



Fuller spectrum operations: the emergence of larval warfare

Biswas Mellamphy Nandita¹

© The Author(s), under exclusive licence to Springer Nature Limited 2025

Abstract

This essay sets out to tackle a theoretical challenge: to offer a conceptual re-framing that addresses how digital technical and cultural transformations have influenced the nature of modern warfare resulting in the emergence of ‘larval warfare’ (*larva* being Latin for ‘mask’ and/or ‘spectre’). The aim is to explore the rationale and theory of larval warfare, as well as speculate about its significance and implications for future security challenges that will necessitate not only managing risks and threats, but also require the creation of new concepts and epistemological tools. Focusing on conceptual/philosophical arguments, I speculate about the emergence of a distinct construct of warfare that conceptually depends on blurring the strict boundaries between military and civilian domains. The *latent*, *emergent*, and *masked* nature of this mode of warfare exceeds, and thus disrupts, traditional domains of theorization. As a construct (rather than as a ‘model’ or ‘prototype’ that can be implemented), the notion of larval warfare allows philosophical rumination about the changing nature of warfare in the context of planetary-wide technical transformations. The first section introduces the theoretical context and empirical trends that have led to the emergence of larval warfare, focusing on outlining selected but relevant interdisciplinary scholarship in international relations, war studies, surveillance/media studies, and cultural studies. The next section offers a philosophical interpretation of the notion of ‘larval warfare’ and lays out its distinctions from the existing models of modern warfare (conventional and non-conventional). The final section concludes with some thoughts on the fundamentally *predatory* quality of larval warfare and its amenability with the contemporary phenomenon of ‘surveillance capitalism.’

Keywords Information · Imperceptibility · Propaganda · Surveillance capitalism · Ambiguity · Warfare · Security · Technology · Digital culture · Everyday life · Weaponization · Civilian · Non-military

Contextualizing larval warfare: ambiguity and the weaponization of imperceptibility

It is challenging to theorize the role that ambiguity plays in international relations. Unlike risk and uncertainty—two other forms of indeterminacy that have preoccupied scholarly attempts to understand the effects of the limits of knowledge on governance—ambiguity has been undertheorized (Best 2008).¹ The concept of ambiguity, unlike the other two terms, refers etymologically to double meanings, equivocalness, and double sense, or more philosophically/conceptually speaking, ‘the inherent slipperiness of interpretation.’² Not only has ambiguity become increasingly problematic in global politics—especially for societies dependent on

social communicational networks—but the specific concept exceeds theorizations focused on risk and uncertainty. Regardless of whether it is in terms of governing (i.e., limiting) ambiguity, or instead of instrumentalizing ambiguity, or alternatively of considering the non-governability of ambiguity, ‘both risk and uncertainty literatures tend to treat uncertainty or radical contingency as the principal categories through which we can apprehend the unknowable that exceeds efforts at calculation. These terms represent the unknown in terms of an indeterminate future. This remains an important form of indeterminacy, but it still downplays the indeterminacy of the present—and, above all, its *interpretive* character [emphasis mine].’³ The interpretive and intersubjective aspects of ambiguity have seldom been the focus of disciplinary accounts of international relations, but this does not mean that theorists outside the discipline have not considered the roles of ambiguity, interpretation, intersubjectivity, and rhetoric in constituting social relations.

✉ Biswas Mellamphy Nandita
nbiswasm@uwo.ca

¹ Department of Political Science, Western University, London, Canada



In fact, Marshall McLuhan had prognosticated over fifty years ago that not only would communication and information networking become routine, and not only would societies orient their social practices toward the formation of media ecologies, but the interpretive ambiguities resulting from the proliferation of new media would blur conceptual and actual hierarchies between military and civilian jurisdictions, expert knowledge and popular culture, as well as conflate the boundaries between war and peace (McLuhan 1970).⁴ McLuhan also knew that these thresholds of ambiguity could be exploited and even weaponized: ‘When information moves instantly to all parts of the globe, it is chemically explosive. [...] It is the normal aspect of our information-flow which is revolutionary now. The new media normalize the state of revolution which is war. [...] The media of communication are not mere catalysts but have their own physics and chemistry which enter into every moment of social alchemy and change (McLuhan 1967).’ McLuhan’s wager was that information would become a driving force of societies, shaping people and everything around them. Media are not merely instruments for communication; for McLuhan, media shape minds and social relations. Media operate subjectively and intersubjectively by operationalizing ambiguity, the fundamental condition of multiplicity and inherent duplicity/doubleness of information that entails ‘a tactical generalization of the battlespace and of the concept of war itself (Macdonald 2011).’ For McLuhan, media are rhetorical war machines that have the power to influence perceptions and impose psycho-technical mandates. ‘Rhetoric, after all, was perhaps the first psycho-technology, the first systematic attempt to manipulate the soul (*psyche*) by means of an art (*techne*) of speech (*logos*).’⁵ According to McLuhan, the computational digital paradigm of media and information—the reduction of letters to a numeric sign (1) and its absence (0)—has begun a re-programming that has weaponized information by making it ‘ethereal.’ Etherealization is the ‘trend toward more and more power with less and less hardware’ (McLuhan 1964).

Likewise in this regard (but different in many others), Paul Virilio argued that technological transformations would catapult warfare beyond the theater of the traditional battlefield, changing the conditions—and thus the very nature—of war. Instead of the modern conception of limited warfare, Virilio suggested that technologically driven capitalist societies would actively and infinitely prepare for war even when not engaged in battle. ‘[T]he situation is no longer very clear between the civil and the military because of the total involvement of the economy in war—already beginning in peacetime’ (Virilio and Lotringer 2008); ‘[a]ll of us are already civilian soldiers, without knowing it. And some of us know it. The great stroke of luck for the military class’s terrorism is that no one recognizes it. People do not recognize the militarized part of their identity, of their

consciousness.’⁶ Both McLuhan and Virilio presaged what future military theorists would highlight as a benchmark of twenty-first century netwarfare: the weaponization of information and communication, the turn to ‘soft power,’ ‘information operations,’ and ‘perception management.’⁷ Warfare would no longer be held in check by policy and politics, and nation states would not be considered the only or most important actors in the business of warfare. The media landscapes of ‘soft’ war are made malleable by state and non-state actors who possess capabilities to wage their own wars through global media platforms (Kaempf et al. 2017). Moreover, domestic terrorism increases as nations consider their own domestic populations to be equal or greater threats to national security than foreign enemies (Hesterman 2019). Top-down, state-centric designs of power are disrupted by the emergence of information contests as civilians and other non-state information actors compete with states to gain influence over social networks and the shaping of public opinion (Mazarr et al. 2019). The category of the ‘civilian’ (non-combatant) shifts from being conceived as a legally, politically and morally protected actor under the international laws of warfare (Winter 2011), to a fuzzy 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, and automated/algorithmic surveillance (Amoore 2020); Browne 2010).⁸

Warfare is being transformed by socio-technical media and the mediatized tendencies of societies dependent on information and communication technologies. Hypermediatization opens the way for anyone to film, edit, and share information, images, and videos in real time, whether traditional media report on these events, or not. This turns anyone into a potential information actor that can distribute messages to audiences of unlimited number and size around the world (Kaempf 2013).⁹ Mass and digital communications have changed governance and state-citizen power dynamics from a single authority speaking to many listeners, to one in which many speak to many (Anderson 2011). Governments and traditional media are no longer the most important players in the information space; now they must compete for their place amid various other actors.¹⁰ Warfare is conducted not only in the contexts of military battlespaces, martial personnel, armed force and weapons. Increasingly, warfare is creeping into the domain of everyday social interactions. Rather than being an extraordinary and highly visible military instrument of last resort for nation states, the media of communications has embedded warfare into the fabric of ordinary, everyday life (Floridi and Taddeo 2014),¹¹ to be waged by social groups, civilians, social networks, firms, contractors, and even social media technologies, in addition to nation states and governments.¹² Today warfare is conducted not only in military battlespaces by martial personnel



using armed force and weapons; increasingly, warfare is creeping into the realms of everyday culture and sweeping across social networks using familiar and ordinary platforms of social communication as weapons for gaining advantage over opponents (Under the Radar; War and Social Media 2022).

