Journal of Strategic Security

Volume 13 | Number 1 Article 7

Cyberwar and Revolution: Digital Subterfuge in Global Capitalism. By Nick Dyer-Witheford and Svitlana Matviyenko. Minneapolis, MN: University of Minnesota Press, 2019.

Mark Peters II
USAF, Retired

pp. 131-134

Recommended Citation
Peters, Mark II. "Cyberwar and Revolution: Digital Subterfuge in Global Capitalism. By Nick Dyer-Witheford and Svitlana Matviyenko. Minneapolis, MN: University of Minnesota Press, 2019.." *Journal of Strategic Security* 13, no. 1 (2020) : 131-134.
DOI: https://doi.org/10.5038/1944-0472.13.1.1807
Available at: https://digitalcommons.usf.edu/jss/vol13/iss1/7

Cyberwar and Revolution: Digital Subterfuge in Global Capitalism. By Nick Dyer-Witheford and Svitlana Matviyenko. Minneapolis, MN: University of Minnesota Press, 2019.

***Cyberwar and Revolution: Digital Subterfuge in Global Capitalism*. By Nick Dyer-Witheford and Svitlana Matviyenko. Minneapolis, MN: University of Minnesota Press, 2019. ISBN 978-1-5179-0411-1. Notes. Sources cited. Index. Pp. 228. $24.95.**

Many excellent cyberwar texts today begin and end their explorations with either state-based actions or non-state terrorism. This superb text, *Cyberwar and Revolution: Digital Subterfuge in Global Capitalism* by Dyer-Witheford and Matviyenko instead investigates how Marxist ideology interprets cyber warfare's expressions within the Global Cyber Commons (GCC). Starting with an attributed Leon Trotsky aphorism: "You may not be interested in war, but war is interested in you," the text first considers war as cyber war in the context of that quote. This basis allows an exploration of theoretical modern Marxism, applies tenets to historical cyber actions, and recommends future solutions. Each case contains numerous relevant references and clearly translates theoretical perspectives into outcomes. Throughout the text, a central theme evaluates digitally distributed capital as distinct from the more traditional material factory triggers typically associated with the Marxist dialectic struggle. This book expertly advances a topic government and private policy experts may have studied previously, but this alternative perspective should be in the must read column.

Cyberwar and Revolution describes how GCC influences fundamentally change relationships between capital and labor when viewed with the Marxist dialectic. A New Cold War highlights the conflict between the first Cold War's capitalist winners and the post-socialist losers' struggle to meet modern standards. Some losing venues, such as Iraq, Syria, and the Ukraine suffer from cyberwar's emergence and continued physical conflicts, which increase struggles for a traditional labor class. Creating state wealth channels through cyber capital should allow labor forces to express revolutionary ideology through resources like WikiLeaks, where Edward Snowden's revelations revealed state-based oppression. These aspects enhance an overall cyberwar viewpoint that transitions from a state tool to a model for future insurgency and espionage options.

The text's exposition begins by reviewing several basic assumptions about Marxist revolution and cyberwar applications. When conflict happens, the

authors assume two different pathways exist: a political revolution against capital, and then the technological revolution internal to capital. These two broad categories succeed through four different conflict methods: class war, state war, revolutionary war, and technological revolution. Each item links to historic examples illustrating how they conform to the overall theoretical architecture. Class cyberwar starts with the 1990s dot-com meltdown before changing to Web 2.0 models and global enablement through the GCC. The broader the technological empowerment base, the more the authors anticipate seeing labor forces employ cyberwar models, with early adopters including the Arab Spring and Occupy movements. State cyberwar explores traditional conflict when the U.S., China, and Russia cyber activities further their goals through cyber efforts against their own citizens like China's Great Firewall, or other states like Stuxnet. Revolutionary war models the historical email recruitment used by Zapista groups in Mexico versus ISIS and Al Qaeda's more modern marketing techniques. Technological revolution refers to situations where capital creates new means to wage war that devalue the worker, such as when cybernetics sciences emerged following WWII to merge man and machine processes. Carefully building the overall framework suggesting how labor may challenge capital forces allows a unique exploration of how cyberwars affect those entangled by the global web.

