Abstract  The War on Terror is an ambiguous term that has been used to circumvent the international laws of warfare. Instead of moving toward peace by way of limited warfare, and instead of preserving the independence of war and peace, War on Terror advances by masking itself in a fog of peace; it proliferates by overlapping the logic of “war-time” and “peace-time” operations. The fog of peace—as it shall herein be called—is a condition wherein the uncertainty qua “fog” of war, along with its militarized logic, overlaps with and eventually replaces civilian peace-time-and-spaces. The War on Terror is thus not a limiting of war by way of the conventional modern mechanisms of international law and diplomacy; it is a continuation of war by other means, including the use covert, often black-boxed methods of information-capture and surveillance. Globally, states are expanding the powers of intelligence organs and deploying covert mass surveillance programs in the name of counter-terrorism. In this manner, counter-terrorism policies become instruments enabling states to become predatory, especially in relation to civilians. Under the banner of fighting terrorism, peace-time has unwittingly become colonized by the logic of war.

Keywords: war on terror; fog of war; peace-time; war-time; surveillance state; data; terrorism

I. Introduction: Beyond War and Peace

Historically in world affairs, states of “war” and “peace” have been rigorously defined and are held to be mutually exclusive: “war” has been defined as a state of armed conflict against an enemy, and its absence is usually defined, in contrast, as “peace.” Technically, without an explicit declaration of war, nations are considered to be in peace-time states with one another. When considered according to these parameters, the War on Terror is not a war at all, although it makes ample use of the language and rhetoric of war. The War on Terror, in fact, obfuscates the strict legal delimitation between war-time and peace-time. For the modern Clausewitzian theory of war, it is necessary to reduce the uncertainties of war, or fog of war, by strictly delimiting military spaces and times from civilian spaces and times. By contrast, I argue that in the War on Terror, the normal and normative limits between war-time and
peace-time become conflated, allowing both to become entangled and to eventually overlap over time—a phenomenon that I will refer to as the fog of peace. The War on Terror, unlike the modern theory of war, amplifies the fog of peace, which expands the boundaries of warfare well beyond war-time. Under the guise of fighting the War on Terror, ever-more-sophisticated intelligent machines are being developed and adopted—not just weaponized drones for use in military operations, but also weapons of information surveillance, from biometric and geolocative technologies to consumer preference tracking technologies that extract and profit from civilian metadata. Nations, groups, individuals, and corporations are increasingly adopting threat-models and entrenching global counter-terrorism technologies that involve globally coordinated systems and processes for capturing, storing, and cross-referencing digital information of any and every sort. The War on Terror, by this argument, is not a “new kind of war” (as the George W. Bush administration claimed after 9/11). It is not a war at all—legally understood—but rather, an increasingly globalized, normalized, and emergent reality that is entirely dependent on the interpenetration of military and civilian spaces, as well as on the conflation of political and technological rationales. While it may have begun as the American government’s politico-military response to terrorism, the War on Terror has gone from being merely the particular military doctrine of the American state and its allies to becoming a hyper-mediatized and normatively opaque politics of ongoing militarization that mobilizes and exploits everyday civilian digital technologies, datalogical techniques, media networks, and virtual platforms. As the authors of the NATO StratCom report conclude: “the exploitation of the virtual space for warfare is taking place at unprecedented levels of sophistication. [. . .] Efforts to control the dissemination of terrorist propaganda or other malicious use of social media, either through technical or policy restrictions, are not an effective solution.” As warfare is waged, more and more, by way of non-military means, it is also becoming increasingly blackboxed and ethico-juridically nebulous, not to mention predatory.

Under the rubric of counter-terrorism, governments and their intelligence organs—in cooperation with information-technology corporations—are tracking user information from social media sites such as Facebook and Twitter in search of potential terrorists via patterns of so-called suspicious behavior. Risk-profiling techniques—technologies designed to classify populations according to their potential degrees of threat—are being deployed to conduct overt and covert surveillance of citizens and civilian spaces, capturing all sorts of data (personal and impersonal) and thereby violating longstanding civil and political rights. By extending the logic of warfare into peace-time indefinitely, the War on Terror has bypassed normal political processes that are meant to regulate warfare and protect citizens. The War on Terror, originally the U.S. government’s official military policy after 9/11 and now a catch-all term for global counter-terrorism, is, de facto, the indefinite militarization of peace-time. This militarization involves not only the enmeshing of governmental organizations, digital media and information-technology corporations, and the everyday lives of consumer citizens, but also increasingly non-state networks, non-military
targets, non-human actors, and technical weapons such as code, algorithms, data analytics, and malware.

In the following, I argue that The War on Terror is not a limiting of war by way of the conventional modern mechanisms of international law and diplomacy; it is a continuation of war by other means (especially non-military), including the use covert, often black-boxed methods of information-capture and surveillance. All over the world, governments are expanding the powers of intelligence organs and deploying mass surveillance programs; in so doing, counter-terrorism responses become unwitting instruments enabling states to become predatory in relation to civilians. In the name of fighting terrorism, peace has unwittingly become a tool for justifying mass surveillance and for the extension of warfare by other means. The first section explores how digital communication and new media have become key weapons of contemporary network-centric warfare. I deploy the term “fog of peace” to conceptualize the ongoing, emergent, and unpredictable relations between governmental intervention, military logistics, and the manipulation of public perception. While modern warfare has been defined as regulated armed conflict between sovereign states via their militaries, the War on Terror has tended towards the opposite, namely the involvement of non-state actors, the circumventing of borders (that is, definite geographical theaters of war), as well as the exploitation of conditions of indeterminacy, contingency and ambiguity. I hypothesize that the War on Terror has become entangled with the emergence of surveillance states, and surveillance societies, turning the state into predator, and civilians into prey. In the final section, I speculate that the War on Terror is not primarily about eradicating terrorism but more about establishing the conditions for total surveillance, social control, and bio-informatic exploitation. I conclude with reflections on the War on Terror and its relation to posthuman governance, that is, the tendency toward replacing human centered command systems with algorithmic mechanisms. The War on Terror has enabled the establishment of a global architecture of surveillance techniques and technologies that emphasize the necessity of hyper-visibility and are driven by information extraction, analysis, manipulation, commodification, and bio-informatic control.

