Journal of Military and Strategic Studies

JMSS

VOLUME 18, ISSUE 4

Annual Award of Excellence 2018

Second Place

Coded Conflict: Algorithmic and Drone Warfare in US Security Strategy

Benjamin Johnson

> Now, we concluded that we were pretty good in our force structure [....] with one key exception, and that turned out to be intelligence surveillance and reconnaissance. For all of those of you in this business, you know you can never have enough. It's a constant guess. And no matter where you end up, you always need more. [....]
>
> So, we'll be looking for promising technologies that we can do in what we call the FYDP, the future years defense program, generally about five years out. We'll

ISSN : 1488-559X

identify long-range advances that we can pull up and hopefully field in the '20s, and then we'll plant the seeds for R&D, which will give us an advantage for the '30s.

So we’re actually thinking of this thing in terms of [...] never ending –

Deputy Secretary of Defense Bob Work,
Willard Hotel, Washington, D.C.,
Jan. 28, 2015[1]

Introduction

It has been argued that that the character of modern conflict has changed when compared to the inter-state conflicts that find their historical antecedents in the Napoleonic wars. These ‘old’ types of conflicts arguably culminated into the *total* and potentially world-ending scenarios that dominated the twentieth-century’s great power confrontations.[2] More recently, the clean outlines that delineate war time from peace time have been rendered seemingly anachronistic. The *where*, *when* and *how* of war, its rationality and logic that Clausewitz elucidated long ago, has by many accounts been displaced by a less bounded form of conflict. War, to echo the sentiment of Bob Work noted above, is now permanent and everywhere.[3]

Whatever the actual qualitative differences between ‘old and ‘new’ wars, technology has undoubtedly always factored into the underlying logic of war-making. In recent years, the place of surveillance and remote strike capabilities have factored heavily into these discussions and have been exemplified by the use of drones, which have become “one of the most highly publicized avatars of high-tech surveillance in the networked era.”[4] Less considered but equally important to modern conflicts are the increasing relevance of algorithms in making sense of the mass quantities of data collected by drones in the field. In

[1] Bob Work, “The third US offset strategy and its implications for partners and allies,” *DoD, Washington* (January 2015).

[2] Mary Kaldor, *New and old wars: Organised violence in a global era* (John Wiley & Sons, 2013).

[3] Derek Gregory, "The everywhere war," *The Geographical Journal* 177, no. 3 (2011).

[4] Mark Andrejevic and Kelly Gates, "Big data surveillance: Introduction," *Surveillance & Society* 12, no. 2 (2014): p. 85.

sum, remote drone operations and algorithmic analysis have contributed to new ways of 'doing war,' especially as US defence and security departments view the need for information and technological superiority as insatiable and 'never ending.'

Both mainstream and critical analysis have been limited in how they understand drones and algorithms. For instance, the use of algorithms is under-theorized relative to the recent surge of literature on drones despite the increasing importance of algorithms to drone operations. This under-theorization is partly due to the technical complexity of algorithms as well as because of their often covert and proprietary nature in both military and commercial technologies. When discussed in terms of security, algorithms have typically been framed in relation to the growing ethical and legal discussion concerning the use of autonomous weapons systems.[5] In comparison, drone warfare has received a great deal of critical attention. This attention has covered a range of subjects, including challenges to its technical and instrumental view; analyzing their role in targeted assassinations; the racialized and feminized aspects of drone violence through the construction of 'Otherness;' the effects of operating drones on drone operators themselves; and lastly their role in effecting new forms of bio-political governance around the globe.[6]

While these critical interventions have made important contributions to theorizing the role of drones in modern conflict settings, these accounts have remained narrowly focused. This paper's key question is: what does the emphasis on algorithmic forms of security imply for the reconfiguration of warfare and societies more widely within current US security rhetoric?

This paper argues that drone and algorithmic warfare are an expression of and an indivisible tool for the 'never-ending' war that is now propelling US security rhetoric. Recent security strategy discourse implies a trend towards the complete mobilization of

[5] For example, see Peter Asaro, "On banning autonomous weapon systems: human rights, automation, and the dehumanization of lethal decision-making," *International Review of the Red Cross* 94, no. 886 (2012); Michael Carl Haas and Sophie-Charlotte Fischer, "The evolution of targeted killing practices: Autonomous weapons, future conflict, and the international order," *Contemporary Security Policy* 38, no. 2 (2017); Benjamin Kastan, "Autonomous Weapons Systems: A Coming Legal Singularity," *U. Ill. JL Tech. & Pol'y* (2013); Armin Krishnan, *Killer robots: legality and ethicality of autonomous weapons* (Routledge 2016).

[6] Mark Duffield, "The digital development-security nexus: Linking cyber-humanitarianism and drone Warfare," in *Handbook of International Security and Development,* ed. Paul Jackson (Cheltenham, Northampton: Edward Elgar Publishing, 2015), pp. 80-94; Katharine Hall Kindervater, "The emergence of lethal surveillance: Watching and killing in the history of drone technology," *Security Dialogue*, *47*, no. 3 (2016).

society in a new type of war, an *algorithmic total war*. As mentioned, both mainstream and critical accounts of modern warfare with respect to the use of drones and algorithms remain limited. Mainstream accounts of drones and algorithms typically focus on the instrumental-technical aspects of their use whereas critical accounts often discuss their legal-normative implications and the construction of certain people as 'threats' within new regimes of surveillance and violence. Further, these limitations are compounded by the fact that that both mainstream and critical analyses retain a preoccupation with a post-9/11 framework that understands power confrontations as a thing of the past whereas new conflicts are contoured by intra-state breakdown, asymmetry and terrorism. In sum, the use of drones and algorithms are rarely considered in a holistic manner and even less so with respect to the evolving rhetoric of US security policy, which once again positions long-term power rivalries as the key imperative shaping American interests.

This paper offers a sketch of the broader concerns animated by these changes. Given the significance and further implications of these concerns, this endeavour is important as algorithmic and drone warfare are part of a much larger set of practices that encompass but are not limited to the focus on surveillance and targeted killings. This paper draws from a wide range of literatures that heretofore have remained relatively independent of one another, but together form a more coherent picture of the historical and theoretical underpinnings of algorithmic and drone warfare. This paper begins with a brief review of the conceptual notion of 'old' and 'new' wars followed by bridging this literature with a discussion on the emergence of networks as an organizational and technical rationale in what has been variously termed as 'netwar,' 'network warfare,' 'liquid war' and 'chaoplexic war.' The role of networks is considered within the framework of liberal peacebuilding and the use of bio-political governance as an expression of this technical rationale. Lastly, this essay reviews and analyzes recent documents from the United States Department of Defense along with secondary sources in order to offer an entry point to an original discussion on the wider implications of an extended reliance on drone and algorithmic warfare in the context of a rapidly changing security policy rhetoric.

'Old' and 'New' Wars

There are two critical inflection points in recent history that receive the bulk of attention in terms of their historical role in dividing 'old' conflicts from 'new' conflicts. The end of the Cold War was famously argued to represent nothing short of the end of history, an ideological and political triumph of liberal democratic capitalism over its competitors, representing victory for the United States and its allies.[7] Roughly a decade later, the events of September 11, 2001 represented for many the limits to American idealism and its commitment to the expansion of liberal cosmopolitanism. For Michael Ignatieff, September 11th "was an awakening, a moment of reckoning with the extent of American power and the avenging hatred it arouses."[8] On the defence front, Donald Rumsfeld argued that September 11 signalled a need for new ways of thinking, training and fighting in order to "prepare for a new type of war."[9] In terms of political economy, Mark Duffield has described the 'hatred' aroused by American imperialism as reflecting for some the tensions between the global north and south.[10] These tensions emerged from a growing sense that the global capitalist system increasingly functioned on a principle of exclusion rather than expanding inclusivism. This exclusion could be argued to fuel the disillusionment with free-markets by a significant proportion of the world's population, thus associated with the expansion of a modern American empire.[11]

Along this theme, Mary Kaldor's often cited work considers 'old' and 'new' wars within a framework that understands 'old wars' as competitions between nation-states over defining modernization and 'new' wars as agitations against liberal universalism. Modern conflicts, in Kaldor's words are "wars in which those who represent particularistic identity politics cooperate in suppressing the values of civility and multiculturalism." Put otherwise, new wars are "wars between exclusivism and cosmopolitanism."[12] Western involvement in the global south is typically framed as a technical exercise. For instance, Kaldor understands the failures of Western intervention to contain the outbreak of conflict in the global South as resulting from top-down practices inherited from 'old wars,' which are antiquated and ineffective. In institutional terms, Anna Leander has argued, following the work of Charles Tilly, that unlike traditional state-making processes that tended towards increased centralization (of power, authority, resources, and especially violence),

[7] Francis Fukuyama, *The end of history and the last man* (New York: Free Press, a division of Simon and Schuster, 2006).

[8] Michael Ignatieff, "The American empire," *New York Times Magazine* 5 (2003).

[9] Donald H Rumsfeld, "Transforming the military," *Foreign Affairs* (2002).

[10] Mark Duffield, *Global governance and the new wars: the merging of development and security* (London and New York: Zed Books Ltd., 2014), p. 4.

[11] Ibid., p. 4

[12] Kaldor, *New and Old Wars*, pp. 10-11.

rulers now “increasingly seem to broker between and bargain with armed forces and local strong men with various degrees of independence.”[13] Kaldor’s notion that old wars were about defining the path towards modernization can be linked to Tilly’s argument that war-making and state-making were effectively a positive relationship.[14] Within this framework, the proliferation of actors jockeying for resources and power outside of states and their institutions has essentially inversed the relationship between war-making and state-making. The consequent effect has been the proliferation of actors in new wars, which undermine the centralization of state authority and power in conflict zones.