The middle chapter describes Lacan's theoretical Marxist connections and how symbolic imperatives incorporate individuals into a singular gestalt. Mobile phones, social networks, and all-encompassing digital networks are the basis for labor acquiring more cyberwar powers and simultaneously becoming more vulnerable to capitalist machinations. Two unusual comparisons on this topic appear, with the first suggesting that cyberwar equates with the French *Levee en Masse* practice to impress every available person to conflict duties. Botnets attempt to recruit available resources and the state's ability to forcibly impress otherwise peaceful computers through these measures seems significant. The other unusual topic addresses gender in cyberwar, and how a traditionally masculine activity such as war takes on feminine characteristics. The final item highlights cyberwar's unconscious and automatic nature for the majority of society due to the required interface necessary for any perception. Cyber conflicts occur beneath view with whole campaigns launched through Twitter and Netflix while digital miners harvest Bitcoin behind free game options. Cyberwar ingests all those who enter the

https://digitalcommons.usf.edu/jss/vol13/iss1/7
DOI: https://doi.org/10.5038/1944-0472.13.1.1807

domain, regardless of personal awareness, and the authors point out how this becomes simply another way in which capital forces use labor resources.

This concise volume's final chapter offers two capitalist cyber war alternatives: first, anti-surveillance campaigns, and second, the hack-back. Anti-surveillance methods address Snowden and Wiki-leaks, suggesting one must recognize that state surveillance is occurring before any counter possibilities exist. Hacking back suggests three levels where labor may generate revolutionary change: operational, organizational, and strategic. Operational change between individual and state appears as fake news, cyber-crime, and dirty wars through covert actions or drone attacks. Organizational struggles play out between state functions like the NSA and those adopting opposite views like the Electronic Freedom Foundation. Finally, large state strategic conflicts may create significant difficulties for labor elements caught underfoot. Three further strategic conflict options appear: worldwide network degradation, hybrid physical/netwar, or cyber "nuclear war," which eliminates networks entirely. The authors adequately sum up their concerns and offer several worthwhile alternatives for how the Marxist dialectic may progress across the GCC.

Excellently written and well-documented, the largest concern for reading *Cyberwar and Revolution* may be that the audience lacks the proper background to consider the full ramifications suggested. Most cyberwar texts adopt a state versus state perspective rather than considering how those actions affect the individual user in terms of collateral actions. Those traditional works also fail to consider the Marxist perspective of how those smaller participants might eventually change the nature of the state. On occasion, one sees interpretations suggesting collateral impacts, but this text goes further by analyzing how those massive actions may empower the individual towards revolutionary change. For improvements, the book could have used several charts or graphs to help illustrate the subject matter at different points. Additionally, the text suffers slightly from overabundant technical references to Marxist theories which may not be immediately apparent to the casual reader.

Interesting, engaging, and well worth anyone's time, this is one of the most original cyber strategy books available. *Cyberwar and Revolution: Digital*

Subterfuge in Global Capitalism offers a creative cyber policy approach based on the Marxist lens. The text was well documented, thoroughly sourced, and coherently argued. A quick read, the authors still packed in a significant amount of information. Their arguments progress from cyberwar's inadvertent effects on the average netizen, to GCC characteristics shaping conflict, and then finally how states may continue to trample ordinary laborers unless a revolutionary challenge emerges. The clear arguments and detailed references meant there is very little not to like about this book. The biggest objection, as mentioned above, emerges from the Marxist fundamentalist base which tends heavily to slanted language and specific terms. Understanding the various GCC player's motivation is critically important to security experts and Dyer-Witheford and Matviyenko thoroughly explore this intriguing area. The book is recommended for anyone engaged in political strategy for fun or profit, as well as those involved in cyber security.

Dr. Mark T. Peters II, USAF, Retired

https://digitalcommons.usf.edu/jss/vol13/iss1/7
DOI: https://doi.org/10.5038/1944-0472.13.1.1807