II. The Surveillance State and Predatory Politics

It is noteworthy that the War on Terror has become embroiled with the development of a growing tendency oriented around struggles for information dominance and data governance, i.e., the politics concerning the creation, capture, dissemination, storage, and ownership of information (especially, but not exclusively, digital information). The internet, mobile devices, and predictive technologies have been used to create popular revolutions against governments perceived as unjust, mobilize huge swathes of populations, and enable large-scale acts of popular protest. However, these technologies are easily hacked and weaponized, making them not only platforms for empowerment but also vehicles for spreading virulent narratives and reactionary ideologies that awaken and inflame historical hatreds and cultural traumas, creating
enormous upsurges of popular sentiment that are difficult to foresee or regulate (let alone legislate). Ironically, while widely-used social media and information communications technologies give users the feeling that they are not passive consumers but rather active creators of information, the new information ecosystem is highly predatory. It tends to exploit vulnerabilities and reinforce rather than challenge opinions, biases, and beliefs. Messages can be easily and directly circulated, modified, and amplified without the need for any centralized authority or adjudicating body. For these reasons, digital communication and new media have become key weapons of contemporary network-centric warfare both for extremist, fundamentalist, and revolutionary groups, as well as for governments that argue that the needs of national security trump the demands of individual civil liberty.

Instead of being a well-defined set of military imperatives governed by the regular norms of war (which would include the necessity for nations to determine and delimit a geographical theater of war), the notion of a War on Terror remains a fuzzy concept. This definitional ambiguity has allowed the term to be widely used by actors across every media platform available. Politically and militarily, the War on Terror is not fought primarily using the laws of war but rather operates in a global environment of hyper-mediatization in which the historical boundaries between wartime and peace-time are increasingly entangled, conflated, and reconfigured against the backdrop of crises and multiple threats to physical, social, and ontological security. Threats, especially so-called “terrorist threats,” are re-configured as omnidirectional, synchronous, and asymmetrical subversions within complex, multiple, and often covert informational ecologies.

This is the figure of today’s threat: the suddenly irrupting, locally self-organizing, systemically self-amplifying threat of large-scale disruption. This form of threat is not only indiscriminate, coming anywhere, as out of nowhere, at any time, it is also indiscriminable. Its continual micro-flapping in the background makes it indistinguishable from the general environment, now one with a restless climate of agitation. Between irruptions, it blends in with the chaotic background, subsiding into its own pre-amplified incipience, already active, still imperceptible. The figure of the environment shifts: from the harmony of a natural balance to a churning seed-bed of crisis in the perpetual making.¹¹

Buttressed by the rhetoric of crisis and disaster, democratic governments have sought to indefinitely modify (and even erode) democratic norms and practices in order to deal with not just current threats but potential future threats as well. In large part, the War on Terror has turned out to be a phenomenon in which near-perpetual connectivity modulates the psychological states of insecurity and security, amplifying emotions, opinions about, and thus affects of potential threats. In this sense, mediatization becomes a weapon of digital warfare, and the (exceptionalist) discourses about “exceptions” to rules and norms thus allow governments and media
corporations to engage in public manipulation of perceptions and mask their roles in extending the logic of war-time operations into the everyday spaces of civil society. The War on Terror exploits the fog of peace: the once separate spheres of war and peace have become overlapped and indistinguishable to such an extent that ambiguity and uncertainty come to serve as tools and weapons used by governments in collusion with law enforcement agencies, militaries, and scientific and knowledge-producing institutions like universities. Ambiguity and crisis feed the production of fear and anxiety, which in turn create opportunities for “hair trigger responses” (a term infamously used by the G.W. Bush Administration after 9/11). As the fog of peace uses uncertainty and ambiguity to its advantage, the War on Terror becomes primarily about gaining advantage over how information is presented and perceived. The fog of peace, fostered by hyper-mediatization, has led to the production of an ongoing and emergent set of unpredictable relations between governmental intervention, military logistics, and the manipulation of public perception. The management of this unpredictability and insecurity has become a primary preoccupation of global security policies. By way of the fog of peace, the War on Terror has basically led to the tactical and indefinite extension of war into all spheres of life.

What happens when the distinction between war-time and peace-time becomes ambivalent and conflated? The distinction between friend and enemy also becomes dangerously ambiguous. The enemy is no longer another sovereign nation but now potentially a network of larval (that is unknown and undefinable) operatives who can and do engage in hypercamouflage (constant shape shifting). The public enemy is constructed by media and security agencies as fundamentally “unknown” and ambiguous, no longer lying outside national borders but now potentially within the body politic which becomes exploited as an immanent plane for encroachment and imperceptible incursion. Thus, counter-terrorism policies, which attempt to root out not just real current terrorist threats but potential future ones as well, end up targeting and militarizing their own civilian populations. This is apparent in the militarization of police forces as well as the militarization of borders and bodies across North America (and elsewhere around the globe). The civilian shifts from being conceived as a legally, politically, and morally protected actor under the international laws of warfare to a set of potentially ambiguous behaviors that become subject to new forms of bio-political and biometric control, social/racial/gender sorting and profiling, risk management systems, and automated/algorithmic surveillance technologies meant to pre-emptively detect patterns of deviance.