Modern conflict is marked by greater chaos and disorder without clear boundaries precisely because the centralization of the state and its monopoly on the use of violence is undermined, creating asymmetric and persistently unstable conflicts. However, recent policy work has challenged the notion that these types of intra-state and asymmetric conflicts are somehow ‘new.’ Gorka argues that the irregularity which characterizes ‘new wars’ actually represents the historical norm rather than conventional warfare between two or more states.[15] Using quantitative data from the *Correlates of War* Project at Pennsylvania State University, Gorka argues that “[w]ar is most often messy and nasty, without easily identified front lines.”[16] This work points to the limitations of the old/new binary when analyzing forms of conflict both historically and currently. While the old/new distinction may have captured the spirit of conflicts in the post-Cold War and post-September 11 environment, almost two decades have passed since then. Like the breakdown of war-time and peace-time under the conditions of a ‘permanent’ and ‘everywhere’ war, the ‘old’ versus ‘new’ distinction no longer captures the global security dynamics unfolding.

[13] Anna Leander, "Wars and the un-making of states: taking Tilly seriously in the contemporary world," In *Contemporary security analysis and Copenhagen peace research,* ed. Stefano Guzzini and Dietrich Jung (New York: Routledge, 2004), p. 74.

[14] Charles Tilly, “War making and state making as organized crime” in ed. Catherine Bestemen, *Violence: A reader* (New York: NYU Press, 1985), pp. 35-60.

[15] Sebastien Gorka, “Adapting to Today’s Battlefield: The Islamic State and Irregular War as the “New Normal” in eds. Hilary Matfess and Michael Miklaucic, *Beyond Convergence: World Without Order* (Washington: Centre for Complex Operations, Institute for National Strategic Studies, 2016), pp. 353-368.

[16] Ibid., p. 354.

The Rise of Networks

While Kaldor and others spoke of changes in the character of modern conflict and its relationship to state-building, the complexities and asymmetries encountered in these conflicts have been advanced theoretically through the concept of networks. Manuel Castells' widely cited treatment concerning the rise of 'network society' proved influential to the social sciences during the 1990s, no less so than in analyzing the emerging character of modern conflict and security.[17] What came to be variously termed as 'network war,' 'netwar' or 'liquid warfare' appeared to define a great deal of the security issues unfolding in the global sphere.[18] Duffield, for example traces the emergence of 'network war' to the Cold War, but one that has been amplified by the particular movement and uncontested dominance of Western capitalism across the globe. Duffield argues that "like the Cold War before it, network war now defines the global predicament. Across this contested landscape, resistance and organized violence engage equally singular systems of international regulation, humanitarian intervention and social reconstruction."[19]

Network war emerged as a consequence of the breakdown in the Cold War order, specifically through the growth of organized networks of non-state actors (including terrorists) that were at one time sponsored by the United States, the USSR and their satellite states. Similar to Leander's argument, Duffield argues that in practice, the post-Cold War environment created an institutional power vacuum, which enabled these previously state-sponsored groups to become self-sufficient and challenge the state-authority that once gave them support.[20]

With respect to technology, Bousquet has discussed the historical co-evolution of military technologies, where the role of networks represented a particular rationality that grew out of the emergence of cybernetics during World War II.[21] Military technologies and rationalities are marked by scientific transformations, from industrial mechanization

[17]Manuel Castells. *The rise of the network society*. Vol. 12 (New York: John Wiley & Sons, 2011).

[18] Pepe Escobar, *Globalistan: How the globalized world is dissolving into liquid war* (Nimble Books LLC, 2006); John Arquilla and David Ronfeldt, *Networks and netwars: The future of terror, crime, and militancy* (Rand Corporation, 2001).

[19] Mark Duffield, "War as a network enterprise: the new security terrain and its implications," *Cultural Values* 6, no. 1-2 (2002): p. 153.

[20] Ibid., p. 157.

[21] Antoine Bousquet. "Chaoplexic warfare or the future of military organization," *International Affairs* 84, no. 5 (2008).

enabled by Newtonian laws of motion, to the role of energy in thermodynamics and atomic weapons. Elsewhere, Bourne critiques the notion that technology itself drives changes in the international system.[22] Network warfare within mainstream realist analysis is not a change in the actual structure of world order (which remains static) but the result of a redistribution of capabilities in that structure. Network warfare has grown because small non-state groups can now mount a legitimate challenge to state authority by virtue of that redistribution. In the field of arms control, this had lead Bourne to critically label the field the "hardware dimension of realism."[23]

James der Derian offers one of the earliest critical interventions of how technology has enabled the creation of 'surveillance regimes,' where "speed as the essence of modern warfare has radically changed the image of battle."[24] Despite the changes enabled by technology and a specific militarized software enabled-rationality that supports their creation,[25] the creation of networks within the so called 'Revolution in Military Affairs' (RMA) is not altogether new. Militarized technological innovation has long desired to overcome the limitations imposed by space and time. As der Derian highlights, "the telephone in the First World War provided generals with the means and the arrogance to send hundreds of thousands of soldiers to their deaths from the relative safety of their chateau headquarters."[26]

In more recent memory, the RMA was discursively adopted by the United States as network technologies became more widespread in the 1990s and early-2000s. The United States' faith in technological superiority was deployed in the Kosovo and Gulf War campaigns where it indeed demonstrated enormous relative power in terms of conventional advantage.[27] However, both technological limits and the incongruence between technology and organizational capacity have been recognized as contributing to

[22] Mike Bourne, "Guns don't kill people, cyborgs do: a Latourian provocation for transformatory arms control and disarmament," *Global Change, Peace & Security* 24, no. 1 (2012).

[23] Ibid., p. 142.

[24] James Der Derian, "The (s) pace of international relations: Simulation, surveillance, and speed," In *Critical Practices in International Theory* (Routledge, 2009), p. 298.

[25] Antoine Bousquet, "A Revolution of Military Affairs? Changing technologies and changing practices of warfare," in ed. Daniel R. McCarthy, *Technology and World Politics: An Introduction* (New York: Routledge, 2018).

[26] James Der Derian, "Virtuous war/virtual theory," *International affairs* 76, no. 4 (2000): pp. 771-772.

[27] Steve Niva, "Disappearing violence: JSOC and the Pentagon's new cartography of networked warfare," *Security Dialogue* 44, no. 3 (2013).

the difficulties for the US military in more recent conflict environments. For all of the discursive hype lobbied around the RMA by Rumsfeld and others, Gregory highlights the underwhelming technologies that were being used in practice. Gregory states that "one reporter discovered that the image of techno-supremacy was replaced by 'an unsung corps of geeks improvising as they went"' and that this reporter "never heard anyone mention the RMA."[28]

Organizationally, the US military apparatus recognized the challenges associated with the growth of non-state actors and the security risks they created. The outgrowth of a network rationality from cybernetics represents an organizational form that appreciates the infinite complexity of social and material life and finds order in that complexity, what Bousquet terms 'chaoplexic warfare.'[29] Consequently, technology is only one aspect of network capabilities. In order to take advantage of advances in networked technology, chaoplexic warfare suggests that organizations themselves must become networked. Indeed, after the discursive ascendance of networks was challenged in actual field operations, the place of networks and its terminology was largely dropped from official rhetoric by the latter half of the 2000s.[30] However, the US military did not abandon the organizational goal of becoming strategically flexible and dynamic. Steve Niva has demonstrated the organizational changes within the US Joint Special Operations Command (JSOC) and argues that the JSOC has evolved into an elite strike force and 'organizational hub' with a largely autonomous and networked command structure.[31] The organizational purpose of US military strategy likewise evolved to encompass more horizontal and vertical flexibility in its command structure as well as increased velocity in decision-cycles and strike capabilities.

While technological innovation is undoubtedly important, Bousquet argues that privileging the role of technology as a key causal mechanism for both military and social transformation is misplaced because the role of technology can only be properly appreciated in relation to the particular social relations in which these technologies are based.[32] Likewise, Haas and Fischer also emphasise the importance of the socio-cultural context in which a technology is inserted because the "the ways in which force is preferably

[28] Derek Gregory, "Seeing red: Baghdad and the event-ful city," *Political Geography* 29, no. 5 (2010): p. 267.

[29] Bousquet, "A Revolution of Military Affairs?"

[30] Bousquet, "A Revolution of Military Affairs?" p. 176.

[31] Niva, "Disappearing violence."

[32] Bousquet, "A Revolution of Military Affairs?"

used tend to be ‘culturally regular.’”[33] Put simply, technology is not a “black box” of the war machine, a view that understands technology as instrumental and a neutral tool, which is “subservient to values established in other spheres i.e. politics and culture.”[34] Consequently, the use of some weapons and not others reinforces the distinction between civilized and legitimate violence against barbaric and illegitimate violence, often within Orientalist hierarchies.

The construction of legitimate and illegitimate violence is predicated on the Westphalian assumption that states, or more specifically *liberal-democratic* states, are the sole arbiters of legitimate violence. This paper advances to consider the liberal character of peace building endeavours and highlight the transition to a remote or distant form of liberal interventionism.

Liberal Interventionism and Bio-political Governance

Understanding technology as more than a neutral tool that is exogenous to political and social life has been an important site of intervention for critical theory, especially in understanding how technology interacts with social and political existence to obscure and perpetrate violence. The conceptual, theoretical and discursive underpinnings of the liberal peace have been advanced and critiqued on a number of fronts. For example, these works have focused on the adherence of research to quantitative ‘large-N’ statistical testing where the liberal peace is treated as a scientific phenomenon;[35] the role of liberal peace as a ‘tripartite international discursive environment’ in which superficial technical solutions to resolve conflict are produced;[36] the ‘punitive ethos’ inherent to liberalism’s normative influence on counter-terrorism policy;[37] the limits to liberalism’s understanding of actors in

[33] Michael Carl Haas and Sophie-Charlotte Fischer, "The evolution of targeted killing practices: Autonomous weapons, future conflict, and the international order," *Contemporary Security Policy* 38, no. 2 (2017): p. 290.