Larva is the Latin word for ‘mask’ referring to the biological sense in which immature insects ‘mask’ their adult forms, but also to an older usage referring to ‘ghost or specter,’ as that which is shrouded (especially in the sense of something that falls outside the spectrum of standard perceptions), deriving from the Old French *mascurer*, ‘to blacken, darken,’ related to the English word ‘mesh.’ Consistent with its serpentine etymology, larval warfare does not behave like war at all; rather its operations are enmeshed: ordinary and everyday, but also spectral and incognito. Its rationale is ambiguous, ambivalent, and ambidextrous, making use of façade, and/or personas but very hard to pin down. I use ‘larval’ in the following seven senses: (1) as ‘masked’ in the ordinary sense of ‘putting on a face/persona’; (2) as ‘masked’ in the non-[re]presentational sense of that which is ‘obscured,’ ‘hidden,’ ‘covered-over,’ ‘blacked-out’ or effaced; (3) as ‘ghost-like’ in the sense of having a spectral, ‘ghostly presence’—i.e., as that which ‘haunts’; (4) as ‘pupating’ in the manner of pupæ—i.e., as ‘emergent’ or in the ‘larval stage or phase’ of becoming; (6) as that which ‘swarms’ in the manner of larval multiplicities (and in this sense ‘formless’ or «informe» in French), as in that which involves multiple/multiplying intersects; (7) in the sense, as well, of ‘backward-masking’ in sound-recording, involving encryption, crypto-steganography/steganology, etc.

Larval warfare exploits the embryonic, ambiguous, ephemeral, multiple, and hieroglyphic gestures of subjectivity and perception. Following Gilles Deleuze’s account, larval subjects are not to be understood as fully constituted and stable selves, but only “‘rough draft[s]” (Deleuze 2004) of subjective potentiality that can become sites for manipulation. ‘Selves are larval subjects;’ ‘the world of passive syntheses constitutes the system of the self, under conditions yet to be determined, but it is the system of a dissolved self’ (Deleuze 1994). Larval subjects are in the process of individuation but not yet individuated. ‘Individuation is mobile, strangely supple, fortuitous, and endowed with fringes and margins. [...] The individual is far from indivisible, never ceasing to divide and change its nature.’¹³ Rhetorical war machines exploit psycho-technologies that manipulate larval subjectivities and can weaponize cognitive and perceptual vulnerabilities to influence individuation processes, opinions, and behaviors.

I suggest that practices of warfare are emerging that are not designed to be *visible* and *spectacular*, but rather, *imperceptible* and *obscure*. More and more, warfare is conducted but we cannot see it—not because it is invisible or because

we are short-sighted (although both those things may be true); but because it is meant to be something we cannot readily identify. This is a mode of warfare *without* the obvious spectacle of war; it is latent and capable of exploiting the thresholds between presence and absence, appearance and disappearance, clarity and opacity. A *larval* form of warfare is emerging that bypasses both the overt, coercive force of the state’s war machinery, as well as the normal political processes that are meant to regulate warfare. This is a distinct construct of warfare in which the rationales and zones of non-combat are re-conceptualized as obscure battlezones (Lu 2022).¹⁴ This style of warfare is not based on the behaviors usually associated with conventional fighting, armed conflict, or the use of force; nor is it synonymous with unconventional fighting like drone strikes, guerilla tactics, or urban warfare (characteristics of unconventional network-centric warfare). Rather than behaving as dominating or domineering, larval warfare encroaches into ordinary life, making use of the appearance of ordinariness, cunningly entangling itself in civilian networks, and incrementally merging with the very media of informational/communicational exchange to exploit socio-technical vulnerabilities from within (Galeotti 2022).¹⁵ Hostile motivations and belligerence remain couched in civilian, aesthetic, ludic, and communicative techniques designed to appear ordinary. Digital cultural techniques like clicking, surfing, tagging, and poking, and technological regimes like online gaming and social media thus become fertile ground for the permeation of techniques of warfare like covert surveillance, tracking, targeting, and espionage into civilian domains and social relations (Robinson 2018; Erbschole 2017).¹⁶ Larval operations mask their character, motives and weapons, having a spectral quality that leaks, sneaks and percolates into various environments, encroaching imperceptibly and undetectably.

Larval warfare refers to warfare that continuously masks its martial character, appearing as benign and civilian. Larval warfare is peacetime conflict, an emergent condition of ongoing warfare in the absence of any declaration of war (Hawkins 2023).¹⁷ As a predatory mode, larval warfare advances by masking its military tactics & strategies through non-military tools and platforms. Instead of being a well-defined set of military imperatives governed by the regular norms of war, larval warfare remains fuzzy, and this ambiguity involves the indefinite militarization of peace encompassing not only the enmeshing of governmental organizations, digital media/information-technology firms, consumers/citizens, and non-state networks, but also the exploitation of non-military assets, non-human actors, and technical weapons such as code, algorithms, data-analytics, and malware (Shattuck 2020; Chang and Yang 2020).¹⁸ Larval warfare exploits the ‘infectious’ qualities of digitality and net centrality, while simultaneously circumventing the physical and legal constraints imposed on the conduct



of normative warfare. Unlike conventional kinetic warfare which is bound by the international laws of war, larval warfare incorporates features of psychological warfare which is said to begin long before the declaration of war and continue much after overt hostilities have stopped. It is the disguised and subversive dimension of psychological warfare that enables making military gains without the use of force. In psychological warfare, all communication can have propaganda effects including induced misperception, distraction, and disorientation, and even diplomacy and public relations are considered to be resources (Linebarger 1948).¹⁹

The ‘information domain’ has become a central focus for cultural diplomacy and geopolitics, and many states have incorporated ‘communication war’ into their military doctrines (Payne, 2008). Larval warfare entails conducting disguised and subversive propaganda and disinformation campaigns against opponents; in this aspect, it exploits the ambiguities between persuasion and manipulation by way of technology/techniques of specific media. The medium of communication becomes an important weapon because it is what not only conducts and transmits influential messages to target populations, but also what shapes people’s perceptions, comprehensions, opinions and decision-making.²⁰ Contemporary socially mediated information warfare uses propaganda objectives of psychological warfare. However, unlike the top-down propaganda of the past based on print (pamphlets), radio, and television media which conceptualize target audiences as passive receivers of messages, digital media involve multiple networks and exchanges of communication and are interactive, requiring the active participation of target audiences. Not only does digital propaganda eliminate the spatial and temporal gaps between the generation, consumption, and circulation of propaganda, but social media networking turns social interaction into a mechanism of amplification (Zuckerman 2018). The amalgamation of content generation, sharing, and discussion produces an alluring effect in which users are unable to divorce content consumption from their personal communication; the consumption of propaganda is ingrained in the structure of social relations permitting propaganda to creep into everyday living. ‘Instead of encouraging you to filter alternative sources of information, participatory propaganda aims to reshape your cognitive filters as well as the relationship between you and your environment (Asmolov and LeJeune 2019).’ Indeed, to harness the trends and potentials of digital social mediation has become a priority both for conducting warfare and for conceptualizing military doctrine. Commanding the trend’ is a social media mechanism of persuasion used in social networking that is fast becoming a weapon of warfare involving the exploitation of preexisting social networks by subversive agents especially through the use of algorithmic/automatic techniques in order to covertly

introduce propaganda effects into social media platforms and ensure the quick and cost-effective circulation of messages, narratives and false information (Prier 2017).²¹ States and non-state actors alike have used this blend of social media trending/trend-setting techniques and propaganda to advance their hostile objectives, to challenge the international community and mainstream media, and to grow their membership base.²²

It is not simply that social media have become used as tools of warfare, but also that military rationale and practice have struggled to keep up with and adapt to the quixotic transformations and permanent disruptive effects of ever-expanding digital networking practices (Oates 2020).²³ Part of the challenge lies in finding appropriate frameworks for conceptualization. State-centric approaches seek to explain information warfare in terms of top-down, strategic models of power. Standard conceptions of information warfare share assumptions that states/state-sponsored agents are the main actors ‘weaponizing’ information, advancing a state-centered view of ‘information dominance’ in which state elites use disinformation in military and strategic terms to manipulate and control civilians who are predominantly seen as passive and/or victimized recipients of state actions. State-centric approaches, as such, cannot really capture the ways in which citizens are taking active roles in curating disinformation (Golovchenko et al. 2018).²⁴