Framing the War on Terror as a “new kind of war,” as the American government did, was itself not new or unprecedented; in fact, “we are in an era of ‘new’ wars, or what have also been called ‘low-intensity conflicts,’ ‘fourth-generation warfare (4GW),’ ‘small wars,’ network-centric warfare,’ ‘nonconventional,’ ‘hybrid,’ and ‘asymmetric’ wars.” Classical symmetric warfare is modeled as a “duel on a larger scale” where two militaries have similar power resources, and tactics. By contrast, asymmetric, non-linear, and/or hybrid conflicts (as they are variously called) occur between powers
that have disparate capabilities (involving non-state actors). Asymmetric conflicts aim for full-spectrum or total dominance that combine the use of unconventional strategies and tactics of war and new mobile information/communication technologies, including social media. Framing warfare as “new” and “irregular” thus allows the logic of war to usurp the norms of peace—to surreptitiously not just depoliticize (and instead moralize) but also militarize the historical distinctions and legal differences between war and peace, states and non-state actors, and combatants and non-combatants. In this regard, peace becomes an extension of war. “Asymmetry” allows historically powerful states to depict themselves as vulnerable victims of non-state actors, thus rhetorically translating technical and strategic differences between states and non-state actors into moral hierarchies between civilizations that then are used to authorize the circumventing and suspension of international laws and norms. Although the American government framed the War on Terror as a new kind of war involving a new kind of enemy, the claim itself was not new and drew on the prevailing discourse of asymmetric warfare used to characterize specific types of armed conflict in densely civilian-populated areas. In addition to the GWOT, examples of asymmetric warfare include civil wars and insurgencies in the former Yugoslavia, Afghanistan and Iraq, Palestine, Somalia, Angola, Congo, and Sierra Leone, as well as low-intensity wars in Colombia, Indonesia, and in Kashmir. The terminology is also applied to the campaigns of non-state actors like al-Qaeda. By emphasizing states’ vulnerabilities to certain kinds of tactics and enemies, this discourse allows states to selectively rationalize brutal tactics against non-state actors; to justify collective punishments of entire populations; and to defend maneuvers that cause high casualties among civilians. The idea of asymmetry functions as a source of legitimacy because it frames the confrontation between states and their “asymmetric” enemies in moral terms and transposes that confrontation onto a neo-colonial template of civilized vs. uncivilized forms of warfare.

The “surveillance state” combines state-sanctioned, corporatized, and ideological politics of social, cultural, racial, and gender policing with propaganda capacities to influence and control individual and collective bodies through the use of the “contagious” architectures and “infectious” objects of new media, i.e., the highly adaptable, manipulable, portable, and often imperceptible information/communication/mediatechnologies (hardware and software) that are quickly becoming the preferred weapons of digital warfare. As globalizing societies become more and more digitally connected and network-centric, so too the nature and conduct of war become digital and network-centric.

Post 9/11, the United States’ decision to wage war against a non-state trans-national network deviated from historical precedence insofar as states tend to treat the violence of non-state actors as a law enforcement issue and under federal legal codes, rather than under military rules. In situations of armed conflict, states can engage in conduct that exempts them from certain domestic and international norms. In war, for instance, it is generally accepted that the state can kill an enemy combatant regardless
of whether s/he is about to commit an atrocity. Moreover, the norms of detention
and prosecution are determined by military law and military courts; for instance,
the state can detain an enemy combatant without charge for the duration of a given
conflict. In peace-time, conversely, liberal human rights regimes expect that the
state will try to domestic laws before it makes decisions about using lethal force;
states are expected to release detainees within a certain period or charge them with
a criminal offense. First and foremost, the American government’s position was
underpinned by the claim that it was in a state of armed conflict but that it faced a
situation of exceptional insecurity because it was at war not with another state but
with a new kind of enemy: a transnational non-state network. This argument allowed
the Bush Administration to both invoke the war-time conditions of international law
and also exempt itself from aspects of the international laws of war. The United
States declared that certain aspects of the Geneva Conventions on the laws of war
did not apply to al-Qaeda because common Article 2, which triggers the provisions
regulating detention conditions and procedures for trial of prisoners of war, is limited
only to declared war or armed conflict between two or more High Contracting parties.
Since al-Qaeda is not a “High contracting party,” the American military’s treatment
of al Qaeda members would not be governed by the Geneva Conventions’ provisions
concerning prisoners of war.

In American response to the War on Terror, George W. Bush and the American
government inaugurated an “international manhunt,” which gave American military
forces the authority to go beyond the conventional legal limits in pursuing the enemy.
Unlike classical warfare, the model of the “manhunt” is not structured along the lines
of a duel and does not take the form of a direct confrontation, but instead proceeds as
a process of tracking down. Moreover, the power relationship between adversaries is
marked by radical dissymmetry in weaponry and the enemy is not recognized as an
equal, but as only prey. In the War on Terror, the manhunt model was intended to
serve as a new military doctrine depicting the enemy as an indefinite and continuously
imminent threat, as well as emphasizing pre-emptive (offensive) warfare.