[34] Bourne, “Guns don’t kill people,” p. 142.

[35] Jarrod Hayes, "The democratic peace and the new evolution of an old idea," *European Journal of International Relations* 18, no. 4 (2012).

[36] John Heathershaw, "Unpacking the liberal peace: The dividing and merging of peacebuilding discourses," *Millennium* 36, no. 3 (2008).

[37] Anthony F. Lang Jr., "Punishment and peace: Critical reflections on countering terrorism," *Millennium* 36, no. 3 (2008).

terms of states and their institutions;[38] the inherent violence of Western modernization and its links to liberal peacebuilding;[39] and lastly the liberal character of empire building through imperial expansion.[40]

This body of literature has teased out the implicit and explicit forms of violence that underpin liberal internationalism. Violence undertaken in the name of spreading liberal democracy has increasingly been exposed and difficult to ignore, especially as war has expanded through visual representations and made available to people outside of conflict zones.[41] James Der Derian has gone so far to argue that with respect to a global liberal project of civilizing the world, "in spite of, and perhaps soon because of, efforts to spread a democratic peace through globalization and humanitarian intervention, war is ascending to an even higher plan, from the virtual to the *virtuous*."[42] Commenting on the discursive narrative that technology enabled distance has allowed for a peaceful or 'clean' type of war, Der Derian goes on to argue that "at the heat of virtuous war is the technical capability and ethical imperative to threaten and, if necessary actualize violence from a distance – with no or minimal casualties" and that "on the surface, virtuous war cleans up the political discourse as well as the battlefield [...] virtuous wars promote a vision of bloodless, humanitarian, hygienic wars."[43]

The notion that liberal war has somehow become surgical and bloodless is linked to what a number of authors have identified as a shift from *government* to *governance*. Rather than 'boots on the ground' and active attempts at state building, liberal interventionism has shifted to emphasize the management of and engagement with populations at a distance. Again, this should not be understood as an altogether new phenomenon. Heathershaw argues that liberal peacebuilding, while theoretically linked to Kant's notion of a perpetual peace, is more recently linked to discourse that proliferated at the end of the Cold War.[44] Democratic peacebuilding was developed by the United Nations (UN) along with its major donors and analysists in the immediate post-Cold War period, which was understood as a

[38] Roger Mac Ginty, "Warlords and the liberal peace: state-building in Afghanistan," *Conflict, Security & Development* 10, no. 4 (2010).

[39] Jörg Meyer, "The concealed violence of modern peace (-making)," *Millennium* 36, no. 3 (2008).

[40] Simon Dalby, "Political space: autonomy, liberalism, and empire," *Alternatives* 30, no. 4 (2005); Ann Laura Stoler, "On degrees of imperial sovereignty," *Public Culture* 18, no. 1 (2006).

[41] Paul Virilio. *The vision machine*, (Indiana University Press, 1994).

[42] Der Derian, "Virtuous war/virtual theory," 772, original emphasis.

[43] Ibid., p. 772.

[44] Heathershaw, "Unpacking the liberal peace."

"watershed moment akin to 1919 or 1945", thus spawning the 'new interventionism' that dominated policy rhetoric during the 1990s and early-2000s.[45]

However, along with this discourse there has been a pronounced shift in practice towards increasing forms of bio-political governance in the Foucaultian sense of the term. For Dillon and Reid, "global liberal governance is substantially comprised of techniques that examine the detailed properties and dynamics of populations so that they can be better managed with respect to their many needs and life chances" and where "biopolitics is the pursuit of war by other means."[46] Foucault has made a lasting contribution to the critique of liberal security and war, which becomes especially useful in theorizing current conflict environments. For Evans, life itself becomes the object of political strategies, which holds implications in terms of security.[47] Echoing Dillon and Reid, Evans states that "in the process of making life live, [those general strategies for effecting power] entail the regulation of populations for society's overall betterment."[48]

The notion of 'bettering' society is implicated in the idea that freedom must be produced in a very particular manner linked to distant governance.[49] The idea that freedom is an actively created condition for life can be related to the work of Mark Duffield, who has offered one of the most comprehensive critiques on liberal interventionism over a number of years. Duffield has demonstrated and analyzed the merging of security, development and humanitarian discourses, all of which are increasingly underpinned by the same logic of 'governance at a distance' enabled by network technologies. In particular, security and humanitarianism has taken an explicitly *neoliberal* turn as disaster affected populations are now expected to self-manage. Duffield explains that the merging of security and humanitarianism within a neoliberal framework has led to the notion of 'resilience,' which "focuses on narcissistic and subjective forms of care-of-the-self."[50] Duffield argues that remote technologies for surveillance and bio-political management are part of the neoliberal

[45] Ibid., pp. 600-601.

[46] Michael Dillon and Julian Reid, "Global liberal governance: biopolitics, security and war," *Millennium* 30, no. 1 (2001): pp. 41-42.

[47] Brad Evans, "Foucault's legacy: Security, war and violence in the 21st century," *Security Dialogue* 41, no. 4 (2010): p. 416.

[48] Ibid., p. 416.

[49] Ibid., p. 418.

[50] Mark Duffield, "Disaster-resilience in the network age access-denial and the rise of cyber-humanitarianism," No. 2013: 23 (DIIS Working Paper, 2013).

shift in political economy more widely.[51] Within this paradigm shift, affected populations are to be "made free" and to "embrace risk and thereby develop foresight and enterprise."[52] Again, the idea of being 'made free' emphasizes the liberal interventionist role of producing freedom, but not in terms of emancipatory conditions circumscribed by a positive commitment to liberty in the philosophical sense, but rather through a contradictory and explicitly negative form of liberty within an absence of formal constraints. A positive form of liberty would imply the need for various forms of material and resource commitment (money, time, people, expertise, etc.), whereas negative liberty simply assumes an ideological and structural commitment to removing obvious obstacles or barriers to expressing one's freedom. People are *made* free via the removal of institutional, cultural and other social restrictions (including social protections), thus enabling their own volition.[53] For Duffield, "resilience embodies a new biopolitics that differs from the actuarial and protective biopolitics [...] that underpins the great modernist project of Welfare Fordism."[54]

This distancing of humanitarianism, development and security should not obscure the violence perpetuated in their name. Just as security begins to appear as an 'everywhere' and 'permanent' war, populations are abandoned to a state of "permanent emergency."[55] These populations are the same groups that are made the objects of securing against, where "liberalism proceeds on the basis that 'Others' are the problem to be solved."[56] The remote management of populations through techniques of biopolitical governance is accomplished with the underlying rationality of risk aversion, which is argued to be intensified by the repeated difficulties encountered by allied Western forces in recent campaigns. There is an explicit relationship between the failures of these campaigns and the growth of remoteness as an ordering logic for state intervention, leading Duffield to argue that ground or "terrestrial" forms of "liberal interventionism now [lie] burie[d] in the ruins of Iraq, Libya and Syria."[57]

This paper now shifts to examining the role of drones as a recent iteration of and tool for remote operations within the peace building endeavours of liberal expansionism while

[51] Mark Duffield, "The resilience of the ruins: towards a critique of digital humanitarianism," *Resilience* 4, no. 3 (2016).
[52] Duffield, "Disaster-resilience," p. 9.
[53] Ibid., p. 10.
[54] Ibid.
[55] Ibid., p. 23.
[56] Evans, "Foucault's legacy," p. 420.
[57] Duffield, "The resilience of the ruins," p. 148.

considering how drones have been framed in relation to the transformation of conflict and societies more generally.

The Rise of Drones

Drones have received a bulk of the attention directed at modern conflicts and governance strategies. The notion of risk-avoidance persists as a theme at the heart of drone warfare, especially as drone-led missions were increased under the Obama administration. While the increase in risk aversive strategies is argued to be the result of costly failures throughout the post-9/11 military campaigns, the understanding of drones as a reactionary technology has been challenged.[58] Rather, Holmqvist argues that "the 'population-centric' counterinsurgency warfare that evolved in Iraq and Afghanistan around 2005-7 was from the outset accompanied by reliance on secret operations featuring military robotics designed to target key individuals for capture or death."[59] Extending this critique further, Kindervater examines drones within the practice of 'lethal surveillance' and historicizes their use in relation to the growth of air power during the World Wars and the Cold War.[60] "Lethal surveillance" is first the convergence between "the increasing importance of intelligence, surveillance, and reconnaissance (ISR) and [second], the development of dynamic targeting."[61] Historically, the role of air power in creating fear became a notable tactic in pacifying populations, where long-range bombings were seen as "terrifying and unstoppable."[62] As such, drones should not be thought of as simply a reactionary and new form of intervention, but the latest configuration of a much longer historical process that has occurred simultaneously with more traditional labour-intensive military campaigns.

In general, drones can be critically thought of within the wider historical fixation on technological solutions to war making and where "technology is seen as the means by which the United States and its allies can continue to exert military influence globally while avoiding both the human casualties and compulsory enlistments such a policy might

[58] Caroline Holmqvist, "Undoing war: War ontologies and the materiality of drone warfare," *Millennium* 41, no. 3 (2013): p. 537.

[59] Ibid., p. 541.

[60] Katharine Hall Kindervater, "The emergence of lethal surveillance: Watching and killing in the history of drone technology," *Security Dialogue* 47, no. 3 (2016).