The emergence of a third construct: standard, non-standard, and larval warfare

The concept of full-spectrum dominance was introduced into military doctrine not only to expand combat capabilities and concretize state superiority in conducting high-tech warfare, but also to redefine military priorities and extend the military’s traditional role beyond warfighting. In high-intensity warfare—the standard model—conflict must be defensively deployed, formally declared, legally acknowledged, and confined to conventional land, air, and sea battlespaces. The aim of warfare is to use force against enemies to achieve kinetic dominance while protecting civilian non-combatants. Implementation of offensive strategies, network-centric warfare such as drone operations, and hybrid warfare focusing on information operations, including cyberattacks and the rise of ‘cross-domain coercion’ and ‘other than war operations’ (OOTW) have led to the turn to non-standard warfare. Techniques and technologies used to wage non-standard warfare, however, have altered the strategic importance of unconventional and emergent battlespaces. While the stretching of thresholds has led to the rise of non-standard operations, it has also led to the emergence of another unacknowledged practice of warfare that is yet-undefined. In addition to the



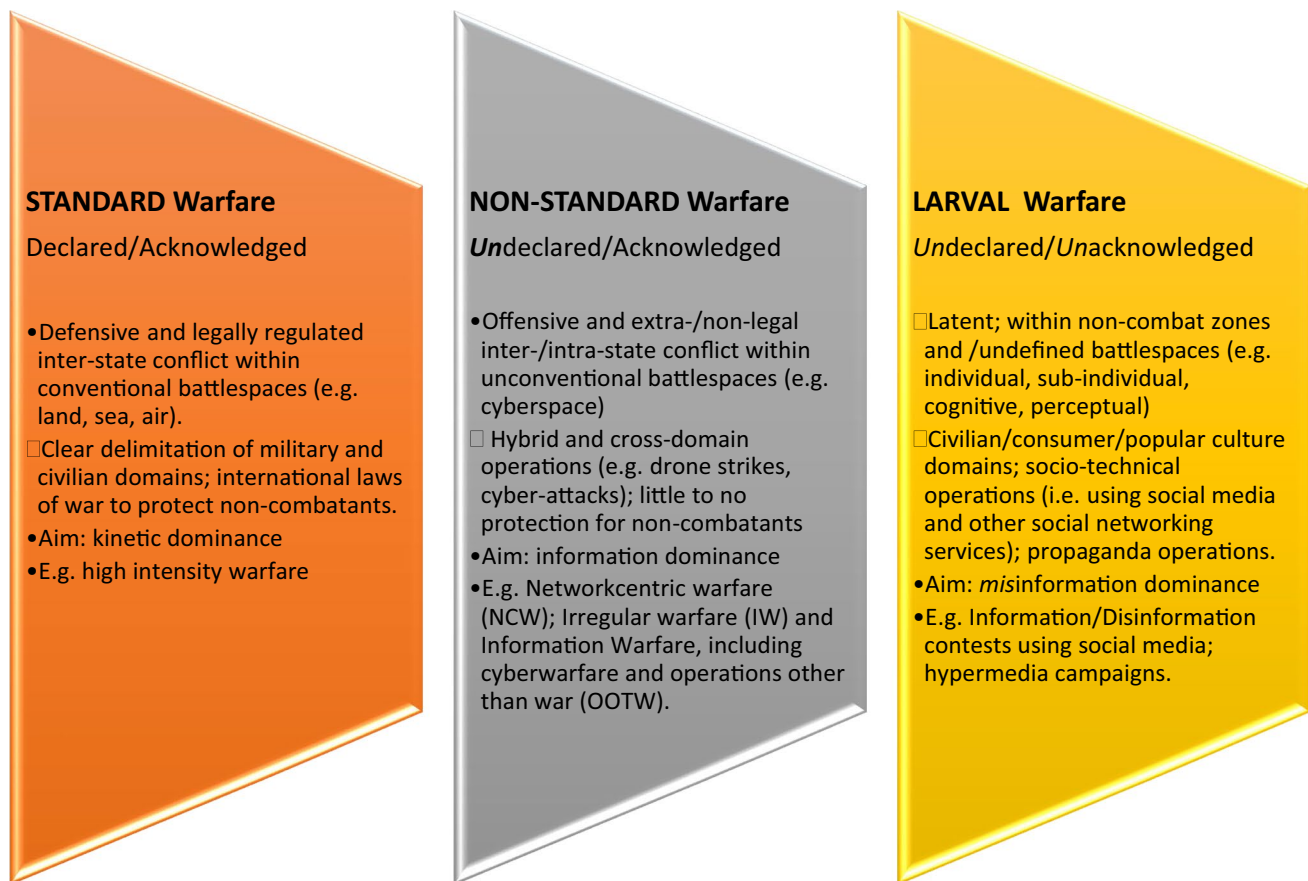


Fig. 1 Three Constructs of Warfare

concepts of standard defensive operations and non-standard offensive operations, a third construct of warfare emerges that could be called ‘larval.’ While all three are theoretically distinct domains of warfare, in practice, they are not mutually exclusive; all three constructs can be deployed concurrently to increase and expand the spectrum of warfare operations possible (Fig. 1).

Larval warfare recalibrates and extends ‘full-spectrum’ capabilities, defined as the superiority resulting from combining military with social, economic, political, psychological and technological control. Unlike conventional defensive armed warfare which is bound by the international laws of war, larval warfare is latent; it exists and continues despite the absence of overt hostilities. It is the disguised and subversive non-military dimension of larval warfare that enables making military gains without the use of force. Larval warfare seeps, creeps, and sweeps into civilian cultures, thereby widening the spectrum of battlespace beyond conventional defensive and unconventional offensive conceptions of warfare.

Larval warfare, unlike standard and non-standard forms of warfare, is not definable and thus not acknowledged as warfare (requiring no declarations of war, no delimitations of

battlespace, and no regulation by policy). Warfare objectives can be operationalized without friction under the radar of normal, unnoticeable, and benign everyday activities. Digital social and cultural environments become battlespaces for the conduct of larval operations that seek to shape tendencies, influence networks, and manipulate balances of power. Larval operations include propaganda and psychological operations, as well as socio-cultural and technical operations like framing, nudging, click-baiting, and other forms of technical manipulation and mediation. Warfare permeates into the micropractices of digital culture through technical ordering and the prioritization of technical rationales, computational techniques, and technological regimes. The overlapping and synchronization of the techniques of warfare with those of digital culture enacts a ‘mission creep’ in which the objectives of warfare quietly seep into everyday practices. Thus, information micro-tracking and mass collecting, metadata and traffic analyses, and micro-surveillance techniques operate easily and gratuitously proliferate in the guise of the gift ecologies of digital culture. Ordinary technoculture becomes marketing, psychological propaganda, and subtly exploiting civilian perceptions, opinions, and cultural practices becomes part of the arsenal of a *fuller*-spectrum of warfare.



Following De Certeau, the machine of war and the machine of consumption merge to produce something else: ‘a rationalized, expansionist, centralized, spectacular and clamorous production is confronted by an entirely different kind of production, called “consumption” and characterized by its ruses, its fragmentation (the result of the circumstances), its poaching, its clandestine nature, its tireless but quiet activity, in short by its quasi-invisibility, since it shows itself not in its own products (where would it place them?) but in an art of using those imposed on it (Certeau 1984).’²⁵

Larval warfare involves non-state actors, non-military targets, conventional consumer digital technologies and unconventional online-weaponry like misinformation, disinformation, hacking, click-baiting and trolling. 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 in the production and manipulation of information. As evinced by the terrible success of cyber-propaganda, quest for dominance in the realm of information has become a significant force driving present and future global conflict. As much as humans continue to believe that they are in control of this informational imperative, what is being revealed is that, more and more, all human endeavors are being shaped by the larval tendencies of information and the effects of larval warfare. From this perspective, the tech we use so ubiquitously are, *de facto*, traps within an opaque predatory economy of information (Mellamphy et al. 2014).²⁶ Perhaps larval warfare is evolving in response to what is being revealed as the indefinable and manipulable nature of information itself. Warfare is no longer just about gaining hegemony over actual physical territory, but also increasingly about informational dominance, or gaining hegemony over virtual domains through viral forms of information and communication. Whereas in the past century, military and political theories of warfare have focused on delimiting the boundaries between war and peace, 21st-century warfare has followed a different tendency, that of war as hunting, as predation or ‘manhunt’ (e.g., this was the model for America’s military doctrine of ‘Global War on Terror’). The concept of larval warfare highlights the predatory framework, the generalized emergence and deployment of technological ‘hunting.’ To think of warfare from this perspective means theoretically describing an emergent condition in which current technological imperatives, initiatives, and infrastructures to track and hunt-down information (especially digital) are increasingly obscured, encrypted, blackboxed, and thus not subject to resistance in conventional terms. What is advancing masked is predatory warfare that hunts data at all costs and thus preys upon capitalist agents of data

production, in this case technologically invested humans who increasingly adopt the point of view that ‘technology is destiny’ (to paraphrase Hans Jonas).