The territorial and terrestrial norms of war (which were once based on the ancient
Greek model of agon, or “contest,” between relatively equal opponents in battle)
involve delimitations (e.g., of the theaters of war), definitions (e.g., regarding rules
and conduct of warfare), and decisions (e.g., regarding organizational planning or
logistics) in accordance with state-centered political rationales. The fog of peace
obfuscates the territorial/terrestrial norms of war by introducing and superimposing
other predatory, asymmetric, and larval motivations and frameworks. The militarized
manhunt departs from normal territorial warfare which relies on linear, laminar, and
hierarchical notions such as fronts, linear battles, and face-to-face confrontations.
The opacity generated by amplifying uncertainty is deployed and used to tactically
(and even radically) to amplify turbulences and flows that disorient—and reorient—the
normal polarities of power. When faced with asymmetrical threats such as small,
mobile, flexible, and unknown non-state actors, the normative model of war structured
like a duel fails to elucidate or give advantage within a nebulous geometry of warfare involving not the face-to-face contestation of military forces but rather a hunting ground that establishes predator-prey behavioral ecologies. The War on Terror becomes entangled with the emergence of surveillance states, surveillance societies, and surveillant assemblages, transmuting the state into a “hunter” and the civilian into the hunted:

In the competition between two enemy combatants, the goal is to win the battle by defeating the adversary – both combatants must confront to win. However, a manhunt scenario differs in that each player’s strategy is different. The fugitive always wants to avoid capture, while the pursuer always wants to engage and capture the target – the pursuer must confront to win, whereas the fugitive must evade to win. The first task no longer involves immobilizing the enemy but instead requires identifying and locating him. The art of modern tracking proceeds by means of a cartography of the prey’s social networks that the “hunter-analysts” piece together in order to succeed in tracing him back, through his friends or relatives, to his hideout. The prey who wants to escape his pursuers tries to become undetectable or inaccessible. The hunter’s power has no regard for borders. It allows itself the right of universal trespassing, in defiance of territorial integrity of sovereign states. It is an invasive power which, unlike the imperial maneuvers of the past, is based less on a notion of right of conquest than of a right of pursuit.

War ceases to be a symmetrical activity engaged in by judicious but opposing nation states according to international norms of conduct and instead becomes conceived as the interaction between predator and prey. The use of unmanned aerial vehicles (UAVs), or drones, to conduct targeted assassinations, as well as the use of drones in commerce and policing, are exemplary of the growing shift towards predatory forms of warfare. The drone is more than just the technology of choice today; it is also an emerging horizon that establishes the predatory game space that will define the norms of social, political and military interaction in the future. Within the model of the manhunt, the imperial will for domination is abstracted from its territorial constraints and redeployed in a nebulous machine of global predation that conflates and connects surveillance, control, and counterterrorism with the history of colonialism, slavery, and racism. Here, the manhunt is not a metaphor so much as a diagram based on “concrete historical phenomena in which human beings were tracked down, captured, or killed in accord with the forms of the hunt.” Being hunted animalizes the prey and ensures that the hunter almost never has to confront the prey directly, deploying both animal (e.g., either mercenaries and/or hunting animals) and machine instruments to track, capture, and kill in its stead. Because of this mediation and substitution, the manhunt exonerates the predator from having to risk its own life and transfers all the risks of death onto the prey. And yet, to capture its prey the predator must also try to think like its prey by masking its predatory nature, becoming in some perverse but
useful sense like its prey and performing the asymmetric sleight of hand in which the strong becomes like the weak and the weak becomes like the strong. The logic of asymmetry allows strong states to depict themselves as vulnerable, thus justifying the rapid development of “risk-transfer war” characterized by remotely-controlled drone strikes, in which all the risks are transferred to populations overseas.  

In many ways, the drone incarnates predation: it is both a weapon claimed to carry out surgically-precise strikes and a mechanic, “mobile panopticon” that can see, track, and elucidate the fog of war with data collected from machines and mechanisms of optical, electronic, and digital information capture and surveillance. The drone turns optical power into weaponry that can be used to sense, track, and kill: “[t]he best definition of drones is probably the following: ‘flying, high-resolution video-cameras armed with missiles.’” The drone—originally designed for reconnaissance purposes in military operations—is more than simply the human master’s faithful servant. It is more than just a technical instrument that can pierce through the fog of war and help win the War on Terror. The drone presents itself as an innovative replacement for animal-powered systems and a technological servant to its human masters, but unlike the dog or horse, its perceptive and computational capacities far exceed that of the animal, even the enlightened human ones. The drone is an instrument and emblem of masked warfare. It appears as illuminating, instrumental, and risk-transferable (where the disadvantages are assumed by opponents), and thus the digitization of warfare is increasing at a rapid pace. However, it also masks its de-territorializing tendencies and makes imperceptible (to the human eye, at least) the systemic and extra-systemic vulnerabilities produced by these deterritorializations. Within such a nebulous regime, the technical capacities to digitally model, trace, analyze, and archive become not just the way of seeing—of tracking and killing enemies—but also a way of knowing, of predicting and forecasting, of re-ordering and re-designing spatialities and temporalities. Drones can record and analyze the lives of targets. Further, when cross referenced with data from other forms of digital communication, drones can be used to go back in time to reconstruct events and to look to the future to predict where targets may be, thus justifying the nebulous regimes of predation, preemption, and prediction.