[61] Ibid., p. 224.

[62] Ibid., p. 226.

otherwise entail."[63] The discursive logic of drones can be better understood as they are positioned as a precise, discriminate and therefore 'humane' instrument of security through their use in the pursuit of 'civilizing warfare.'[64] The expansion of drone operations under the Obama administration represents a continuation of a trend towards covert and distant forms of intervention while also representing a rhetorical shift in security discourse. Within the framework of liberal internationalism, drone usage has been justified by the purported inability or unwillingness of some states to maintain their territorial integrity and border security. These areas (such as North Africa and Pakistan's FATA region) become produced as "spaces of exception" that are removed from political recourse.[65] While sovereignty is understood to be the legal and normative standard of the Westphalian state system, sovereignty in practice is undermined by network technologies and the weapons derived from them. The 'unbordering' of sovereignty via globalization and communications technology is a well-worn argument. However, the use of armed drones reflects a particular unbounding of the constraints supposedly imposed by sovereignty.[66] The legal and ethical imperative for drone strikes in otherwise sovereign states is rhetorically made through the inability or unwillingness of those states to uphold their responsibility to protecting the integrity of the international order. This rationality can be understood as part of the wider notion that the liberal peace is increasingly something that needs to be created or produced, which "becomes an obligation – indeed a prerogative – of the (Western) self as the sole agent of order."[67] Kindervater has likewise argued that "territory is mobilized [...] to legally justify the use of force and the reach of US sovereign power."[68] Recalling the themes of 'permanent' and 'everywhere' war, Kindervater highlights the place of 'imminence' in eliciting the normative and legal rationalities necessary for drone assaults. Within the framework of imminence, security threats are not understood as a "'ticking time bomb' scenario, but rather signalled by participation in a terrorist group that is continuously planning attacks."[69] Consequently, a great deal of critical work has gone into examining the

[63] Bousquet, "A Revolution of Military Affairs?" p. 177.

[64] Bourne, "Guns don't kill people."

[65] Ronald Shaw, Ian Graham and Majed Akhter, "The unbearable humanness of drone warfare in FATA, Pakistan," *Antipode* 44, no. 4 (2012): p. 1505.

[66] Christine Agius, "Ordering without bordering: drones, the unbordering of late modern warfare and ontological insecurity," *Postcolonial Studies* 20, no. 3 (2017): p. 370.

[67] Meyer, "The concealed violence of modern peace (-making)," p. 555.

[68] Katharine Hall Kindervater, "Drone strikes, ephemeral sovereignty, and changing conceptions of territory," *Territory, Politics, Governance* 5, no. 2 (2017): p. 208.

[69] Ibid., p. 211

perceived legality of drone strikes and by extension the use of targeted assassinations in extra-judicial spaces.[70] This focus has in turn been critiqued as further obscuring the violence committed by drone strikes because the emphasis on a legalistic lens implicitly suggests that an ethical drone program is possible when conditioned by international legal norms, which have arguably never effectively circumvented war-making endeavours in the first place.[71]

The theme of violence, widely analyzed in the critical literature on democratic peace and liberal governance, is reproduced in work that draws attention to and problematizes the notion that drones are somehow neutral avatars of liberal security. In particular, the inconsistencies between drone violence and the rhetorical principles of liberal peace are made apparent.[72] Again, drones are not an aberration of liberal peace but understood to reflect an underlying rationality of violence inherent to liberal interventionism itself. According to Agius, what she terms 'vertical Orientalism' reflects the growing awareness that while drone strikes have been portrayed as precise and humane tools of security, in practice they have created deep *insecurity* for specific groups of people.[73] This insecurity is created and normalized through the omnipresence of drones in post-colonial spaces and the practices of surveillance along with the constant threat of missile strikes. Drones have inflicted brutal violence on civilian populations in the FATA region of Pakistan, the Middle-East and North Africa, and have been termed in this respect 'necropolitical.'[74] In part, the actual structure and interface of drone operations itself aids in the construction of 'Otherness'. While drone operations are portrayed through a risk aversive lens in that drone operators are working in dangerous zones of conflict comfortably from domestic soil, this distance has a significant consequence. Drone operators, as Asaro explains, can only

[70] For example, see Gabriella Blum and Philip Heymann, "Law and policy of targeted killing," *Harv. Nat'l Sec. J. 1* (2010); Megan Braun and Daniel R. Brunstetter, "Rethinking the criterion for assessing CIA-targeted killings: Drones, proportionality and jus ad vim," *Journal of Military Ethics* 12, no. 4 (2013); Martin S. Flaherty, "The constitution follows the drone: Targeted killings, legal constraints, and judicial safeguards," *Harv. JL & Pub. Pol'y* 38 (2015); Gregory S McNeal, "Targeted killing and accountability," *Geo. lj* 102 (2013); Ruth Blakeley, "Drones, state terrorism and international law," *Critical Studies on Terrorism* (2018).

[71] Marina Espinoza & Afxentis Afxentiou, "Editors' introduction: drones and state terrorism," *Critical Studies on Terrorism,* vol. 11, no. 2 (2018).

[72] Agius, "Ordering without bordering."

[73] Ibid.

[74] Ibid.; see Tyler Wall, "Ordinary emergency: Drones, police, and geographies of legal terror," *Antipode* 48, no. 4 (2016).

make limited choices with respect to how they interact with other actors in the field because of their remoteness.[75] While human interactions allow for a multitude of nuanced decisions and options, the "limit to fidelity" encountered through drone mediation and remote surveillance reduces that interaction to a simple and troubling binary: kill or not kill.[76] The damaging effects of this violence on drone operators themselves has also been well documented, which challenges a conventional notion that drone operations can be reduced to the experience of video games.[77]

There is, consequently, a 'humanness' to drone warfare that is often overlooked.[78] Using Marx's theory of commodity fetishism, Shaw, Graham and Akhter point to the way drones are often portrayed as simply objects while their use is reflected as a relationship between *things* rather than between people. Like commodities, there is a corporeality inherent to drones that is, to borrow from Marx, 'mystified' and 'masked' especially as drones are typically portrayed in terms of technical language.[79] Likewise, Kindervater has demonstrated that mainstream accounts of drones often obscure the "human experience of war."[80]

Within this theoretical lens, drones are part of a longer historical context that is rooted in colonial management, where the liberal-technological state represents a continuation of this historical lineage.[81] State-led terror has become, according to these authors, a 'non-event' as it is concealed by the practices and discourses born out of the liberal-technical state.[82] Increasingly, these practices are shared between the national and international context.[83] Wall argues that what is often understood as explicitly military and therefore extraordinary forms of power in the international sphere can actually be

[75] Peter M. Asaro, "The labor of surveillance and bureaucratized killing: new subjectivities of military drone operators," *Social semiotics* 23, no. 2 (2013).

[76] Ibid., p. 221.

[77] Ibid.; see M. Bentley, "Fetishised data: Counterterrorism, drone warfare and pilot testimony," *Critical Studies on Terrorism*, 11, no. 1 (2018).

[78] Shaw, Graham, and Akhter, "The unbearable humanness of drone warfare in FATA, Pakistan."

[79] Ibid., p. 1501.

[80] Kindervater, "Drone strikes," p. 211.

[81] S. Rupka & B. Baggiarini, "The (non) event of state terror: drones and divine violence," *Critical Studies on Terrorism,* vol. 11, no. 2 (2018).

[82] Ibid.

[83] Wall, "Ordinary emergency"; see Mark Neocleous, "Air power as police power," *Environment and Planning D: Society and Space* 31, no. 4 (2013); Mark Neocleous, *War power, police power* (Edinburgh University Press, 2014).

understood with reference to ordinary policing practices in the domestic context.[84] Shaw has considered this blurring of the national/international through the increasing use of drones across these spaces within the framework of American empire.[85] According to Shaw, "we are witnessing a transition from a labour intensive American empire to [...] a machine – or capital-intensive Predator Empire" that produces contradictions which must be "violently policed."[86]

In sum, drones, while not altogether new from the historical standpoint of colonial imperialism, are indeed aiding in the transformation of battlefields from discreet spatial entities to borderless environments, ultimately collapsing the world into a single battlespace. [87] This discussion now considers the correlate but less discussed role of algorithms and machine intelligence in modern warfare and the underlying rationalities they signal.

Algorithmic Warfare

The role of algorithms in conflict has only recently begun to be theorized and, when they are considered, they are only peripherally related to the role of drones. In part, this is because algorithms have only been emphasized in public communications by defence and security agencies over the last several years. The first notable use of algorithms in warfare came through the deployment of 'Stuxnet,' a malicious computer worm that formed part of the 'Olympic Games' covert assault carried out by the United States and Israel against Iranian Nuclear capability.[88] Stuxnet's effects were such that they caused physical systems to degrade and experience actual destruction.[89] In April of 2017, the US Department of Defense (DoD) released a memorandum concerning the establishment of their 'Algorithmic Warfare Cross-Functional Team' (AWCFT) codenamed 'Project Maven.'[90] The purpose of Project Maven is to "accelerate DoD's integration of big data and machine learning" where

[84] Wall, "Ordinary emergency."

[85] Ian G.R. Shaw, "Predator empire: The geopolitics of US drone warfare," *Geopolitics* 18, no. 3 (2013).

[86] Ibid., pp. 5-6.

[87] Ibid.

[88] Jason Healey, "Stuxnet and the Dawn of Algorithmic Warfare," *Huffington Post* (16 June 2013).

[89] Ibid.