Larval operations can supplement conventional and unconventional warfare. American military doctrine, for example, has shifted focus to ‘stability operations’ defined as activities to ‘promote and protect US national interests by influencing the threat, political and information dimensions of the operational environment through a combination of peacetime developmental, cooperative activities and coercive actions in response to crisis (Taws 2012).’²⁷ Considered as a ‘revolution’ in doctrine by some²⁸ and by others as the next step in the ‘evolution’ of warfare,²⁹ the significance of the turn to non-military operations cannot be overlooked or underestimated: peacetime activities, civil society, and civilians have become targets of warfare and part of battlefield operations. ‘Information is a commodity receptive to weaponization[.] [...] The fourth generation battlefield encompasses the entire enemy society, and—contrary to twentieth century experience—massed force may prove detrimental to victory. The object of military operations becomes collapsing the enemy internally rather than destroying the enemy in combat (this latter being the aim of both conventional and unconventional forms of warfare). Legitimate targets will include popular support for the conflict, and “actions will occur concurrently throughout all participants’ depth, including their society as a cultural, not just a physical, entity (Knopf 2012).”³⁰

In terms of international law, war is defined as regulated armed conflict between sovereign states via their militaries (Higgins 1909; Convention 1949).³¹ From such a viewpoint, warfare operates in conditions of uncertainty, which is why the legal boundaries between ‘war’ and ‘peace’ are supposed to be rigorously upheld. The military theorist Carl von Clausewitz called this uncertainty the ‘friction’ and ‘fog’ of war (Clausewitz 2007); Kiesling 2001).³² This uncertainty or fog is part-and-parcel of the whole process of warfare according to Clausewitz—war being a realm where opacity, volatility, complexity and ambiguity reign supreme. It is the goal of military strategy to reduce, contain, and overcome the fog of war as much possible. The strategy of the modern international system has been to establish a juridical and normative framework to diminish and control the fog of war. Thus, central to the task of both military logistics as well as normative mechanisms of international law have been the codification and enforcement of norms and laws that reduce and regulate the fog of war—especially in relation to minimizing collateral damage to the civilian bystanders of war. Warfare is something that is supposed to happen between sovereign states and their representatives—a last resort to be avoided in favor of political mechanisms of conflict-resolution. War is to



be the exception, and peace the norm. War is 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.³³ By limiting warfare to interstate conflicts, the international laws of war are meant to separate and safeguard civilian 'non-combatants' from the negative effects of the fog of war.³⁴ In this schema, conflicts within a nation are to be resolved peacefully³⁵ either through domestic legal and political means or conversely—if there is internal civil war—through the state's legitimate use of force against citizens to restore order. War derives its legitimacy from its subservience to political reason, which is concretely embodied in the sovereignty of state power and is expressed in the state's power to use force and suspend laws in states of emergency. Classical warfare is, as such, a limited state of exception, and it is the sovereign's right to decide when such a state of emergency would be enacted (Schmitt 2005; Agamben 2005).³⁶ The nation-state, buttressed by the concept of state sovereignty, becomes the mediator and administrator of all other identities, affiliations and jurisdictions. Historically, this geo-political vision was reinforced by the political/normative theory that the sovereign state has, in the last instance, the authority to decide over matters within and pertaining to its own terrestrial/territorial borders.

This geo-political vision, however, is being challenged today. There are not only competing notions of sovereignty at play (commercial, economic and financial for example), there are also trans-national networks that make territorial borders secondary to trans-political sovereignties and multi-national identities. Geo-political sovereignty is being eclipsed by data-based, platform-driven and protocologically oriented architectures that are converging. Unlike the Clausewitzian concept of the 'fog of war,' which describes a condition of uncertainty that military strategy must overcome, larval warfare draws its power from the amplification of uncertainty and the efficacious exploitation of the effects of uncertainty. Techniques of warfare thus become indefinite, absolute, and omnipresent, but imperceptible—not only via the technological development of weapons of mass destruction, not only via the development of virtual and viral information technologies that make physical and national boundaries irrelevant, but—perhaps more fundamentally—from the strategic manipulation and exploitation of tendential effects. As François Jullien hypothesizes, when warfare is conceived from the perspective of tendencies and manipulation of effects, it can become omnipresent and inhuman, imposing its own logic on all activities: '[T]he whole strength of totalitarian authoritarianism lies in the following: oppression carried to extremes will no longer be seen as oppression but as its opposite—something spontaneous, natural, and requiring no justification. This is the case

partly because such pressure creates a long-term habitus that becomes second-nature to the individuals subjected to it. More fundamentally, human law, in becoming inhuman, takes on the characteristics of natural law. Insensitive and hence equally pitiless and omnipresent, it imposes its constraints on everyone, at every moment (Jullien 1995).'

Larval warfare operates above all on conditions of ambiguity. Unlike classical/standard warfare, larval warfare does not seek to delimit but rather *amplify* the fog and is, as such, normatively opaque and ethico-juridically nebulous. Larval warfare advances under cloak of benign banality since most of its techniques and instruments make ample use of everyday digital technologies and information profiling-&-mining techniques. Set within the context of the hyper-driven excesses of communication, larval warfare is a symptom of the widespread fiction of communication, its excessiveness rather than its deprivation (Baudrillard 2009).³⁷ Communication loops are traps, creating silos that can then be weaponized and used to manipulate public opinion, affect decision-making, and even alter elections. While the new media and information communication technologies in widespread use give users the feeling that they are not passive consumers but active creators of information, the new information ecosystems are highly contagious, predatory and tend to exploit vulnerabilities. Larval warfare deploys the technical force of non-human entities and increasingly autonomous machines of information capture and surveillance to gain control over how information can be modulated, manipulated and monetized. Larval warfare is not fought primarily using the laws of war, but instead operates in hyper-mediated environments in which the boundaries between war and peace become increasingly entangled, conflated, and reconfigured. In contrast with the standard concept of limited, high-intensity warfare in which the goal of military action is to reduce the uncertainties or 'fog' of war by strictly delimiting military from civilian domains, larval warfare amplifies the fog of uncertainty in order to confound the boundaries between war and peace, allowing both to become entangled and to eventually overlap. Instead of a 'fog' of war, this is, rather, a fog of peace that renders warfare omnidirectional, synchronous, and asymmetrical.

What this means is that there is no distinction between what is or is not the battlefield; all conventional domains (ground, sea, air, outer-space) in addition to non-military factors like politics, economics, culture, and morality are to be considered battlefields and thus warfare can be conducted in different spaces at the same time. Instead of phases with accumulated results of multiple battles, strategic results can now be attained rapidly by simultaneous actions. '[I]nformation warfare that integrates electronic warfare, cyber-warfare, and psychological operations (PSYOPS) into a single



fighting organization will be central to all warfare in the future (Svetoka 2016).³⁸ Intelligence agencies, as well as governmental agencies, are embracing this strategy, especially in the context of problems such as international and domestic terrorism. Instead of thinking of terrorism politically by looking for the root causes of terrorism in history and foreign policy, intelligence agencies have framed terrorism as an informational problem, the solution to which is a regime of ‘total information awareness’ in which citizens are expected to accept and adapt to existential instability by out-innovating and out-surveilling the enemy with better intelligence and information technologies. Yet these instruments extend both the state as arbiter of control as well as the state *of* control.