As the distinctions separating war and peace become more porous and entangled, so too do the distinctions between distant foreign enemies and enemies within become more enmeshed and confounded. Thus, predatory politics reconceptualizes the nebulous “terrorist enemy” as larval and ambiguous. Rather than being concrete, localizable, and identifiable, it is ephemeral, fleeting, ungraspable, and spectral. “In contrast, the asymmetric enemy, wrapped in civilian dress, is harder to trace. Indeed, their ‘disguise’ gives them an armour more effective, in some respects, than that worn by conventional soldiers.” The implication is that the enemy is a type of “shape-shifter” that is capable of something which, on the one hand, makes it harder to identify, recognize, and kill but which, on the other hand, makes it all the more inhuman or quasi-human and thus more necessary to kill without compunction. The
asymmetric logic of the asymmetric enemy is depicted as capacities and behaviors that are ambiguous, decentralized (even “swarm-like”), stealthy, and in a state of indiscernibility in which the switching of identities (especially between friend and enemy, predator and prey) is used to exploit and gain advantage.

III. Posthuman Governance: Data Hegemony and Algorithmic Regulation

The concept of planetary information surveillance is about control, not terrorism, because it has less to do with sovereign rights and state responsibilities to protect nations and citizens against the threat of terrorism and more to do with the business of gaining hegemony over the mediation of information. While governments and states continue to compete with one another to gain advantage economically, politically, and militarily, emerging data surveillance architectures are learning how to exploit the infectious qualities of digitality and net-centricity while simultaneously discovering how to circumvent the physical and legal constraints imposed on the conduct of international warfare. War is no longer just about gaining hegemony over actual physical territory—it is increasingly about informational dominance, or gaining hegemony over virtual domains through viral forms of information and communication. This ambiguous mode of warfare involves non-state actors, non-military targets, conventional consumer digital technologies, and unconventional online weaponry like misinformation, disinformation, cyber hacking, and trolling, which center on heightening rather than diminishing widespread cultural insecurities and ideological fears of so-called terrorist related threats. The War on Terror is not primarily about eradicating terrorism; instead, the various competing discourses of counter terrorism in circulation (whether focused on security or conversely on liberty) heighten societal insecurities and create conditions for total surveillance, social control, and economic exploitation.

More and more, governments and militaries all over the world (regardless of ideological affiliations and geo-political interests) are employing modes of persuasion that are primarily non-military and increasingly informational, techno cultural, and mediational. War is no longer something that arises chiefly between sovereign states and their militaries—something in which the spatial and temporal boundaries between it and peace can easily be identified, maintained, and regulated by international norms and laws. Instead, emerging surveillance states seek to deploy the primarily technical (not political) force of viruses, algorithms, and increasingly autonomous machines of information capture and surveillance to use against humans. This is despite state rhetoric that this force is to increase human security and benefit human beings in the long term. While app-driven mobile technologies have been touted as positive instruments which enhance political liberty and economic transformation, these very technologies have been used to galvanize the politics of fear and create widening ideological, racial, economic, and socio-cultural insecurities and instabilities in global affairs.33

Framed within the discourses of counter terrorism and national security and
buttressed by the rhetoric of internet centrism and technological solutionism, the War on Terror and its arsenal of surveillance, biometric, and cognitive technologies are developing at a rapid pace by circumventing the political laws of armed conflict. It is not simply that digital technologies are becoming central to emerging practices of warfare; it is that the horizons of political possibilities are being shaped by technical rationales in which the goal of competing actors becomes dominance within the sphere of information. As evidenced by the terrible success of groups such as ISIS and the cyber-propaganda initiatives of nations such as Russia, the quest for dominance in the realm of information has become a significant force driving present and future global conflict. The growing use of digitally-networked information and communication technologies has resulted in making the access and control of information a central object of governmental, financial, scientific, commercial, and popular struggles for power. Yet these very same technologies are revealing a power to affect and modulate their users: to prime user perceptions, influence user beliefs and behaviors, and make users subject to an emergent regime of info-gluttony and datamania.

The rise of the Big Data paradigm—that is to say, the paradigm of massive scale data analytics that governs not only university research but every other discipline and field of human endeavor today—has ushered in a datalogical turn, in which humans and their everyday behaviors become datafied. The term data, of course, is in no way new. Scientific and social-scientific research have been data-driven for the better part of six decades now, especially since the integration of computer and computational systems into the research process. What is new, however, is that data is no longer viewed simply as signal parsed from noise (that is, as raw data that has been cleaned). The real allure of Big Data is not found in its representational content—that is, in its ability to “describe a stabilized system or to follow a representational trail, but instead to collect information that would typically be discarded as noise. Indeed, it is those data that are most typically bracketed out as noise[ . . . ]—that is: affect, or the dynamism of non-conscious or even non-human capacity—that are central to the datalogical turn.” This is an important point to keep in mind because it is key to understanding how and why increasing digital connectivity is quickly phasing human decision making and intervention out of the datalogical loop, thereby establishing data hegemony through information feedback and feedforward networks. This is what I call post-human governance—that is, the tendency toward replacing human centered command systems with algorithmic based commands. Historically, this idea of a commanding or governing principle became the seed idea for Norbert Wiener’s conception of cybernetics (who borrowed the term directly from Plato), which extended the commanding principle to animals (including humans) and machines. Cybernetics, according to Wiener, is the science of governance, namely the ability of a closed system to maintain its stability by constantly learning and adapting itself to changing circumstances. Cybernetics was conceived, especially by Wiener, as a kind of “new Scientific Enlightenment,” which would liberate humans from servitude and renew the scientific and moral spirit of humanity (largely caused by the deleterious consequences of the scientific development of the atomic
Algorithmic based command or regulation thus promises to fulfill the dream of cybernetic governance and is currently being promoted as a new technical paradigm for social and political governance based on online, digitally-interconnected services that directly respond to user generated data. Algorithms are any encoded procedure for calculating input data into a desired output, and algorithmic logic regulates what and how information is perceived and presented to users, entrenching the dominion of computational governance into human living through grammars of action and protocological or network control (e.g., within machine-to-machine communications). Algorithmic regulation has come to take center-stage in the contemporary sciences of governance by way of data hegemony: the condition in which data and the datalogical are in command of decision-making processes, a command that in a bygone era was occupied by humans.