[90] Deputy Secretary of Defense, "Establishment of an Algorithmic Warfare Cross-Functional Team (Project Maven)," *Department of Defense Memorandum* (26 April 2017).

its objective "is to tum the enormous volume of data available to DoD into actionable intelligence and insights at speed."[91] The initial mission of this warfare cell is to automate the process of visual analysis of video feeds captured by drones in Iraq and Syria.[92] Media for the Department of Defense states that:

> Project Maven focuses on computer vision – an aspect of machine learning and deep learning – that autonomously extracts objects of interest from moving or still imagery [...] Biologically inspired neural networks are used in this process, and deep learning is defined as applying such neutral networks to learning tasks.[93]

According to Marine Corps Col. Drew Cukor, who is chief of the AWCFT, algorithms were set to deploy by the end of 2017 "onto government platforms to extract objects from massive amounts of moving or still imagery."[94] Traditionally, this analysis process has been performed manually by thousands of military and civilian personnel who are simply unable to adequately and effectively comb over mass amounts of video data being rapidly produced from these conflict spaces.

Algorithms are consequently as important to drone warfare as the drones themselves insofar as they are used to analyze the data collected by drones and then produce the targets destined to be on the receiving end of remote strikes.[95] Algorithms are often thought of in conventional discourse as relating to the growth in 'big data,' which has emerged from recent technological innovations in data collection, storage and analytical capabilities, particularly over the last several years, which has seen more data created than ever before in human history.[96] Accordingly, the issue of surveillance has also become linked to the functioning of big data technologies. With respect to drones, while the majority of work has emphasized their use in kill-strikes, Andrejevic and Gates note that

[91] Ibid., see Travis Axtell, "Operational Perspective: Project Maven," in *Challenges in Machine Generation of Analytic Products from Multi-Source Data: Proceedings of a Workshop*, pp. 7-9 (The National Academy Press, 2017).

[92] Marcus Weisgerber, "The Pentagon's New Algorithmic Warface Cell Gets Its First Mission: Hunt ISIS," *Defense One* (May 14, 2017).

[93] Cheryl Pellerin, "Project Maven to Deploy Computer Algorithms to War Zone by Year's End," *DoD News, Defense Media Activity* (21 July 2017).

[94] Ibid.

[95] Jutta Weber, "Keep adding. On kill lists, drone warfare and the politics of databases," *Environment and Planning D: Society and Space* 34, no. 1 (2016).

[96] Bernard Marr, "Big data: 20 mind-boggling facts everyone must read," *Forbes,* 30 September 2015.

military drones are able to capture all available wireless data traffic in a given area through devices called 'Air Handlers,' which are used by the NSA and enable drones to possess a 'double image of surveillance' capabilities.[97] The point of Air Handlers and other data gathering technologies is to collect data on an industrialized scale, represented through the 'three V's' of big data – volume, velocity.[98]

Like the use of drones, algorithms have not emerged from an altogether new form of rationality, but one that is inherited from the rise of cybernetics and the context of the Cold War.[99] However, algorithms do represent both an increasingly "technical process" as well as a "synecdoche for ever more complex and opaque socio-technical assemblages," which "imply new ways of knowing, even as their actual operations are increasingly inaccessible."[100] The post-9/11 security environment, constructed through the framework of counter-terrorism, has provided the context for which algorithmic security has been advanced as a solution to an increasingly complex and asymmetric spectrum of threats.[101] Algorithms, viewed instrumentally, are used as a tool to make sense of the deluge of data being created, which in turn allows for a greater creativity and diversity in security policies. For example, the monitoring and analysis of financial networks have become a major source of data for security agencies tracking the movement of capital used to finance terrorist activity.[102] Within this form of governance, "projections are produced from fragments of data, from isolated elements that are selected, differentiated and reintegrated to give the appearance of a visual whole" and consequently "the purpose of financial link analysis [...] is not to trace the steps and seize the assets of known criminals or terrorists but to visualize networks of association and to identify the 'unknown terrorist.'"[103] Likewise, Hall and Mendel have examined the appropriation of public and consumer data by security agencies, whose objective can be said "to anticipate needles before terrorists or criminals

[97] Andrejevic & Gates, "Big data surveillance."

[98] Ibid.; Sara Esposti, "When big data meets dataveillance: The hidden side of analytics," *Surveillance & Society* 12, no. 2 (2014).

[99] Louise Amoore and Rita Raley, "Securing with algorithms: Knowledge, decision, sovereignty," *Security Dialogue* 48, no. 1 (2017).

[100] Ibid., p. 3.

[101] Ibid., p. 5.

[102] Mara Wesseling, Marieke de Goede, and Louise Amoore, "Data wars beyond surveillance: opening the black box of SWIFT," *Journal of Cultural Economy* 5, no. 1 (2012).

[103] Ibid.,pp. 57-58.

have even thought to place them within the haystack."[104] One white paper has also argued that research should be undertaken in order to understand what is needed for artificial intelligence to counter the radicalization process.[105] Using algorithms as a way to pre-emptively modify radicalized behaviour shares a similar logic to the use of algorithms within commercial technologies, where they are used to shape the behavioural patterns of consumers in order to anticipate and tailor their purchases.

Just as the use of drones in international spaces have been identified as sharing the same underlying rationality as domestic policing practices, the algorithmic management of populations becomes reproduced across national and international spaces. For example, big data is increasingly used by policing agencies, who collect and analyze data from various sources to project possible future outcomes. The algorithmic creation of 'heat lists' in Chicago, which consist of individuals "identified by a risk analysis as most likely to be involved in future violence" is one example.[106] In New York City, the NYPD has created a 'Domain Awareness System' with the help of Microsoft, which collects and organizes data from several sources in order to create and track surveillance targets with detailed information.[107] There are notable similarities between the creation of 'heat lists' by policing agencies and the creation of 'kill lists' in conflict zones. Jutta Weber discusses the role of the 'disposition matrix', which is a key database of kill lists in the US war on terror. As the war on terror often concerns individuals with loose and often fluid associations, algorithms are used to analyze data from increasingly peripheral and broadly defined networks.[108] Overall, big data and algorithmic analysis has specifically enabled a form of biopolitical governance that is directly enacted through a framework of risk, which becomes almost obsessive in managing both present and future threat scenarios.

When viewed in terms of their underlying cybernetic rationality, which serves to enforce a liberal cosmopolitanist form of security across the globe, algorithms are infused with a "generative capacity" in that they serve "to make worlds in and through data" while

[104] Alexandra Hall and Jonathan Mendel, "Threatprints, threads and triggers: imaginaries of risk in the 'war on terror,'" *Journal of Cultural Economy* 5, no. 1 (2012): p. 2.

[105] Gary Kessler, Diane Maye & Aaron Richman, "Artificial Intelligence in Shaping Preferences and Countering the Radicalization Process," *White Paper for the Decadal Survey of the Social and Behavioral Sciences for National Security* (Philadelphia: TAM-C Intelligence, 2017).

[106] Elizabeth E Joh, "Policing by numbers: big data and the Fourth Amendment," *Wash. L. Rev.* 89 (2014): p. 35.

[107] Ibid., p. 35.

[108] Weber, "Keep adding."

creating “new forms of political authority.”[109] Duffield, in his discussion on the merging of security and humanitarian discourses with remote technologies (producing what he calls a ‘cyber-humanitarianism’) has argued that this world-building endeavor increasingly resembles Hanna Arendt’s notion of ‘world alienation.’ [110] For Duffield, our experience of reality and the intersubjective construction of our identities is reduced to a “digital recoupment of the consequent loss of face-to-face contact.” [111] Put otherwise, Arendt’s conception of ‘world alienation’ speaks to the loss of physical interactions and material structures that result from the efforts of our labour and serve as the preconditions for meaningful political action.[112] Digital and distant interactions cannot replace or replicate the materialism that Arendt understood as necessary for creating a better and more inclusive world. Algorithms are part of the same overarching rationality that considers remoteness as both a practical and cost-effective solution to the increasing challenges and risks associated with access to disaster zones and conflict sites. For example, Duffield notes how algorithms were deployed in Darfur in order to address the issue of capturing the changes in Darfur’s camps for its displaced populations. [113] In sum, Duffield argues that algorithms have enabled “a simultaneous digital remapping and reinterpreting of these new cartographic ‘white spaces’ together with an increasing ability, through remote sensing and the algorithmic analysis of metadata, to substitute ground truth with pattern recognition and behavioural analysis among the now hard-to-reach populations.”[114]

The substitution of human interaction, learning, analysis and decision making with algorithmic computation is at the heart of discussions on the ethical issued posed by the use of artificial intelligence in decision making loops. In terms of its technological capacity to transform battle, critical analysis has largely focused on the role of algorithms in the creation and functioning of autonomous weapons.[115] Haas and Fischer argue that machine autonomy is likely to contribute to the normalization and outgrowth of targeted killing practices within the policy applications of counter-terrorism. [116] For Curtis, the use of

[109] Amoore and Raley, “Securing with algorithms,” p. 6.

[110] Duffield, “The digital development-security nexus,” p. 81.

[111] Ibid., 81; Duffield, “The resilience of the ruins,” p. 150.

[112] Johanna Luttrell, “Alienation and global poverty: Arendt on the loss of the world,” Philosophy & Social Criticism 41, no. 9 (2015).

[113] Duffield, “the digital development-security nexus,” p. 85.

[114] Duffield, “The resilience of the ruins,” p. 150.

[115] Haas and Fischer, "The evolution of targeted killing practices.”

[116] Ibid.

algorithms cannot be separated from drone warfare and their principle function, which contrary to popular understandings is not to target specific people but rather their social environments using mass amounts of surveillance information that "renders explicit, and thereby problematic and dangerous, the background communication, movement and sociality that are essential to any human being's existence."[117] Drones create an ontological insecurity for 'Others,' not as a byproduct or externality of its functioning but as a direct result of its design and purpose.