Larval warfare can proceed without any need for ‘states of exception’ because the tendencies of digital and virtual technologies make it much easier to transcend and circumvent laws, policies and legislation that depend on the primacy of territorial boundaries and physical spaces. Instead of the laminar and striated geo-political design (Bratton 2016)³⁹ of classical state-centered warfare, larval warfare has established itself in the smooth time[s]/space[s] of non-friction by exploiting the fog of uncertainty. Larval warfare exploits the fog of peace in which tactical deployments are not configured by visible military friction. The nebulous and contagious spaces of non-friction or peace are indistinguishable from the terrestrial and striated, merging commerce and surveillance, and turning the forces of peace into micro-agents of larval warfare. Geo-political sovereignty is being eclipsed by an emergent ‘cloud sovereignty’ based on a nebulous *nomos*—that is to say, *data*-based, *platform*-driven and *protocologically* oriented architectures that converge and that subject territorial sovereignty to the *deterritorializing* effects of digitization and platformization, seeking to replace the logic of territorial sovereignty with more technocratic options and/or versions (Pasquale 2017).⁴⁰

Larval warfare does not require spectacular, high-intensity armed conflict, and relies instead on omnidirectional, synchronous, and asymmetrical larval operations. While cyber-warfare seeks to attack information and communication systems (like oil refineries, trains systems, databases, or runaway satellites), larval warfare covertly seeks to disrupt, damage, or modify what a target population knows or thinks it knows about the world around it. Because of its capacities to capture and circulate information at high speeds and low costs, as well as the challenges of tracking the veracity and authenticity of informational sources that arise, techniques of larval warfare can be used to achieve specific military effects. Moreover, ‘noise’ or ‘informational fog’ around a topic can be created in order to distract attention from more strategically important events.

Larval warfare departs from standard territorial warfare which relies on linear, laminar, and hierarchical notions such as fronts, linear battles and face-to-face confrontation. The opacity generated by amplifying uncertainty is deployed and used to tactically to amplify turbulences/flows that dis-/re-orient the normal polarities of power. Rather than the face-to-face contestation of military opponents, this concept of warfare is contextualized within predator–prey behavioral ecologies and takes the form of ‘hunting’ or processes of ‘tracking-down’ in which power-relationships are marked by asymmetry in weapons and in which the enemy is not recognized as an equal but only as prey. This is not the Greek ideal of *agon* or contest; instead, it is the scenario of the hunter and the hunted where each has a different strategy: the hunted always wants to avoid capture, while the hunter always wants to engage; the hunter must confront to win, whereas the hunted must evade to win. The hunted, however, tries to become imperceptible by becoming larval, masked, and inaccessible to the hunter. Predation is invasive and never ethical: the hunter has no regard for borders and claims the right to defy territorial sovereignty. 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 counter-terrorism with the histories of colonialism, slavery, and racism (Browne 2015).⁴¹ Being hunted animalizes the prey and ensures that the hunter almost never has to confront the prey directly, deploying both animal and machine instruments to track, capture and kill in its stead. Because of this mediation and substitution, hunting 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 (Chamayou and Rendall 2012).⁴²

Conclusion: larval warfare and predatory politics

The current politics of surveillance and counter-terrorism thrives on the furious medialities, contagious viralities, and necro-penal economies that aim to exploit uncertainty and that use digital fantasies and virtual theologies as enduring instruments of current and future designs of ‘global governance.’ This could be akin to what Philip Howard calls ‘the new world order of the *pax technica*’:



‘The primary fissures of global politics will be among rival device networks and the competing technology standards and media ecosystems that entrench the internet of things. People will use the internet of things for connective action, especially for those cryptoclans organized over networks of trust and reciprocity established by people and mediated by their devices’ (Howard 2015); ‘[a]s with the Pax Romana, the Pax Britannia, and the Pax Americana, the pax technica is not about peace. Instead, it is about the stability and predictability of political machinations that comes from having such extensively networked devices.’⁴³

‘The pax technica is a political, economic, and cultural arrangement of social institutions and networked devices in which government and industry are tightly bound in mutual defense pacts, design collaborations, standards setting, and data-mining. [...] In the *pax technica*, the core and the periphery are not territorially assigned but socially and technologically constructed. Or, rather, what connects us is not fixed infrastructure like roads and canals, but pervasive devices with connected sensors.’⁴⁴

Larval warfare manipulates and exploits the network-centric tendencies of pax technica. Nets are a tools of hunting; net-centricity is the mode by which larval warfare tracks and pursues its prey. How are we going to deal with this future tendency toward netcentricity, larval warfare, and predatory-style politics? As Michel Foucault has already suggested, the genealogy of power is largely the story of the transformation of power’s automaticity—that is to say, power’s ability to become automatic and autonomous, power’s capacity to govern humans through the exploitation of its machinic properties. Power governs humans by exploiting its own post-human or ‘machinic’ tendencies. The machinic helps the economic converge with the technological and the social: machines advance economic rationality through technological innovation by cutting the costs of human labor by way of non-human decision-making mechanisms. What we are seeing today with netcentricity and larval warfare is a continuation of the development of power’s automaticity, its growing reliance on machinic command and its shedding reliance on a now-outdated atomistic portrait of the human individual. If the normative schema of governing human relations is disintegrating and being replaced by a technical schema of increasingly converging information networks, then what role does the ‘normative’ play? The growing pax technica will ensure that netcentricity not only continues to thrive, but also that corporations, governments, and tech firms will continue to engage in predatory modes of information capture and information manipulation. Societies across the globe are competing to harness the power of information, to be sure,

but these societies themselves are also being harnessed and morphed by the increasing volume, velocity and variety of digital information. While the expansion and adoption of new digital information-and-communication media makes it easier for human beings to become connected beyond physical boundaries and national borders, it also means that everything that we do will be generating data that can be mined and monetized. Information, in the form of data, has become the most important societal resource, and societal infrastructures-norms are being re-engineered to privilege activities that generate continuous digital information-flows; those human activities that do not generate data are downplayed, deprived, eventually defunct because soon there will be little to no part of life that will not be governed and thus subject to computational protocols and digital interfaces.

The rise of internet-centrism and 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 what some are calling a ‘datalogical turn,’ in which humans and their everyday behaviors become ‘datafied’ (Gregory et al. 2015).⁴⁵ While it has arisen historically out of market liberalism, this emergent but domineering form of information-capitalism has gained ascendancy largely through a ‘self-authorized extraction of human experience for others’s profit’ which amounts to ‘unilateral surveillance’ that penetrates and transgresses ‘the boundaries of private human experience’ as Shoshana Zuboff claims.⁴⁶ This emergent logic of accumulation in the networked sphere is characterized by opaque and masked mechanisms of extraction, of commodification, and of control that alienate people from their own bodies and behaviors, all the while generating new markets of prediction and speculation. Not only does surveillance capitalism arise in tandem with the rise of the internet-centrism, but also in tandem with larval warfare. Larval warfare is conducted with the increasing integration of *pax technica* and surveillance capitalism’s hunt for behavioral surplus produced by digital habits.

We are going to have to figure out how to deal with and theorize this kind of warfare that is not conducted by way of armaments and armies, but through the automated medium of an increasingly ubiquitous computational architecture of ‘smart’ networked infrastructures. Within this predatory logic, increasing profits means increasing data-extraction, and one way is to promote data-gluttony—that is, to get people addicted to spending more time online by offering free and improved apps and making them as addictive as possible in hopes of harvesting data from the world’s population, especially the many poor. This is a kind of inhuman digital prospecting in which data-producing humans are literally conceptualized as geological strata—as geologies or ecologies to be mined and exploited for valuable resources. Companies like Google, Amazon, and Facebook are more



than just service providers; they are prospectors and hunters motivated by an underlying rationale: to make money from monitoring everything we do, which requires access to more and more data-rich sources of monetizable information to exploit. And as the trend toward ‘smartification’ continues with the adoption of ubiquitous and ambient computing (e.g., the Internet of Things and Smart Cities), the pressure/incentive to integrate 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’ (which is a term used to describe the process of hydraulic fracturing used in extracting oil which causes earthquakes and other environmental hazards). It might be worth considering the analogy more seriously, and to wonder how we have become subject to fracking—in this case info-fracking. Not only are humans colonizing each other by way of technologies and information, but also in the empire of the digital, all humans are being colonized by a parasitic and hidden logic of warfare as the digital takes hold over the planet and in every sphere of knowledge.