Increasingly, the War on Terror is under the sway of posthuman governance mechanisms that are establishing data-hegemonies throughout societies at all levels of social life. Under the auspices of Big Data analytics and their ideologies of security which claim that the emerging techno sciences of prediction, biometrics, and facial recognition can serve as powerful and enabling ways to fight global terrorism, the War on Terror has become enmeshed with the emergence of surveillant assemblages. Though fragile, algorithms are not merely abstract and technical achievements but rather key drivers of the tendency towards data hegemony and posthuman governance which are converging to form a planetary wide apparatus of information governance and regulation.

The concept of information itself has no single, unified definition, even though there are various theories that have been put forward to conceptualize it (i.e., initially, as a communication process based on signal/noise transmission, or feedback and/or stimulus/response circuits). However, information is increasingly being conceptualized as data or a thing akin to a commodity-cum-object that can be possessed (indeed purchased), traded, and legislated. Governance in the information era is the governance of information: all data, whether big or small, both signal and noise alike, are appropriated and applied (captured, categorized, and conveyed) by military, market, and techno-scientific mechanisms of informatic regulation. Whereas in the past, the mission of research was to cleanse data of noise in order to extract usable and codeable data (that is, large patterns of regularity that could then be made subject to various processes of data analytics), today’s data hegemony operates on the military principle of total information awareness. Noise “is always already valuable information because it allows for resetting parameters. Not only do big data technologies seek to parse, translate, and value noise, but also they enhance its production by taking volatility as their horizon of opportunity.”

IV. Conclusion: Welfare, Surveillance, and Capitalism

From politics and warfare to commerce and social-media, it is data hegemony that is directing the course of planetary futurity. The data sciences are not just a method or
set of methods, but a frame that is reorganizing how knowledge is being perceived, generated, and categorized and how circuits of power are being reconfigured and renormalized. While it is true that the internet, mobile devices, and social-networking apps have been used to mobilize populations and to enable large-scale acts of popular protest, these very same technologies are first and foremost corporate tools. Moreover, they are monitored (never mind monetized) networks: networks that are themselves used as nets to gather, go through, and govern (that is, “lead,” “steer,” “direct”) information by way of misinformation, namely through many networks of relays and re- or rather misdirection that make use not of Truth and its symbolic interpretations, but on truthiness, illusion, hyperbole, falsification, divergence, hysteria, and the diffusion of a larval, cryptic, and fractal kind of terror. Such platforms are, consequently, rather perfect for the spreading of so-called viral narratives in all of their fragmentary forms. These are engines that are perfectly “primed,” as they say, for reactionary ideas that typically awaken and inflame historical and histrionic hatreds and appeal to the base and basic mechanisms inherent to the social mechanics (social-structure) of the human animal. In consequence, the structure and dynamics of these platforms foster enormous upsurges of popular sentiment which are difficult to foresee or to regulate (never mind legislate). The War on Terror has enabled the establishment of a global architecture of surveillance technologies that emphasize the necessity of hyper-visibility and are driven by information extraction, analysis, manipulation, commodification, and control. In the information era, political governance and larval war are intertwined; both entail governing not only physical bodies and relations but increasingly virtual ones as well. As globalization extends further by way of the expansion and adoption of digital information and communication technologies that make it easier for human beings to become connected beyond physical boundaries and national borders, every human activity will involve generating data that can be mined and monetized. This is an emergent logic of accumulation in the networked sphere and what some are calling surveillance capitalism, which is characterized by often opaque mechanisms of extraction, commodification, and control that alienate people from their own bodies and behaviors while generating new markets of prediction and speculation. As the trend towards smartification continues with ubiquitous and ambient computing (e.g., the Internet of Things and smart cities), the complete integration of physical and virtual environments will mean that every aspect of the environment—including the body—becomes potentially data-rich and ready to be tapped, even fracked. Humans are not only colonizing each other by way of technologies and information. In the empire of the digital, all humans are being colonized by algorithmic mediation as the digital takes hold over the planet and every sphere of knowledge. Under the banner of fighting the War on Terror, ever-more-sophisticated intelligent machines are being developed and adopted, not just weaponized drones for use in military operations, but also as weapons of information surveillance, from biometric and geo-locative technologies to consumer preference tracking technologies that extract and profit from information about civilian metadata. Politically and militarily, the War on Terror has not been fought primarily using the laws of war but has operated in a global surveillance
environment in which the historical boundaries between war-time and peace-time are increasingly entangled, conflated, and reconfigured due to so-called crisis conditions. Reinforced by the rhetoric of crisis and disaster, the War on Terror has played a central role in introducing and perpetuating war-time operations within public and private civilian life. War is no longer merely a tool of policy, as the traditional theory of modern warfare that is supposed to currently govern the global system might assume. Policy itself is adapting to the larval and shape-shifting imperative of war that targets human and non-human alike. As much as humans continue to believe that they are in control of this informational imperative, what is being revealed instead is that human endeavors themselves are being shaped by the larval tendencies of information.