While critical literatures on liberal internationalism, drones and algorithms have been welcome interventions into mainstream and policy accounts of modern conflict, those interventions have been limited in their focus by considering their roles in a static post-Cold War/ post-September 11 environment, which was nearly twenty years ago. Framing algorithmic analysis and drone strikes strictly within the parameters of counter-terrorism and the rubric of liberal-internationalism has serious limitations. An important shortcoming of this framework is that it reproduces the simple and reductionist dichotomy of 'new' and 'old' wars, where the consequences of an increasing cybernetic rationality have focused on the violence and forms of insecurity inflicted by algorithmic surveillance and drone strikes in post-colonial spaces. This focus has come at the expense of analyzing the further blurring of lines between military and civilian spaces as well as the implications for a future understood to be dominated by the *longue durée* of major power competition rather than a pronounced focus on terrorism. This paper now shifts to a broader discussion on recent trends in US security strategy in relation to the perceived changes in the international order, which can be argued to display a return to inter-state power competition.

Drones, Algorithms and Decision-Cycle Dominance in US Security Strategy

The recent *2018 National Defense Strategy of the United States of America* declares that:

> Today, we are emerging from a period of strategic atrophy, aware that our competitive military advantage has been eroding. We are facing increased global disorder, characterized by decline in the long-standing rules-based international order – creating a security environment more complex and volatile than any we have experienced in recent memory. Inter-state strategic

[117] Neil Curtis, "The explication of the social: Algorithms, drones and (counter-) terror," *Journal of Sociology* 52, no. 3 (2016): p. 523.

> competition, not terrorism, is now the primary concern in U.S. national security.[118]

Recent international trends, especially concerning Russia's actions in Ukraine, have undermined the normative basis of the international order and created a "gray zone conflict along its external borders with NATO."[119] Along with the increasing power of China, US defence strategy has shifted to focus its attention and resources on "the re-emergence of long-term, strategic competition between nations."[120] What does the simultaneous emphasis on remote and automatic forms of warfare entail for this strategy? In policy and resource terms, the United States' defensive position has been undermined by its terrestrial interventions over the last two-decades. These interventions have been enormously costly politically as well as in terms of money, resources and lives. Confronted with an increasingly aggressive Russia in Europe and Chinese power in the Indo-Pacific, the United States recognizes how its sprawling interventions have stretched its defensive resource base and undermined effective deterrence. In short, the United States' pursuit of peace and counter-terrorism abroad came at the expense of maintaining its relative advantage to other nation-states.

The 2018 National Defense Strategy states that "today, every domain is contested – air, land, sea, space, and cyberspace."[121] Rather than a straightforward return to inter-state conflict, however, the United States National Defense Strategy states that the "security environment is also affected by *rapid technological advancement and the changing character of war*."[122]

Consequently, the role of technology remains a dominant theme of US security strategy. The United States no longer understands its dominance to be secured by conventional weapons and force advantage alone, but through the expansion of its surveillance and information gathering and analytic capabilities. In this respect, information itself is not the end goal. Instead, the end goal is to "exploit information" and

[118] Department of Defense, *Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge* (2018), p. 1.
[119] Haas and Fischer, "The evolution of targeted killing practices," p. 294.
[120] Department of Defense, *Summary of the 2018 National Defense Strategy*, p. 2.
[121] Ibid., p. 3.
[122] Ibid., p. 3, original emphasis.

to "deny competitors those same advantages [...]."[123] This emphasis on information exploitation represents a continuation of the United States' focus on cyber-capabilities inherited from the Cold War. In particular, Project Maven and algorithmic warfare represents an initial step in the United States' pursuit of dominating cyber-space, which in turn can translate the projection of force to all other domains. A presentation by Lieutenant General Jack Shanhan, OUSDI Director for Defense Intelligence (Warfighter Support) states that "in future fights, [the] best we can achieve [is] likely to be decision cycle advantage, not information dominance or even information superiority."[124] For US security strategy, 'decision cycle advantage' can be argued to translate into the goal of "challeng[ing] competitors by maneuvering them into unfavorable positions, frustrating their efforts, precluding their options while expanding our own, and forcing them to confront conflict under these adverse conditions."[125] Confronted with a reality where technology and information is easily accessible to a number of actors, both state and non-state based, the current US security strategy is to deprive its enemies the ability to use that technology or exploit the mass quantities of information readily produced. Algorithms and drones will undoubtedly represent a significant aspect of this strategy, especially as the United States and other nation-states race to create advanced forms of artificial intelligence (AI) through machine learning and neural-network technologies.

Extending considerations of the critical literature previously discussed, the obvious indicators point to an increased militarization of social life and an expanding theatre of violence through the normalization of autonomous military systems. Indeed, the further integration of and conflicts arising from military and industrial development pose one of the most important areas for further analysis. For its part, the Department of Defense argues that interfacing with private industry will be a critical component of developing comparative advantage in its path towards the development of new intelligence-based systems and the modernization of existing weapons. The 2018 National Defense Strategy states that:

> new commercial technology will change society and, ultimately, the character of war. The fact that many technological developments will come from the commercial sector means that the state competitors and non-state actors will

[123] Ibid., p. 6.

[124] Lt. General Jack Shanahan, "Algorithmic Warfare Cross-Functional Team (AWCFT) aka Project Maven," *Department of Defense of the United States of America* (26 October 2017).

[125] Department of Defense, *Summary of the 2018 National Defense Strategy*, p. 5.

> also have access to them, a fact that risks eroding the conventional overmatch to which our Nation has grown accustomed.[126]

Thus, part of the US national defense strategy is to integrate and exploit commercial technology. This integration represents in some forms a reversal of the historical trend where military technology was transferred to the civilian sphere. In practice, the transfer of commercial technologies to security and military agencies has already begun. In June of 2013, Booz Allen Hamilton (an American consulting firm) employee, Edward Snowden revealed to the world the extensive and secretive nature of modern surveillance programs (e.g. PRISM) by the US National Security Agency (NSA), including the involvement of private corporations such as Verizon.[127] Despite the Snowden leaks, the integration of private corporations with US security agencies and the US military has only become amplified, albeit not without contestation. For example, Project Maven's recent 'Industry Day' represents its drive to "partner with industry, academia and national laboratories to develop and deploy artificial intelligence-based algorithms against some of DoD's toughest challenges."[128] Project Maven itself has recently been challenged in relation to the role played by Google, where the company has reportedly been aiding the US Department of Defense as a subcontractor with developing its artificial intelligence platform to accomplish Project Maven's goal of algorithmically analyzing drone footage.[129] A number of employees at Google were reportedly dismayed by this information, specifically in what Google's Eric Schmidt described as "a general concern in the tech community of somehow the military-industrial complex using their stuff to kill people incorrectly."[130]

The notion that people can be killed 'incorrectly' represents the dominant concern in military appropriation of civilian technologies and replicates the same troubling issue that is identified by post-colonial critiques of drone warfare: that implicitly there is a 'correct' and therefor ethical way to kill people at all. However, even the post-colonial focus on how

[126] Ibid., p. 3.

[127] Susan Landau, "Making sense from Snowden: What's significant in the NSA surveillance revelations," *IEEE Security & Privacy* 11, no. 4 (2013).

[128] Cheryl Pellerin, "Project Maven Industry Day Pursues Artificial Intelligence for DoD Challenges," *DoD News, Defense Media Activity,* 27 October 2017.

[129] Kate Conger and Dell Cameron, "Google is Helping the Pentagon Build AI for Drones," *Gizmodo,* 06 March 2018.

[130] Ibid., see Scott Shane, Cade Metz and Daisuke Wakabayashi, "How a Pentagon Contract Became an Identity Crisis for Google," *The New York Times,* 30 May 2018.

surveillance and kill targets are 'Othered' and the violence encountered through that process is only part of a larger set of issues raised by the focus on algorithmic warfare. Given that security discourse is beginning to re-emphasize the importance of long-term interstate competition and a security strategy predicated on information-decision cycle dominance through algorithmic superiority, the implications posed go beyond the violence of surveillance and killing.

For one, the increasing militarization of everyday life supports the normalization of drones and weapons, which in turn legitimates their use in regimes of violence. This in and of itself is not a departure from the liberal way of war but a strengthening of its underlying rationality – that peace must be secured through force.

Second, while the focus has also been on the role of algorithms in shaping autonomous weapons without the perceived ethics of a human consciousness (which itself is a problematic position), the implications of algorithmic decision making go much farther than autonomous weapons. The most recent security strategy rhetoric, which defines its adversarial advantage in terms of decision-making cycles, shares a similar but amplified form of the game-theoretic rationality that underpinned Cold-War thinking under the rubric of 'mutually assured destruction' (MAD). However, unlike MAD, which theoretically maintained a balance of power (however uncomfortable) between the US and USSR, the new logic of decision cycle advantage has been combined with an equal shift towards a rhetorical need for weapons that exist below the threshold of non-use (whether because of their destructive capability or cost). While the National Defense Strategy states an overall strategy of interaction "below the level of armed conflict,"[131] there is a troubling scenario presented when decision making is theoretically collapsed into the *instantaneous* without humans necessarily 'in the loop.'[132] Combined with a rhetorical stance that has emphasized a need for new weapons and a modernized nuclear arsenal with 'small-yield' warheads, which are argued to introduce a measure of 'limit' and tactical capability within US nuclear deterrence,[133] the expansion and normalization of algorithmic violence seems a likely future for societies across the globe. Dillon and Reid have already alluded to the possibilities encountered in this environment. They argue that:

[131] Department of Defense, *Summary of the 2018 National Defense Strategy*, p. 6.
[132] See Paul Virilio, *Speed and Politics* (Cambridge: MIT Press, 2006).
[133] Paul Sonne, "Pentagon unveils new nuclear weapons strategy, ending Obama-era push to reduce U.S. arsenal," *The Washington Post,* 2 February 2018.