Notes

1. ‘[U]ncertainty speaks to our inability to anticipate what the future holds while risk underlines both our sense of fragility and our constant attempt to reduce it by making those unknowns calculable. Critical IR scholars drawing on the risk-society and global governmentality literatures have therefore turned to these concepts in order to help them make sense of the transformations taking place in the governance of security, migration, development and finance, precisely because these processes of governance appear increasingly concerned with managing risk and uncertainty.’
2. Best, 356.
3. Best, 360.
4. ‘World War III [will be] a guerrilla information war with no division between military and civilian participation’. Marshall McLuhan, ‘Culture Is Our Business,’ 1970, 66.
5. <https://enculturation.net/martial-mcluhan#8>
6. Virilio, *Pure War*, 34.
7. ‘[T]he conduct and outcome of conflicts increasingly depend on information and communications. More than ever before, conflicts revolve around “knowledge” and the use of “soft power.” Adversaries are learning to emphasize “information operations” and “perception management”—that is, media-oriented measures that aim to attract or disorient rather than coerce, and that affect how secure a society, a military, or other actor feels about its knowledge of itself and of its adversaries. Psychological disruption may become as important a goal as physical destruction.’ John Arquilla and David Ronfeldt, ‘The Advent of Netwar (Revisited),’ in *Networks and Netwars: The Future of Terror, Crime, and Militancy*, ed. John Arquilla and David Ronfeldt (Santa Monica, CA: Rand, 2001), 1.
8. See Louise Amoore, *Cloud Ethics: Algorithms and the Attributes of Ourselves and Others* (Durham, London: Duke University Press, 2020), 1, 4. Governments are increasingly profiling individuals and their ordinary behaviors through emerging biometric and algorithmic tools. Amoore cites Simone Browne’s theory of digital epidermalization which argues that biometric algorithms risk damaging the recognition of the body as human, as a fully political entity. Brown considers the ways in which ‘epidermal thinking’ operates in the discourses surrounding certain surveillance practices and her theory focuses on how bodies are shaped with and against biometric technologies. See for example, Simone Brown, ‘Digital Epidermalization: Race, Identity and Biometrics,’ *Critical Sociology*, 2010, Vol.36 (1), 131–150.
9. Kaempf describes how states have historically presided over non-state actors during traditional conflict due to their military capabilities and mass media platforms. However, with the emergence of ubiquitous digital technologies, the current media landscape is characterized by heteropolarity in which there are a range of media actors that alter the traditional relationship between media and war. Most notably, non-state actors and individuals can contest state narratives. Both sides can wage wars between state and non-state actors through modern media platforms.
10. Kaempf, ‘The Mediatisation of War in a Transforming Global Media Landscape,’ 598. Kaempf suggests that because digital technology is so cheap and user-friendly, non-state groups and individuals have been able to break the monopoly that state actors have held over media. Examples include the Zapatistas, Al Qaeda, Hezbollah, and Jamal Islamiyah, who have used various digital media platforms to gain sympathizers, define their strategies and counter opponents’ media campaigns.
11. McCormack and Chatterjee argue that the growing reliance on information and communication technologies blurs the lines in Just War theory between prevention and pre-emption, making preventative wars more and more likely. Unlike conventional war, virtual wars appear ‘risk-free’ but can be considered a covert form of aggression that states will turn to more and more. See Wayne McCormack and Deen Chatterjee, ‘Technology, Information, and Modern Warfare: Challenges and Prospects in the 21st Century’ in Luciano Floridi



- and Mariarosaria Taddeo, *The Ethics of Information Warfare* (Cham, Switzerland: Springer, 2014), 68.
12. Kaempf, 'The Mediatisation of War in a Transforming Global Media Landscape,' 599–600.
 13. Deleuze, *Difference and Repetition*, 257.
 14. Fangyi also suggests that the battlefield has extended to the realm of everyday life by showing that contemporary warfare supports 'sofa warfare' or 'sofa troops' who can engage in warfare from their home environments.
 15. Galeotti suggests that culture is used as a tool of warfare to subtly convince domestic and foreign populations. Larval warfare weaponizes cultural power or soft power because its methods appear ordinary and therefore benign and peaceful.
 16. See for example, Linda Robinson, *Modern Political Warfare: Current Practices and Possible Responses* (Santa Monica, CA: RAND Corporation, 2018), 226–228. Robinson argues that the rise of digital media has led to mass investment in information warfare by political actors. Iran's IRIB is available in 45 countries with five foreign language channels; Russia also invests heavily in news and broadcasting, maintaining RT network and affiliates including RT International, RT America, Rusiya Al-Yaum (Arabic), Actualidad RT (Spanish), etc.). Democratic countries also invest in information warfare, although to a lesser extent. The US maintains the *Voice of America*, and the UK maintains the BBC, whose purpose is to 'represent the UK, its nations, regions and communities.' Non-state actors also invest heavily in information operations. ISIL releases information through several media organizations like its magazines *Dabiq*, *Dar al-Islam*, and *Constantinople*. According to Erbschole, supporters of ISIL use various social media platforms like the former *Twitter* to incite retaliation against the US and other countries. See Michael Erbschole, *Social Media Warfare: Equal Weapons for All* (New York, NY: Auerbach Publications, 2017), 157–159.
 17. Hawkins describes the increasing presence of Chinese 'police stations' in countries worldwide. Such operations have been found to exist in Canada, the UK, Germany, and the Netherlands. The outposts do not seem to be staffed by actual police officers, and their outward purpose is to help Chinese citizens abroad with administrative tasks, like renewing driver's licenses. However, reports suggest that officers have been involved in 'persuade to return' operations that attempt to persuade criminal suspects or dissidents to return to China. Although these police stations do not seem to conduct any explicitly illegal activity, their actions are subversive, covert, and all the while, there is no official declaration of war between China and the countries in which police stations have been found to exist.
 18. See for example, Thomas J. Shattuck, 'The Race to Zero?: China's Poaching of Taiwan's Diplomatic Allies,' *Orbis* 64, no. 2 (Spring 2020): 334–52, <https://doi.org/10.1016/j.orbis.2020.02.003>, 345–348. Also see Chia-Chien Chang and Alan H. Yang, 'Weaponized Interdependence: China's Economic Statecraft and Social Penetration against Taiwan,' *Orbis* 64, no. 2 (Spring 2020): 312–33, <https://doi.org/10.1016/j.orbis.2020.02.002>, 312–313. Chang and Yang show how China uses economic statecraft and social penetration to expand its soft power providing multiple examples of how China uses its non-military resources to increase its power. China can also coerce states to support its actions by offering significant financial assistance, as it did in various African and South American states. Beijing has also launched several global exchange programs to increase Chinese cultural influence abroad, including cultural, educational, professional, journalistic, and think-tank exchanges. These exchanges are intended to widen the base for 'China's Grand External Propaganda.' Although China does not use military weapons or explicitly commit acts of war during its operations, its imperatives are to increase Chinese power globally.
 19. Paul M.A. Linebarger, *Psychological Warfare* (New York, NY: Duel Sloan and Pearce, 1954).
 20. R. Schleifer, *Psychological Warfare in the Arab-Israeli Conflict* (London, UK: Palgrave Macmillan, 2016), 17–19.
 21. '[I]nstead of attacking the military or economic infrastructure, state and non-state actors [...] can access regular streams of online information via social media to influence networked groups within [...] The ease of use and large numbers of active bots and sleeper bots indicate a high likelihood of social media continuing to be used for propaganda, especially as more and more state and non-state organizations realize the impact they can make on an adversary.'
 22. *Ibid.*, 62.
 23. 'It is not so much that we need to understand the digital aspect of modern warfare; rather we need to see that digital warfare is a new way of understanding war in the digital age.'
 24. As Golovchenko et al 2018 suggest in their study of information warfare, neither disinformation nor counter-disinformation is as strongly state-driven as is often assumed in the case of Ukraine: 'citizens are not just the purveyors of government messages,' they are 'curators both of disinformation and counter-disinformation, even in the context of state-sponsored information and



state-controlled media.’ Citizen-driven social media has also challenged the role of traditional mass media’s production and dissemination of news. ‘The digital age facilitates user-generated content and visibility as citizens actively search for, and produce, new information.’ This is not to say that citizens are not subject to state-controlled and pro-government discourses; but they can curate information and generate their own content as well. ‘Information warfare is not what it used to be. In the age of social media, individual citizens can be more influential than states and professional mass media in spreading information.’ ‘We need to adopt new approaches.’

