-sachs-new-york-city-new-york/> [accessed November 27, 2019].
- Foucault, Michel. 1995. *Discipline and Punish: Birth of the Prison*. New York, NY: Vintage Books.
- Foucault, Michel. 2008. *The Birth of Biopolitics: Lectures at the Collège de France, 1978–1979*. Basingstoke, UK: Palgrave Macmillan.
- Gallagher, Ryan, and Henrik Moltke. 2018. The Wiretap Rooms: The NSA's Hidden Spy Hubs in Eight U.S. Cities. *The Intercept*, June 25. <https://theintercept.com/2018/06/25/att-internet-nsa-spy-hubs/> [accessed September 13, 2019].
- Gerstell, Glenn R. 2019. I Work for the N.S.A. We Cannot Afford to Lose the Digital Revolution. *The New York Times*, September 10. <https://www.nytimes.com/2019/09/10/opinion/nsa-privacy.html> [accessed September 13, 2019].
- Gitelman, Lisa, and Virginia Jackson. 2013. Introduction. In *“Raw Data” is an Oxymoron*, edited by Lisa Gitelman, 1–14. Cambridge, MA: The MIT Press.
- Graham, Stephen. 2010. *Cities Under Siege: The New Military Urbanism*. London, UK: Verso Books.
- Greenwald, Glenn. 2014. *No Place to Hide*. New York, NY: Metropolitan Books.
- Grothoff, Christian, Andy Müller-Maguhn, Laura Poitras, Marcel Rosenbach, Michael Sontheimer, and Christian Grothoff. 2014. Treasure Map: The NSA Breach of Telekom and Other German Firms. *Der Spiegel*, September 14.

- <http://www.spiegel.de/international/world/snowden-documents-indicate-nsa-has-breached-deutsche-telekom-a-991503.html> [accessed September 13, 2019].
- Haggerty, Kevin D., and Richard V. Ericson. 2000. The Surveillant Assemblage. *British Journal of Sociology* 51 (4): 605–622.
- Hansen, Mark B.N. 2015. Our Predictive Condition; or, Prediction in the Wild. In *The Nonhuman Turn*, edited by Richard Grusin, 101–139. Minneapolis, MN: University of Minnesota Press.
- Harvey, David. 2005. *A Brief History of Neoliberalism*. Oxford, UK: Oxford University Press.
- Hippler, Thomas. 2017. *Governing from the Skies: A Global History of Aerial Bombing*. London, UK: Verso Books.
- Hogan, Mel. 2015. Data Flows and Water Woes: The Utah Data Center. *Big Data and Society* 2 (2): 1–12.
- Hu, Tung-Hui. 2015. *A Prehistory of the Cloud*. Cambridge, MA: The MIT Press.
- Kitchin, Rob. 2014. Big Data, New Epistemologies and Paradigm Shifts. *Big Data and Society* 1 (1): 1–12.
- Lyon, David. 2015. The Snowden Stakes: Challenges for Understanding Surveillance Today. *Surveillance & Society* 13 (2): 139–152.
- Massumi, Brian. 2015. *Ontopower: War, Powers, and the State of Perception*. Durham, NC: Duke University Press.
- McLaughlin, Jenna. 2015. U.S. Mass Surveillance has no Record of Thwarting Large Terror Attacks, Regardless of Snowden Leaks. *The Intercept*, November 17. <https://theintercept.com/2015/11/17/u-s-mass-surveillance-has-no-record-of-thwarting-large-terror-attacks-regardless-of-snowden-leaks/> [accessed September 13, 2019].
- Metahaven, dir. 2016. *The Sprawl (Propaganda About Propaganda)*. Netherlands: Metahaven and Lighthouse and the Space. <http://sprawl.space/>.
- Miller, Rich. 2013. NSA Utah Data Center Facing Unexpected Energy Taxes. *Data Center Knowledge*, May 20. <http://www.datacenterknowledge.com/archives/2013/05/20/utah-legislators-hit-nsa-data-center-with-energy-tax/> [accessed September 13, 2019].
- Murakami Wood, David. 2017. Editorial: The Global Turn to Authoritarianism and After. *Surveillance & Society* 15 (3/4): 357–370.
- Nye, Joseph S., Jr. 2009. Get Smart: Combining Hard and Soft Power. *Foreign Affairs* 88 (4): 160–163.
- O’Neil, Cathy. 2016. *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*. New York, NY: Crown Publishing Group.
- Rouvroy, Anoinette. 2009. Governmentality in an Age of Autonomic Computing: Technology, Virtuality and Utopia. In *Law, Human Agency and Autonomic Computing*, edited by Mireille Hildebrandy and Antoinette Rouvroy, 135–156. Abingdon-on-Thames, UK: Routledge.
- Rumsfeld, Donald H. 2002. Transforming the Military. *Foreign Affairs*, May/June. <https://www.foreignaffairs.com/articles/2002-05-01/transforming-military> [accessed November 27, 2019].
- Ryan, Maria. 2014. ‘Full Spectrum Dominance’: Donald Rumsfeld, the Department of Defense, and US Irregular Warfare Strategy, 2001–2008. *Small Wars and Insurgencies* 25 (1): 41–68.
- Schuppli, Susan. 2014. Deadly Algorithms: Can Legal Codes Hold Software Accountable for Code that Kills? *Radical Philosophy* 187: 2–8.
- Segal, Mark E. 2014. Guest Editor’s Column. *The Next Wave: The National Security Agency Review of Emerging Technologies* 20 (4): 2–3.
- Steedman, Carolyn. 1998. The Space of Memory: In an Archive. *History of the Human Sciences* 11 (4): 65–83.
- Townshend, Ashley, Brendan Thomas-Noone, and Matilda Steward. 2019. Averting Crisis: American Strategy, Military Spending and Collective Defence in the Indo-Pacific. United States Studies Centre, August 19. <https://www.ussc.edu.au/analysis/averting-crisis-american-strategy-military-spending-and-collective-defence-in-the-indo-pacific> [accessed November 27, 2019].
- Ullman, Harlan K., and James P. Wade. 2004. *Shock & Awe*. London, UK: Pavilion Press.
- US Department of Defense. 2000. Joint Vision 2020. Washington, DC: US Government Printing Office.
- US Department of Defense. 2018. Summary of the National Defense Strategy of the United States: Sharpening the American Military’s Competitive Edge. Washington, DC: US Government Printing Office.
- US House Select Intelligence Committee. 2013. Hearing on Disclosure of National Security Agency Surveillance Programs, June 18. https://fas.org/irp/congress/2013_hr/disclosure.pdf [accessed September 13, 2019].
- van der Velden, Lonneke. 2015. Leaky Apps and Data Shots: Technologies of Leakage and Insertion in NSA-Surveillance. *Surveillance & Society* 13 (2): 182–196.
- van Dijck, José. 2014. Datafication, Dataism and Dataveillance: Big Data Between Scientific Paradigm and Ideology. *Surveillance & Society* 12 (2): 197–208.
- Weizman, Eyal. 2011. Thanato-tactics. In *Beyond Biopolitics: Essays of the Governance of Life*, edited by Patricia T. Clough and Craig Willse, 177–210. Durham, NC: Duke University Press.