Nandita Biswas Mellamphy is Associate Professor and Undergraduate Chair of Political Science; an affiliate in Gender, Sexuality, and Women's Studies; core faculty in (and former Associate Director of) the Centre for the Study of Theory and Criticism; and founding Director of The Electro-Governance research group (EGG), all at Western University in Canada. Currently, she is Assistant Editor of the *Canadian Journal of Political Science*, as well as an Associate Editor of *Interconnections: Journal of Posthumanism*. Her areas of study are situated at the intersection of Political Theory, Continental Philosophy, and Information/Media Studies.

Notes and References

1. The “War on Terror,” or the GWOT (Global War on Terrorism), is a term referring to the global military campaign spearheaded by the United States after September 11, 2001 to deal with terrorist threats. The term has been hard to define concisely, as it is complex and subject to a high degree of definitional ambiguity and conceptual contestation. The Dictionary of Terrorism, for instance, provides an expansive rather than narrow definition of the term “War on Terror” as being “a complex array of domestic and foreign policies;” as an “open-ended conflict” resulting in “curtailing of civil liberties;” and also as “a series of policies” enacted at “the military, political, cultural and legal levels,” both domestic and international. David Wright-Neville, *Dictionary of Terrorism* (London: Polity, 2010), 200-1. As yet, there is no internationally-accepted definition of the term. Anne Bayefesky, ed., “There Is No UN Definition of Terrorism,” *Human Rights Voices*, 2018, [http://www.humanrightsvocies.org/un-101-facts/there-is-no-un-definition-of-terrorism](http://www.humanrightsvocies.org/un-101-facts/there-is-no-un-definition-of-terrorism).

2. Kenneth Roth argues that the War on Terror “stretches the meaning of the word ‘war’ [. . .]. The Bush administration has used war rhetoric precisely to give itself the extraordinary powers enjoyed by a war-time government to detain or even kill suspects without trial. In the process, the administration may have made it easier for itself to detain or eliminate suspects. But it has also threatened the most basic due process rights. [. . .] By literalizing its ‘war’ on terror, the Bush administration has broken down the distinction between what is permissible in times of peace and what can be condoned

3. According to Mary Ellen O’Connell, “the Bush Administration’s case has virtually no support in the wider international legal community—the community beyond the Administration’s own people. The claim of global war is a radical departure from mainstream legal analysis. Moreover, claiming global war is turning out to have negative unintended consequences, such as enhancing the status of terrorists on the international plane and creating a dangerous legal precedent that other states are following. [...] Now the Russians, in addition to Americans, believe they may target their enemies anywhere—including the streets of peaceful cities. These declarations of war are undermining the prohibition on the use of force, enhancing the status of terrorists and making the world a more dangerous place where human life is ever more de-valued.” Mary Ellen O’Connell, “The Legal Case against the Global War on Terror,” Case Western Reserve Journal of International Law 36, no. 2 (January 1, 2004), 357.

4. War operates in conditions of uncertainty. The military theorist Carl von Clausewitz called this uncertainty in the context of war, “friction” or as it came to be known as the “fog of war.” This uncertainty, or “fog,” is part-and-parcel of the whole process of war, according to Clausewitz—war being a realm where opacity, volatility, complexity and ambiguity reign supreme. The frictions or impediments caused by the uncertainty of war could include such intangible factors as fear, chance obstacles, and informational challenges—anything that hampers the military commander’s capacity to control, exploit and ultimately overcome the effects of uncertainty in battle. It is the goal of military strategy to reduce, contain, and overcome the fog of war as much possible. War must remain in service of the normative political goals of nation-states; it should be regarded as a tool of policy and must always be in service of advancing a state’s political aims; military logic must always be subservient to political rationale. Carl von Clausewitz, *On War*, trans. Michael Howard and Peter Paret, *Oxford World’s Classics* (Oxford: Oxford University Press, 2008), 8, 30.

5. “Even the vocabulary of this war will be different. When we ‘invade the enemy’s territory’, we may well be invading his cyberspace. There may not be as many beachheads stormed as opportunities denied. Forget about ‘exit strategies’; we’re looking at a sustained engagement that carries no deadlines. We have no fixed rules about how to deploy our troops; we’ll instead establish guidelines to determine whether military force is the best way to achieve a given objective.” Donald H. Rumsfeld, “A New Kind of War,” *The New York Times*, September 27, 2001, sec. Opinion, https://www.nytimes.com/2001/09/27/opinion/a-new-kind-of-war.html

6. The term “hyper-mediatized” is a version of what Hoskins and O’Loughlin call the *mediatization of war*: “If we probe the connections between humans, technology and media to interrogate the emergent character of war and terrorism, we find that they all inhabit the same and unavoidable knowledge environment, what we have called our new media ecology. To write of the mediatization of the conduct of war is to refer to
the manner in which media are integral to those practices in which actual coercive or kinetic force is exercised, such the guiding of troops and vehicles, the use of drones, the symbolic acts of violence central to terrorism, insurgency, and, indeed, major military operation.” A. Hoskins and B. O’Loughlin, *War and Media: The Emergence of Diffused War* (Cambridge: Polity, 2010), 5.

By hyper-mediatization, I am attempting to push this idea toward the conclusion that the mediatization of war is itself set within the context of the hyper-driven excesses of communication, or as Jean Baudrillard explains, “the problem of our whole society expanding, transcending, exhausting itself in the fiction of communication. […] We are at the critical limit where all effects can be reversed and communication vanishes into an excess of communication. […] Today, oppression occurs not primarily by way of coercion, force, and repression of political power — that is, through the deprivation of information and communication — but rather through the excesses of information, and by way of the obligation to be more and more connected, more and more closely tied to the screen in restless circularity and auto-referentiality as integrated network.”