25. Michel De Certeau, *The Practice of Everyday Life*, 31.
26. For a more detailed argument, see Dan Mellamphy and Nandita Biswas Mellamphy. 2014. ‘From the Digital to the Tentacular, or From iPods to Cephalopods: Apps, Traps, and Entrées-without-Exit.’ In *The Imaginary App*, eds. Svitlana Matviyenko and Paul Miller. Boston: MIT Press, 231–249.
27. See Jennifer Taws, *Mission Revolution* (New York: Columbia University Press), 2012, 7–8.
28. ‘There have thus been two transformations in the past ten years, the much-touted and oft-debated RMA and the quieter but arguably more significant elevation of stability operations’ (Taws 2012: 4). ‘Military leaders are touting this as a revolution, and it is playing out in doctrine and in changes to training, force structure, and procurement,’ Taws, *Mission Creep*, 2.
29. ‘Yet some argue that this has been more evolutionary than revolutionary and reflects not a dramatic departure but rational next steps in the military’s development.’ Taws, *Mission Creep*, 5.
30. Christina M. Knopf, Fourth Generation Warfare and the US Military’s Social Media Strategy: Promoting the Academic Conversation; *Air and Space Power Journal*, Volume 3, Issue 4, 2012, 5, 8.
31. See Pearce Higgins, *The Hague Peace Conferences and Other International Conferences concerning the Laws and Uses of War* (Cambridge: Cambridge University Press, 1909). Also see ‘The Geneva Conventions of 1949 and their Additional Protocols’ in *The International Committee of the Red Cross* (ICRC), available at <https://www.ICRC.org/eng/war-and-law/treaties-customary-law/geneva-conventions/overview-geneva-conventions.htm>.
32. Carl von Clausewitz, *On War* (Oxford: Oxford University Press, 2007), 46. Eugenia Kiesling notes that ‘like most military concepts, “fog of war” is normally attributed to Clausewitz, who receives credit for the alliterative “fog and friction”—friction referring to physical impediments to military action, fog to the commander’s lack of clear information. [...] “Friction” is, of course, a central element of Clausewitz’s theory of war; the word appears at least thirteen times in the text and serves an important analytical purpose. [...] Although Clausewitz uses “fog” four times, he never actually uses “fog of war”. [...] That Clausewitz never mentions the fog of war does not mean that he would deny the importance of the ideas subsumed today under the phrase. On the contrary, uncertainty is central to Clausewitz’s argument. In fact, separating fog from friction actually weakens his claims: friction becomes the purely physical hindrances to military action and fog the confusion that arises from absent, misleading, or contradictory intelligence. This distinction is alien both to the text and to the spirit of Clausewitz’s argument. Rejecting the friction-fog dichotomy allows a better understanding of what Clausewitz actually means by friction. Instead of mental fog and physical friction, he guides us to see two different forms of friction. On one hand, friction encompasses the physical difficulties of moving and fighting armies. On the other, he links friction with intangible factors—fear, physical hardship and problems of information that hamper the military commander. In *Military Review*, September–October, 2001, 85, 86–87. Also available at Clausewitz.com/bibl/Kiesling-OnFog.pdf.
33. ‘[T]herefore, it is clear that war should never be thought of as something *autonomous* but always as an *instrument of policy* [...]. War is more than a true chameleon that slightly adapts its characteristics to the given case. As a total phenomenon its dominant tendencies always make war a paradoxical trinity—composed of primordial violence, hatred, and enmity, which are to be regarded as a blind natural force; of the play of chance and probability within which the creative spirit is free to roam; and of its element of subordination, as an instrument of policy, which makes it subject to reason alone’—Clausewitz, 30.
34. See especially the fourth *Geneva Convention* related to the protection of civilians in war (IHL-Databases.ICRC.org/applic/ihl/ihl.nsf/INTRO/380?OpenDocument), in particular Common Article 3 (<https://www.IHL-Databases.ICRC.org/applic/ihl/ihl.nsf/WebART/365–570,006?OpenDocument>).
35. See the *Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations*, E<https://www.GibNet.com/library/un2625.htm>.
36. ‘This principle is reflected in the legal concept of *Ausnahmestand*, or “state of emergency,” as discussed by German jurist Carl Schmitt: ‘The sovereign is he who decides upon the exception. [...] The exception,



which is not codified in the existing legal order, can at best be codified as a case of extreme peril, a danger to the existence of the state, or the like. But it cannot be circumscribed factually and made to conform to a preformed law. It is precisely the exception that makes relevant the subject of sovereignty, that is, the whole question of sovereignty”—Carl Schmitt, *Political Theology, Four Chapters on the Concept of Sovereignty* (Chicago: University of Chicago Press, 2005), 5, 6. For a discussion and critique of this concept see Giorgio Agamben, *State of Exception* (Chicago: University of Chicago Press, 2005).

37. As theorist Jean Baudrillard once proposed: ‘We are at the critical limit where all effects can be reversed and communication vanishes into an excess of communication’—that is, ‘restless circularity and auto-referentiality as integrated network.’
38. David Stupples quoted in Svetoka, S., 2016. Social Media as a Tool of Hybrid Warfare. Riga: NATO Strategic Communications Centre of Excellence, p. 10.
39. For the details of this argument, see Bratton, Benjamin, H. *The Stack: On Software and Sovereignty*. Cambridge MA: MIT Press. 2016.
40. This is what Frank Pasquale and others have called ‘functional sovereignty’: ‘I want to explain how this shift from territorial to functional sovereignty is creating a new digital political economy. Amazon’s rise is instructive. As Lina Khan explains, “the company has positioned itself at the center of e-commerce and now serves as essential infrastructure for a host of other businesses that depend upon it.’ The ‘everything store’ may seem like just another service in the economy—a virtual mall. But when a firm combines tens of millions of customers with a ‘marketing platform, a delivery and logistics network, a payment service, a credit lender, an auction house...a hardware manufacturer, and a leading host of cloud server space,’ as Khan observes, it’s not just another shopping option. Digital political economy helps us understand how platforms accumulate power”—Frank Pasquale, ‘From Territorial to Functional Sovereignty,’ in *Law and Political Economy*. December 6, 2017. Available at LPEblog.org/2017/12/06/From-Territorial-to-Functional-Sovereignty-the-case-of-Amazon.
41. See for example, Simone Browne, *Dark Matters: On the Surveillance of Blackness*. Duke University Press, 2015. <https://doi.org/10.2307/j.ctv11cw89p>.
42. For a more detailed argument see Chamayou, G (2012) *Manhunts: A Philosophical History*. Trans. Rendall S. Princeton, NJ: Princeton University Press.
43. Howard, xx.
44. Howard, 53.
45. Gregory, K, Clough, P, Scannell, J & Haber, B 2015, The datalogical turn. in P Vannini (ed.), *Non-Representational Methodologies: Re-Envisioning Research*. 1 edn, Chapter 9, Routledge Advances in Research Methods, Routledge, pp. 146–164.
46. Shoshana Zuboff, (2019) *Surveillance Capitalism*, 24–5.

Declarations

Conflict of interest On behalf of all authors, the corresponding author states that there is no conflict of interest.

References

- Agamben, Giorgio. 2005. *State of Exception*. Chicago: University of Chicago Press.
- Amoore, Louise. 2020. *Cloud Ethics: Algorithms and the Attributes of Ourselves and Others*. Durham, London: Duke University Press.
- Anderson, C. 2011. Deliberative, Agonistic, and Algorithmic Audiences: Journalism’s Vision of its Public in an Age of Audience Transparency. *International Journal of Communication* 5: 529–547.
- Asmolv, Gregory, and Lorrie LeJeune. 2019. The Effects of Participatory Propaganda: From Socialization to Internalization of Conflicts. *Journal of Design and Science*. <https://doi.org/10.21428/7808da6b.833c9940>.
- Baudrillard, Jean. 2009. The Vanishing Point of Communication. In Jean Baudrillard. *Fatal Theories*. New York: Routledge.
- Best, Jacqueline. 2008. Ambiguity, Uncertainty, and Risk: Rethinking Indeterminacy. *International Political Sociology* 2 (4): 355–374.
- Bratton, Benjamin H. 2016. *The Stack: On Software and Sovereignty*. Cambridge MA: MIT Press.
- Browne, Simone. 2010. Digital Epidermalization: Race, Identity and Biometrics. *Critical Sociology* 36 (1): 131–150.
- Browne, Simone. 2015. *Dark Matters: On Surveillance of Blackness*. Durham: Duke University Press. <https://doi.org/10.2307/j.ctv11cw89p>.
- Chamayou, Grégoire., and Steven Rendall. 2012. *Manhunts: A Philosophical History*. NJ: Princeton University Press.
- Chang, Chia-Chien., and Alan H. Yang. 2020. Weaponized Interdependence: China’s Economic Statecraft and Social Penetration against Taiwan. *Orbis* 64 (2): 312–333. <https://doi.org/10.1016/j.orbis.2020.02.002>.
- Clausewitz, Carl. 2007. *On War*. Oxford: Oxford University Press.
- De Certeau, Michel. 1984. *The Practice of Everyday Life*. Translated by Steven Rendal. Berkley: University of California Press.
- Geneva Convention. 1949. The Geneva Conventions of 1949 and their Additional Protocols. In The International Committee of the Red Cross (ICRC). Available at <https://www.icrc.org/en/doc/war-and-law/treaties-customary-law/geneva-conventions/overview-geneva-conventions.htm>.
- Deleuze, Gilles. 1994. *Difference and Repetition*. Translated by Paul Patton. New York: Columbia University Press.
- Deleuze, Gilles. 2004. *Desert Islands and Other Texts 1953–1974*. Translated by Mike Taormina. Cambridge: MIT Press.
- Erbschole, Michael. 2017. *Social Media Warfare: Equal Weapons for All*. New York, NY: Auerbach Publications.