> endless war is underwritten here by a new set of problems [because] these wars no longer benefit from the possibility of scoring outright victory, retreating, or achieving a lasting negotiated peace by means of political compromise. Indeed, deprived of the prospect of defining enmity in advance, war itself becomes just as complex, dynamic, adaptive and radically interconnected as the world of which it is part. That is why 'any such war to end war becomes a war without end [...].[134]

This is not to suggest that the future looks like the totalitarian and apocalyptic scenarios of fiction. However, the 'unending' and 'everywhere' war does imply, following Focault's interest in the continuation of war once peace has been declared, that the spatial and temporal parameters of conflict are increasingly escaping even the foggiest notion that peace and war are inseparable. Shaw has argued that failing to conceive of artificial intelligence in terms of its behavioural agency (which is implicitly limited to humans) fails to consider how artificial intelligence and robots will transform the global political order independent of their instrumental use by.[135] At its most seemingly innocuous end in terms of the spectrum of possibilities encountered, the set of issues posed suggest that war and security will increasingly become a routinized, normalized and indeed biopolitical in terms of its structure for even the smallest processes of everyday life across multiple spaces. At the other end of this spectrum towards the seemingly impossible nightmare scenarios encountered in fiction, algorithmic warfare is posed to extend the liberal rationality of 'peace through force' into the realm of totalitarianism and the threat of mass techno-inflicted violence across the globe.

Conclusion

The notion that war is now 'never-ending' has a two-fold dimension. The first is that in order to retain advantage over one's opponents, one must be continuously adapting and innovating, especially as those opponents are able to play 'catch-up' at an increasing speed. The second dimension is that, as a consequence of the first dimension, the life-worlds of individuals and societies will be increasingly subjugated to a particular militarized and securitized logic of adaptation and innovation, such that human life itself risks being lost to

[134] As cited in Evans, "Foucault's legacy," p. 422.

[135] Shaw, "Robot Wars," p. 454.

totalitarian governance or even total destruction. This of course is a dramatization of the latent possibilities in a 'permanent' and 'everywhere' war. However, as a great deal of research has shown, these latent possibilities are already actual realities for an increasing number of people across the globe. Thus, the potential consequences of these dramatic possibilities should not be discounted.

As a brief summary of the expansive discussion made above, this article has argued that drone and algorithmic warfare are an expression of and an indivisible tool for the 'never-ending' war that is now propelling US security strategy rhetoric. These technologies and the never-ending war itself are not 'new' in the sense that there is a clean break between the conflicts of yesterday and today. However, modern warfare is not the same either. Rather, these technologies and the rationalities that underpin them are part of a much larger set of practices that are historically rooted with linkages to the Cold War, the World Wars, and even to the Napoleonic Wars, but have increasingly penetrated the lives of everyone in new and complex ways. In this respect, drone and algorithmic warfare represent a particular configuration of a simultaneous evolution in technological capability and an acute faith in that capability to mitigate the risks of uncertainty, which paradoxically appear to be increasing as a result of globalized networks. Fukuyama's 'end of history' it seems gave birth to the very conditions that are undermining its own stability. While the policies and technologies associated with counter-terrorism have formed and will undoubtedly continue to form a major part of this security environment, the return of 'great power competition' entails much wider implications stemming from an intensified focus on distance and autonomy. If the recent US security strategy is to serve as an indicator for where history will go, it will be a race to not only decide more than the 'Other', whoever that may be, but to know, decide and, if necessary, strike *faster* – to essentially collapse the spectrum of domains and dominate a singular domain of *space-time.* To accomplish this may require a totalizing endeavor not dissimilar to the complete and total mobilization of society needed to wage the World Wars, the culmination of *total war*. However, unlike the blurring of the civilian and military spheres along with the mass mobilization of labour and industrial capacity, total war in the 'never-ending' sense implies that it will happen in the networks and minutia of everyday life, perhaps without us even knowing it.

Bibliography

Agius, Christine. "Ordering without bordering: drones, the unbordering of late modern warfare and ontological insecurity." *Postcolonial Studies* 20, no. 3: 370-386 (2017).

Amoore, Louise, and Rita Raley. "Securing with algorithms: Knowledge, decision, sovereignty." *Security Dialogue* 48, no. 1: 3-10 (2017).

Andrejevic, Mark, and Kelly Gates. "Big data surveillance: Introduction." *Surveillance & Society* 12, no. 2: 185-196 (2014).

Arquilla, John, and David Ronfeldt. *Networks and netwars: The future of terror, crime, and militancy*. Rand Corporation, 2001.

Asaro, Peter M. "The labor of surveillance and bureaucratized killing: new subjectivities of military drone operators." *Social semiotics* 23, no. 2: 196-224 (2013).

Asaro, Peter M. "On banning autonomous weapon systems: human rights, automation, and the dehumanization of lethal decision-making." *International Review of the Red Cross* 94, no. 886: 687-709 (2012).

Axtell, Travis. "Operational Perspective: Project Maven." In *Challenges in Machine Generation of Analytic Products from Multi-Source Data: Proceedings of a Workshop*, 7-9. The National Academies Press, 2017. https://www.nap.edu/catalog/24900/challenges-in-machine-generation-of-analytic-products-from-multi-source-data

Bentley, M. "Fetishised data: Counterterrorism, drone warfare and pilot testimony." *Critical Studies on Terrorism*, 11, no. 1: 88-110 (2018).

Blakeley, Ruth. "Drones, state terrorism and international law." *Critical Studies on Terrorism*, 11, no. 2: 1-21 (2018).

Blum, Gabriella, and Philip Heymann. "Law and policy of targeted killing." *Harv. Nat'l Sec. J.* 1: 145-170 (2010).

Bourne, Mike. "Guns don't kill people, cyborgs do: a Latourian provocation for transformatory arms control and disarmament." *Global Change, Peace & Security* 24, no. 1: 141-163 (2012).

Bousquet, Antoine. "Chaoplexic warfare or the future of military organization." *International Affairs* 84, no. 5: 915-929 (2008).

Bousquet, Antoine. "A Revolution of Military Affairs? Changing technologies and changing practices of warfare." In McCarthy, Daniel R. (ed.), *Technology and World Politics: An Introduction*, 165-181. New York: Routledge, 2018.

Braun, Megan, and Daniel R. Brunstetter. "Rethinking the criterion for assessing CIA-targeted killings: Drones, proportionality and jus ad vim." *Journal of Military Ethics* 12, no. 4: 304-324 (2013).

Castells, Manuel. *The rise of the network society*. John Wiley & Sons, 2011.

Conger, Kate and Dell Cameron. "Google is Helping the Pentagon Build AI for Drones." *Gizmodo* (March 6, 2018). https://gizmodo.com/google-is-helping-the-pentagon-build-ai-for-drones-1823464533

Curtis, Neal. "The explication of the social: Algorithms, drones and (counter-) terror." *Journal of Sociology* 52, no. 3: 522-536 (2016).

Dalby, Simon. "Political space: autonomy, liberalism, and empire." *Alternatives* 30, no. 4: 415-441 (2005).

Department of Defense. *Summary of the 2018 National Defense Strategy of The United States of America: Sharpening the American Military's Competitive Edge*. 2018. https://www.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf

Deputy Secretary of Defense. "Establishment of an Algorithmic Warfare Cross-Functional Team (Project Maven)." *Department of Defense Memorandum*, Washington, DC. (April 26, 2017). https://www.govexec.com/media/gbc/docs/pdfs_edit/establishment_of_the_awcft_project_maven.pdf

Der Derian, James. "Virtuous war/virtual theory." *International affairs* 76, no. 4: 771-788 (2000).

Der Derian, James. "The (s) pace of international relations: Simulation, surveillance, and speed." In *Critical Practices in International Theory*, pp. 55-74. New York: Routledge, 2009.

Dillon, Michael, and Julian Reid. "Global liberal governance: biopolitics, security and war." *Millennium* 30, no. 1: 41-66 (2001).

Duffield, Mark. “War as network enterprise: the new security terrain and its implications.” *Cultural values* 6, no. 1-2: 153-165 (2002).

Duffield, Mark. *Disaster-resilience in the network age access-denial and the rise of cyber-humanitarianism*. No. 2013: 23 (2013). DIIS Working Paper. https://www.diis.dk/files/media/publications/import/extra/wp2013-33_disaster-resilience-cyber-age_duffield_web.pdf

Duffield, Mark. *Global governance and the new wars: the merging of development and security*. London and New York: Zed Books Ltd, 2014.

Duffield, Mark. "The digital development-security nexus: Linking cyber-humanitarianism and drone warfare." In *Handbook of International Security and Development*, edited by Paul Jackson, 80-94. Cheltenham, Northampton: Edward Elgar Publishing, 2015.

Duffield, Mark. “The resilience of the ruins: towards a critique of digital humanitarianism.” *Resilience* 4, no. 3: 147-165 (2016).

Escobar, Pepe. *Globalistan: How the globalized world is dissolving into liquid war*. Nimble Books LLC, 2006.

Espinoza, Marina & Afxentis Afxentiou. “Editors’ introduction: drones and state terrorism.” *Critical Studies on Terrorism*, vol. 11, no. 2: 295-300 (2018).

Esposti, Sara. “When big data meets dataveillance: The hidden side of analytics.” *Surveillance & Society* vol. 12 no. 2: 209-225 (2014).

Evans, Brad. "Foucault’s legacy: Security, war and violence in the 21st century." *Security Dialogue* 41, no. 4: 413-433 (2010).

