Book Review

Review of Dyer-Witheford, Nick, and Svitlana Matviyenko. 2019. *Cyberwar and Revolution: Digital Subterfuge in Global Capitalism*. Minneapolis: University of Minnesota Press. 232 pp. Paper. US\$24.95. ISBN: 9781517904111.

Steve Bailey

York University, Canada
bailey@yorku.ca

Nick Dyer-Witheford and Svitlana Matviyenko's *Cyberwar and Revolution: Digital Subterfuge in Global Capitalism* makes a significant contribution to the literature on digitality and geopolitics. This remarkably compact book reflects a doubly ambitious project: to provide a theoretical approach fusing Marxism and psychoanalysis in the service of both an analysis of contemporary "cyberwar" and also to provide some practical strategies for resistance and perhaps revolution within the context of digital capitalism. The centrality of psychoanalysis for this effort is noteworthy given the relative paucity of psychoanalytic perspectives in theorizing questions of digital and algorithmic culture (the work of André Nusselder is an important exception here as well as a handful of authors mentioned in this book). While Slavoj Žižek and the associated Ljubljana School of psychoanalytic thought have attempted their own, deeply Hegelian–Marxist–psychoanalytic perspective and there is surely no shortage of Lacanian cultural theory, often cryptic and sometimes cultic, the critical utility of Lacanianism for an investigation into a digital present has never been explored with such nuance and verve. The turn in the final chapter toward strategizing a radical Left response to cyberwar is similarly innovative, taking the Marxist injunction to praxis seriously and in doing so refusing an exhausted defeatism that is tempting in the face of a monstrous but often elusive socio-technical foe.

The authors begin with an introduction that provides a solid historical context for the work following, as well as establishing a "maximalist" definition of cyberwar, one capable of accounting for a broad array of phenomena, including government-sanctioned cyber-attacks but also a range of hacking practices, digital insurgencies, and surveillance activities. In the first chapter, Marxist aspects of the theoretical blend described above are demonstrated through extended analyses of several crucial global instances of cyberwar, including the ongoing conflicts between the People's Republic of China and the United States and the concurrent and certainly newsworthy struggles between Russia and the US, particularly in regard to election interference and misinformation campaigns. However, in line with the widened understanding of cyberwar, the authors also discuss a range of other instances of militarized digital practices, including the vast network associated with the alt-right and white supremacy in the US, as well as attacks by the "Cyber Caliphate" and recruiting efforts associated with the Islamic State in Iraq and Syria (ISIS). The analysis of the last, while brief, is of particular value in illustrating the degradation of Marxist revolutionary spirit into fundamentalism and sectarianism as well as its position in a "dialectic of disaster" (a term the authors borrow from Fredric Jameson) with neo-liberalism. The chapter also provides some valuable reflection on the largely failed radical struggles associated with revolutionary actions in Egypt and Ukraine, as well as a wider range of "occupy" movements; the authors link the speed with which such movements rose and fell

Bailey, Steve. 2019. Review of Dyer-Witheford and Matviyenko's *Cyberwar and Revolution: Digital Subterfuge in Global Capitalism*. *Surveillance & Society* 17(5): 757-759.

<https://ojs.library.queensu.ca/index.php/surveillance-and-society/index> | ISSN: 1477-7487

© The author(s), 2019 | Licensed to the Surveillance Studies Network under a [Creative Commons Attribution Non-Commercial No Derivatives license](#)

with the vertiginous pace of digital culture as well as its unstable, viral character. The analysis thus provides a cautionary note for any irrational exuberance regarding the liberatory possibilities of digital praxis yet does not sink into a luddite refusal of all radical potential therein, recognizing, for example, the “complex diagram” required to chart contemporary cyberwar, with vertical and horizontal axes and a wide array of vectors of resistance and state dominance.