- Floridi, Luciano, and Mariarosaria Taddeo. 2014. *The Ethics of Information Warfare*. Cham, Switzerland: Springer.
- Galeotti, Mark. 2022. *Weaponisation of Everything: A Field Guide to the New Way of War*. New Haven, CT: 177–179: Yale University Press.
- Golovchenko, Yevgeniy, Mareike Hartmann, and Rebecca Adler-Nissen. 2018. State, media and civil society in the information warfare over Ukraine: citizen curators of digital disinformation. *International Affairs* 94 (5): 975–994. <https://doi.org/10.1093/ia/iiy148>.
- Gregory, K., P. Clough, J. Scannell, and B. Haber. 2015. The data-logical turn. In *Non-Representational Methodologies: Re-Envisioning Research Routledge Advances in Research Methods*, ed. P. Vannini, 146–164. Abingdon-on-Thames: Routledge.
- Hawkins, Amy. “Explainer: China’s Covert Overseas ‘Police Stations.’” *The Guardian*, April 20, 2023. <https://www.theguardian.com/world/2023/apr/20/explainer-chinas-covert-overseas-police-stations>.
- Hesterman, Jennifer L. 2019. “Domestic Terrorism and the Home-grown Threat.” Essay. In *Soft Target Hardening: Protecting People From Attack*, 65–121. New York, NY: Routledge.
- Higgins, Pearce. 1909. *The Hague Peace Conferences and Other International Conferences concerning the Laws and Uses of War*. Cambridge: Cambridge University Press.
- Howard, Philip. 2015. Pax Technica: How the Internet of Things May Set Us Free or Lock Us.
- Jullien, François. 1995. *The Propensity of Things: Towards a History of Efficacy in China*. New York: Zone Books.
- Kaempf, Sebastian. 2013. The Mediatisation of War in a Transforming Global Media Landscape. *Australian Journal of International Affairs* 67 (5): 586–604. <https://doi.org/10.1080/10357718.2013.817527>.
- Kaempf, Sebastian. 2017. “The Ethics of Soft War on Today’s Mediatized Battlespaces”, essay. In *Soft War: The Ethics of Unarmed Conflict*, ed. Michael L. Gross and Tamar Meisels, 168–189. Cambridge, UK: Cambridge University Press.
- Kiesling, Eugenia. 2001. Military Review. September–October. 85–87. Available here: <https://www.clausewitz.com/bibl/Kiesling-OnFog.pdf>.
- Knopf, Christina M. 2012. Fourth Generation Warfare and the US Military’s Social Media Strategy: Promoting the Academic Conversation. *Air and Space Power Journal* 3 (4): 3–35.
- Linebarger, Paul M.A. 1948. Psychological Warfare. Project Gutenberg. <https://www.gutenberg.org/files/48612/48612-h/48612-h.htm>.
- Lu, Isabel Fangyi. 2022. To Subdue the Enemies without Fighting: Chinese State-Sponsored Disinformation as Digital Warfare. *Digital War* 3 (1): 96–106. <https://doi.org/10.1057/s42984-022-00052-7>.
- Macdonald, Michael. Martial McLuhan I: Framing Information Warfare, December 2011, <https://enculturation.net/martial-mcluhan>.
- Mazarr, Michael, Ryan Bauer, Abigail Casey, Sarah Heintz, and Luke Matthews. 2019. *The Emerging Risk of Virtual Societal Warfare: Social Manipulation in a Changing Information Environment*. Santa Monica: RAND Corporation.
- McLuhan, Marshall. 1964. *Understanding Media: The Extensions of Man*. Toronto: McGraw-Hill.
- McLuhan, Marshall. 1967. *Verbi-Coco-Visual Explorations*. New York: Something Else Press.
- McLuhan, Marshall. 1970. *Culture Is Our Business*. New York: Ballantine Books.
- Mellamphy, Dan, and Nandita Biswas Mellamphy. 2014. From the Digital to the Tentacular, or From iPods to Cephalopods: Apps, Traps and Entrées-without-Exist. In *The Imaginary App*, ed. Paul Miller and Svitlana Matvivenko, 231–249. Boston: MIT Press.
- Oates, Sarah. 2020. The easy weaponization of social media: Why profit has trumped security for U.S. companies. *Digital War* 1: 117–122. <https://doi.org/10.1057/s42984-020-00012-z>.
- Pasquale, Frank. 2017. From Territorial to Functional Sovereignty. Law and Political Economy. December. LPEblog.org/2017/12/06/From-Territorial-to-Functional-Sovereignty-the-case-of-Amazon.
- Payne, Kenneth. 2008. Waging Communication War. *Parameters* 38 (2): 37–51.
- Prier, Jarred. 2017. Commanding the Trend: Social Media as Information Warfare. *Strategic Studies Quarterly* 11 (4): 50–85.
- Robinson, Linda. 2018. *Modern Political Warfare: Current Practices and Possible Responses*, 226–228. Santa Monica: RAND Corporation.
- Schmitt, Carl. 2005. *Political Theology, Four Chapters on the Concept of Sovereignty*. Chicago: University of Chicago Press.
- Shattuck, Thomas J. 2020. The Race to Zero?: China’s Poaching of Taiwan’s Diplomatic Allies. *Orbis* 64 (2): 334–352. <https://doi.org/10.1016/j.orbis.2020.02.003>.
- Svetoka, S. 2016. Social Media as a Tool of Hybrid Warfare. Riga: NATO Strategic Communications Centre of Excellence.
- Taws, Jennifer. 2012. *Mission Revolution*. New York: Columbia University Press.
- “Under the Radar; War and Social Media.” *The Economist*, May 14, 2022. link.gale.com/apps/doc/A703415898/AONE?u=lond95336&sid=bookmark-AONE&xid=41c0aae5.
- Virilio, Paul, and Sylvère Lotringer. 2008. *Pure War*. Cambridge: MIT Press.
- Winter, Yves. 2011. The Asymmetric War Discourse and Its Moral Economies: A Critique. *International Theory* 3 (3): 488–514.
- Zuboff, Shoshana. 2019. *The Age of Surveillance Capitalism*. New York: Hachette Book Group.
- Zuckerman, E. 2018. Four Problems For News and Democracy. Medium.com. <https://medium.com/trust-media-and-democracy/we-know-the-news-is-in-crisis-5d1c4fbf7691>

Springer Nature or its licensor (e.g. a society or other partner) holds exclusive rights to this article under a publishing agreement with the author(s) or other rightsholder(s); author self-archiving of the accepted manuscript version of this article is solely governed by the terms of such publishing agreement and applicable law.

Biswas Mellamphy Nandita is Associate Professor in the faculty of Social Sciences, and former Undergraduate Chair (2021-4) of Political Science at Western University in London, Ontario, Canada. She is an affiliate in Gender, Sexuality, and Women’s Studies, as well as core faculty in the Centre for the Study of Theory and Criticism and founding Director of The Electro-Governance research group (EGG) at Western University. She has served as Assistant Editor of the Canadian Journal of Political Science (2020-23) and is currently an Associate Editor at Interconnections: Journal of Posthumanism. Her areas of study are situated at the intersection of Political Theory, Continental Philosophy and Communications/Media Studies.