Flaherty, Martin S. "The constitution follows the drone: Targeted killings, legal constraints, and judicial safeguards." *Harvard. Journal of Law & Public Policy* 38: 21-42 (2015).

Fukuyama, Francis. *The end of history and the last man*. New York: Free Press, a division of Simon and Schuster, 2006.

Gorka, Sebastien. “Adapting to Today’s Battlefield: The Islamic State and Irregular War as the “New Normal”.” In *Beyond Convergence: World Without Order*, edited by Hilary Matfess and Michael Miklaucic. Washington: Center for Complex Operations, National Defense University, 2016. http://cco.ndu.edu/Portals/96/Documents/books/Beyond%20Convergence/BEYOND%20CONVERGENCE%20%20World%20Without%20Order%20.pdf?ver=2016-10-25-125406-170

Gregory, Derek. "Seeing red: Baghdad and the event-ful city." *Political Geography* 29, no. 5: 266-279 (2010).

Gregory, Derek. "The everywhere war." *The Geographical Journal* 177, no. 3: 238-250 (2011).

Haas, Michael Carl, and Sophie-Charlotte Fischer. "The evolution of targeted killing practices: Autonomous weapons, future conflict, and the international order." *Contemporary Security Policy* 38, no. 2: 281-306 (2017).

Hall, Alexandra, and Jonathan Mendel. "Threatprints, threads and triggers: imaginaries of risk in the ‘war on terror’." *Journal of Cultural Economy* 5, no. 1: 9-27 (2012).

Hayes, Jarrod. "The democratic peace and the new evolution of an old idea." *European Journal of International Relations*18, no. 4: 767-791 (2012).

Healey, Jason. “Stuxnet and the Dawn of Algorithmic Warfare.” *Huffington Post* (June 16, 2013). https://www.huffingtonpost.com/jason-healey/stuxnet-cyberwarfare_b_3091274.html

Heathershaw, John. "Unpacking the liberal peace: The dividing and merging of peacebuilding discourses." *Millennium*36, no. 3: 597-621 (2008).

Holmqvist, Caroline. "Undoing war: War ontologies and the materiality of drone warfare." *Millennium* 41, no. 3: 535-552 (2013).

Ignatieff, Michael. "The American empire." *New York Times Magazine* (January 5, 2003). https://www.nytimes.com/2003/01/05/magazine/the-american-empire-the-burden.html

Joh, Elizabeth E. "Policing by numbers: big data and the Fourth Amendment." *Wash. L. Rev.* 89: 35-68 (2014).

Kaldor, Mary. *New and old wars: Organised violence in a global era*. Cambridge: Polity Press, 2012.

Kastan, Benjamin. "Autonomous Weapons Systems: A Coming Legal Singularity." *U. Ill. JL Tech. & Pol'y*: 45-82 (2013).

Kessler, Gary, Maye, Diane & Aaron Richman. "Artificial Intelligence in Shaping Preferences and Countering the Radicalization Process." *White Paper for the Decadal Survey of the Social and Behavioral Sciences for National Security*. Philadelphia: TAM-C Intelligence, 2017. https://sites.nationalacademies.org/cs/groups/dbassesite/documents/webpage/dbasse_179881.pdf

Kindervater, Katharine Hall. "The emergence of lethal surveillance: Watching and killing in the history of drone technology." *Security Dialogue* 47, no. 3: 223-238 (2016).

Kindervater, Katharine Hall. "Drone strikes, ephemeral sovereignty, and changing conceptions of territory." *Territory, Politics, Governance* 5, no. 2: 207-221 (2017).

Krishnan, Armin. *Killer robots: legality and ethicality of autonomous weapons*. New York: Routledge, 2016.

Landau, Susan. "Making sense from Snowden: What's significant in the NSA surveillance revelations." *IEEE Security & Privacy* 11, no. 4: 54-63 (2013).

Lang Jr, Anthony F. "Punishment and peace: Critical reflections on countering terrorism." *Millennium* 36, no. 3: 493-511 (2008).

Leander, Anna. "Wars and the un-making of states: taking Tilly seriously in the contemporary world." In *Contemporary security analysis and Copenhagen peace research*, edited by Stefano Guzzini and Dietrich Jung, 85-96. New York: Routledge, 2004.

Luttrell, Johanna C. "Alienation and global poverty: Arendt on the loss of the world." *Philosophy & Social Criticism* 41, no. 9: 869-884 (2015).

Mac Ginty, Roger. "Warlords and the liberal peace: state-building in Afghanistan." *Conflict, Security & Development* 10, no. 4: 577-598 (2010).

Marr, Bernard. “Big data: 20 mind-boggling facts everyone must read.” *Forbes* (September 30, 2015). *https://www.forbes.com/sites/bernardmarr/2015/09/30/big-data-20-mind-boggling-facts-everyone-must-read/*

McNeal, Gregory S. "Targeted killing and accountability." *Geo. lj* 102: 681-794 (2013).

Meyer, Jörg. "The concealed violence of modern peace (-making)." *Millennium* 36, no. 3: 555-574 (2008).

Neocleous, Mark. "Air power as police power." *Environment and Planning D: Society and Space* 31, no. 4: 578-593 (2013).

Neocleous, Mark. *War power, police power*. Edinburgh: Edinburgh University Press, 2014.

Niva, Steve. "Disappearing violence: JSOC and the Pentagon’s new cartography of networked warfare." *Security Dialogue* 44, no. 3: 185-202 (2013).

Pellerin, Cheryl. “Project Maven Industry Day Pursues Artificial Intelligence for DoD Challenges.” *DoD News, Defense Media Activity* (October 27, 2017). https://www.defense.gov/News/Article/Article/1356172/project-maven-industry-day-pursues-artificial-intelligence-for-dod-challenges/

Pellerin, Cheryl. “Project Maven to Deploy Computer Algorithms to War Zone by Year’s End.” *DoD News, Defense Media Activity* (July 21 2017). https://www.defense.gov/News/Article/Article/1254719/project-maven-to-deploy-computer-algorithms-to-war-zone-by-years-end/

Rumsfeld, Donald H. "Transforming the military." *Foreign Affairs* (May/June, 2002): 20-32. https://www.foreignaffairs.com/articles/2002-05-01/transforming-military

Rupka, S. & Bianca Baggiarini. “The (non) event of state terror: drones and divine violence.” *Critical Studies on Terrorism*, vol. 11, no. 2: 342-356 (2018).

Shanahan, Jack, Lt. General. “Algorithmic Warfare Cross-Functional Team (AWCFT) aka Project Maven.” Presentation for National Defense Industrial Association, *Department of Defense of the United States of America* (October 26, 2017). https://www.ndia.org/-/media/sites/ndia/divisions/cet/ndiaoct17secured.ashx?la=en

Shane, Scott, Metz, Cade and Daisuke Wakabayashi. “How a Pentagon Contract Became an Identity Crisis for Google.” *The New York Times* (May 30, 2018).

https://www.nytimes.com/2018/05/30/technology/google-project-maven-pentagon.html

Shaw, Ian GR. "Predator empire: The geopolitics of US drone warfare." *Geopolitics* 18, no. 3: 536-559 (2013).

Shaw, Ian GR. "Robot Wars: US Empire and geopolitics in the robotic age." *Security Dialogue* 48, no. 5: 451-470 (2017).

Shaw, Ronald, Ian Graham, and Majed Akhter. "The unbearable humanness of drone warfare in FATA, Pakistan." *Antipode* 44, no. 4: 1490-1509 (2012).

Sonne, Paul. "Pentagon unveils new nuclear weapons strategy, ending Obama-era push to reduce U.S. arsenal." *The Washington Post* (February 2, 2018). https://www.washingtonpost.com/world/national-security/pentagon-unveils-new-nuclear-weapons-strategy-ending-obama-era-push-to-reduce-us-arsenal/2018/02/02/fd72ad34-0839-11e8-ae28-e370b74ea9a7_story.html?utm_term=.35d334218a0f

Stoler, Ann Laura. "On degrees of imperial sovereignty." *Public Culture* 18, no. 1: 125-146 (2006).

Tilly, Charles. "War making and state making as organized crime." In *Violence: A reader*, edited by Catherine Bestemen, 35-60. New York: NYU Press, 1985.

Virilio, Paul. *The vision machine*. Bloomington & Indianapolis: Indiana University Press, 1994.

Virilio, Paul. *Speed and Politics*. Cambridge: MIT Press, 2006.

Wall, Tyler. "Ordinary emergency: Drones, police, and geographies of legal terror." *Antipode* 48, no. 4: 1122-1139 (2016).

Weber, Jutta. "Keep adding. On kill lists, drone warfare and the politics of databases." *Environment and Planning D: Society and Space* 34, no. 1: 107-125 (2016).

Weisgerber, Marcus. "The Pentagon's New Algorithmic Warfare Cell Gets Its First Mission: Hunt ISIS." *Defense One* (May 14, 2017). https://cdn.defenseone.com/b/defenseone/interstitial.html?v=8.15.0&rf=https%3A%2

F%2Fwww.defenseone.com%2Ftechnology%2F2017%2F05%2Fpentagons-new-algorithmic-warfare-cell-gets-its-first-mission-hunt-isis%2F137833%2F

Wesseling, Mara, Marieke de Goede, and Louise Amoore. "Data wars beyond surveillance: opening the black box of SWIFT." *Journal of Cultural Economy* 5, no. 1: 49-66 (2012).

Work, Bob. "The third US offset strategy and its implications for partners and allies." Speech delivered at Willard Hotel, Washington, *Department of Defense, Washington* (January 28, 2015). https://www.defense.gov/News/Speeches/Speech-View/Article/606641/the-third-us-offset-strategy-and-its-implications-for-partners-and-allies/