While Chapter 1 provides the larger geo-political landscape in reference to cyberwar and both situates and analyzes it through a Marxist lens, the second chapter, “Cyberwar’s Subjects,” takes up the “psychosocial pathologies of cyberwar,” as the authors put it. Starting with a revisitation of Althusserian ideology theory and particularly processes of interpellation, the authors launch a thorough theoretical and empirical investigation into the particular forms of social subjectivity produced by and associated with cyberwar. The question of interpellation is crucial for the authors given their particular interest in the “cyberwar apparatus” (playing off of Althusser’s famous ideological and repressive state apparatuses) and the deployment of digital technology in the production of compliant subjects. Intriguingly, the authors consider trolling as itself a practice of interpellation, a useful corrective to a view of such malignant practices as a kind of purposeless, purely affective aggression. Rather, the authors argue, they construct an enemy that provides the grounds for amplifying rage and producing a kind of negative solidarity. While not mentioned by the authors, this line of argument recalls both Erich Fromm’s analysis of the centrality of disgust in authoritarian attitude formation and Kenneth Burke’s discussion of the importance of a “powerful” scapegoat for producing collective political formations. Of course, such interpellation is significantly impacted by the importance of automated functions and the “internet of things,” as the authors discuss in relation to the “automatic subject.” The role of the non-human actor in processes of interpellation is surely important for the future trajectory of critical work on digital culture so its appearance here is noteworthy.

While much of the preceding remains within an admittedly expanded Althusserian model, much of what follows in Chapter 2 takes on a range of issues more closely related to Freudian and by extension Lacanian paradigms, as in the discussions of the unconscious and dreams as they related to the titular concerns. Here, the authors provide an analysis of contemporary developments that reinvigorates classical psychoanalytic concepts, as in the discussion of the internet’s often opaque structures and confusing and erratic practices and their role in producing the “dazed and confused” subject of cyberwar. For example, the “double falsification” of compounding fake news processes is analyzed quite deftly as a manifestation of this spiraling mystification. Dreams, similarly, are recontextualized and to a degree retheorized by playing with filmmaker Werner Herzog’s provocative cinematic transformation of Carl von Clausewitz’s claim that “Sometimes war dreams of itself” into the question “Does the internet dream of itself?” and considering what lies beneath the sunny dreams of digital peace and harmony. While theoretical insights are distributed throughout *Cyberwar and Revolution*, for this reader, Chapter 2 constitutes the centerpiece of the book’s theoretical innovation.

As noted, though, theoretical synthesis is only the first aspect of the book’s larger contribution and the second, a consideration of radical political strategy in conditions of cyberwar, is the subject of the final chapter. Rather bluntly titled “What is to be Done” (echoing Lenin with at least some irony), the chapter moves through “tactical,” “operational,” and “strategic” issues in formulating a radical response to the capitalist cyberwar machine. With regard to the first, there is a discussion of two prominent modes of digital resistance, hacking and anti-surveillance practices; while both have been the source of significant popular and academic interest, their placement with the Marxist–Freudian framework gives the analysis the wider conceptual horizon associated with the Marxist tradition and, conversely, some of the subjective depth associated with the Freudian and Lacanian schools. The reflections on tactics suitable for resisting dominant cyber-forces are quite measured and might strike some readers as timid or even excessively gloomy. However, given the extensive documentation of the profound power of state-sponsored cyberwar activities for both geopolitical action and constituting subjects, a sudden turn to an overexcited “optimism of the will” would be intellectually suspect. Subsequent sections in the chapter work through a range of possible paths for action, including crucial but less commonly discussed issues such as political party formation, the question of the vertical versus horizontal organization of resistance movements, and connections to other

struggles within contemporary geopolitics. The Rojava Revolution in Syria is explored in some detail as a possible prototype (albeit with significant limits) for revolutionary struggle, and near the end of the chapter a model of “corporeal care” is provided as a longer-term strategic response to cyberwar. The chapter then concludes with a coda exploring the precarious place of the university in conditions of cyberwar, a likely concern for most if not all readers of the book.

Cyberwar and Revolution: Digital Subterfuge in Global Capitalism, then, is a major contribution to the literature on the intersection of digital culture, neoliberal capitalism, and political resistance, offering both theoretical and conceptual advances and thoughtful advice regarding practices of resistance. In its blend of Marxist and psychoanalytic thought and in the diversity of examples and breadth of its historical global reach, Dyer-Witheford and Matviyenko provide a keen diagnosis of contemporary conditions, one likely to interest a wide array of readers across numerous academic disciplines.