7. Anna Reynolds, ed., *Social Media as a Tool of Hybrid Warfare* (Riga: NATO Strategic Communications Centre of Excellence, 2016), 34, 40.

8. Reynolds, *Social Media as a Tool*.


10. “The deployment of particular threat and referent labels established in discourse before events such as 9/11 or 7/7, such as ‘international’ terrorism, helped enable the shift from counterterrorism law from temporary emergency response to permanent policy practice.” Kathryn Fisher, “Terrorist Threat Construction and the Transition to Permanent British Counterterrorism Law,” *Journal of Terrorism Research* 2, no. 3 (November 11, 2011),


17. Ibid, 490.


21. “On July 22nd, Secretary of Defense Donald Rumsfeld issued a secret directive ordering Air Force General Charles Holland, the four-star commander of Special Operations, ‘to develop a plan to find and deal with members of terrorist organizations.’ He added, ‘The objective is to capture terrorists for interrogation or, if necessary, to kill them, not simply to arrest them in a law-enforcement exercise.’ The manhunt would be global in its reach, Rumsfeld wrote, and Holland was to cut through the Pentagon bureaucracy and process deployment orders ‘in minutes and hours, not days and weeks.’” Seymour M. Hersh, “Manhunt: The Bush Administration’s New Strategy in the War against Terrorism,” The New Yorker, December 15, 2002, https://www.newyorker.com/magazine/2002/12/23/manhunt.


24. “The transformation of territorial lines into a Mœbius-strip rearticulates the sovereign games that states usually play. While big data collection blurs categorizations of what is ‘domestic’ and what is ‘foreign’, the consequent reconfiguration of the boundaries of the sovereign state into a Mœbius-strip has in turn become a site, in and of itself, of political struggles, resistance and dissent. Along the Mœbius-strip, states, social movements, and individuals can play a variety of games, reenacting the meanings of sovereignty and citizenship, security, and liberty.” Zygmunt Bauman et al., “After Snowden: Rethinking the Impact of Surveillance,” International Political Sociology 8, no. 2 (June 1, 2014): 121–44, at 128.

25. “[W]e are witnessing a convergence of what were once discrete surveillance systems to the point that we can now speak of an emerging ‘surveillant assemblage’. This assemblage operates by abstracting human bodies from their territorial settings and separating them into a series of discrete flows. These flows are then reassembled into distinct ‘data doubles’ which can be scrutinized and targeted for intervention. In
the process, we are witnessing a rhizomatic leveling of the hierarchy of surveillance, such that groups which were previously exempt from routine surveillance are now increasingly being monitored.” Kevin D. Haggerty and Richard V. Ericson, “The Surveillant Assemblage,” The British Journal of Sociology 51, no. 4 (2000): 605–22, at 606.


28. Chamayou, Manhunts, 7.


34. See Evgeny Morozov, To Save Everything, Click Here: The Folly of Technological Solutionism (New York: Public Affairs, 2014).

35. See StratCom’s analysis of ISIS and Russia’s use of social media in Reynolds, Social Media as a Tool of Hybrid Warfare, 21–41.


39. The cybernetic research of Wiener and his colleagues were in keeping with military research (Wiener had participated in the war effort by developing a servo-mechanical weapon known as the AA predictor); military applications were also the context for the development of Claude Shannon’s theory of telegraphic information transmission (as set out in *The Mathematical Theory of Communication* in 1949). See Céline Lafontaine, *L’Empire cybernétique. Des machines à penser à la pensée machine*, SEUIL edition (Paris: SEUIL, 2004), 28–9.


41. Grammars of action occur when computational logic and modeling of human activity become normalized: “The capture model describes the situation that results when grammars of action are imposed upon human activities, and when the newly reorganized activities are represented by computers in real time.” Philip E. Agre, “Surveillance and Capture: Two Models of Privacy,” *The Information Society* 10, no. 2 (April 1, 1994): 101–27, at 125. Protocol “is a totalizing control apparatus that guides both the technical and political formation of computer networks, biological systems, and other media. Put simply, protocols are all the conventional rules and standards that govern relationships within networks. Quite often these relationships come in the form of communication between two or more computers, but ‘relationships within networks’ can also refer to purely biological processes, as in the systemic phenomenon of gene expression.” Alexander Galloway and Eugene Thacker, “Protocol, Control, and Networks,” *Grey Room* 17 (October 2004): 6–29, at 8.


45. “In modern 21st-century warfare, non-military approaches—propaganda, and economic, cultural and humanitarian sabotage—will play a greater role than purely military methods, Russian Armed Forces chief Valery Gerasimov argued, a year before the Russian occupation of Crimea. ‘In a couple of months, even days, a well-functioning state can be turned into a theater of fierce armed conflict, can be made a victim of invasion from outside, or can drown in a net of chaos, humanitarian disaster and civil war’, he wrote. The purpose of war today is not the physical destruction of the enemy, but the internal eroding of our readiness, will, and values.” Eerik-Niiles Kross, “Putin’s War of Smoke and Mirrors,” *POLITICO* (blog), April 9, 2016, https://www.politico.eu/article/vladimir-putin-war-smoke-and-mirrors-russia-occupation-crimea-ukraine/.

Also see Shoshana Zuboff, “Big Other: Surveillance Capitalism and the Prospects of an Information Civilization,” *Journal of Information Technology* 30, no. 1 (March 1, 2015): 75–89.