International Journal of Communication 13(2019), Book Review 5137–5139 1932–8036/2019BKR0009

Justin Joque, **Deconstruction Machines: Writing in the Age of Cyberwar**, Minneapolis, MN: University of Minnesota Press, 2018, 248 pp., $26.75 (paperback).

Reviewed by
Brett van Niekerk
University of KwaZulu-Natal, South Africa

Justin Joque's ***Deconstruction Machines: Writing in the Age of Cyberwar*** is a thought-provoking philosophical view of the threat of cyberwar. The book is topical, in a time where nations attempt to grapple with cyberspace as a possible instrument of power for both state and nonstate actors. The fields of cybersecurity and cyberwar often are mistakenly considered as purely technical; however, there are a number of strategic aspects that are still being grappled with, for example, the applicability of international humanitarian law to cyber operations covered by Schmitt (2013, 2017) in the two *Tallinn Manuals*. Despite the increasing attention being given to the concept of cyberwar, Joque's perspective is unique in its philosophical stance. As the title suggests, the analysis of cyberwar throughout the book is largely based upon Jacques Derrida's perspectives of deconstruction, which is a method to comprehend the linkages between text and its meaning.

Five chapters (including the introduction) are named after common cyberattack methodologies, but the conclusion's name implies a weakness: "Firmware Vulnerabilities." These, however, do not necessarily correspond to the types of attacks that are discussed in the chapter. In forming his analysis throughout the book, Joque draws from some of the original thought pieces predicting cyberwar, such as Arquilla and Ronfeldt's *Cyberwar Is Coming!* (1993) and *Networks and Netwars: The Future of Terror, Crime, and Militancy* (2001) and more contemporary works by authors with experience dealing with cyberwar since it has evolved, such as Carr's *Inside Cyber Warfare* (2012).

The author states that the book was written before the alleged Russian interference in the 2016 U.S. presidential elections (p. 28); therefore, some excellent examples such as the WannaCry and NotPetya outbreaks of 2017 are not covered. Some broader (and more modern) discourses of how to define cyberwar may have provided additional discussion points, and may have prevented some contentious statements like, "early outbreaks of cyberwar, such as a series of Russian attacks on Estonia in 2007" (p. 1) and "it increasingly appears as though Russia waged a multipronged cyberwar to undermine the election process and the solidity of U.S. institutions" (p. 28). These two statements define those acts as cyberwar; however, this is strongly disputed, and it appears that they will not be classed as an act of war based on legal definitions as outlined by Schmitt (2013, 2017). He does concede that the concept of cyberwar resides "between these two poles as it hides in the theoretical space between war and nonwar" (p. 8).

The introduction, "Root Kit," discusses the definition, or lack of a widely accepted one, for cyberwar. The subsequent historical overview of confirmed and purported incidents is one that most avid readers and scholars of cybersecurity would be familiar with; however, it forms a good overview for readers who are new to the topic. The intersections and contrasts of cyberwar and media wars are discussed with particular reference to the alleged North Korean cyberattack on Sony. The role and function of computing technology in society are addressed, drawing from a number of theorists and philosophers. This leads to the author's proposition of computer programs (the underlying code) as text designed to take textual input, interpret its "meaning," and provide textual output. This is where the Derridean and Deleuzian philosophies come to the fore, where Joque argues that Derrida's concept of undecideability indicates a new type of violence is emerging because of cyberwar. He then postulates that cyberwar is not just a strategic evolution due to advancements in technology, but a philosophical one as well.

The first chapter, "Buffer Overflow," provides a focus on the concepts of space and time, and how these may change due to networked societies. Joque proposes that the concept of geographical space becomes less relevant, while new concepts of space based on information flow arise. Various discussions on space and time, such as the "strategic value of slowness" (p. 43) and the concept of state sovereignty related to cyberwar, lead on to the concept of space internal to systems, based on the text (code and information stored in databases) that make up these systems. The rhizomatic nature of cyberwar is introduced; however, existing academic research on the topic, for example, Huhtinen, Hirvela, and Kangasmaa (2014), are not considered in-depth. The chapter concludes that cyberwar is a new form of "high-dimensional warfare" because of the number of spaces and time considerations in which it operates.

A deeper consideration of cyberwar and computing systems as a form of writing, and the need to redefine deconstruction is the focus of the second chapter, "Injection Attack." The concept or catastrophe is redefined for the digital age, where the destruction of the bits and bytes destroys its meaning. This chapter delves deeper into Derrida's concept of military deconstruction and catastrophe, evolving it from the nuclear scenario to one for the digital era. The comparison of nuclear war and cyberwar is common; however, in the context of deterrence and attribution, the deconstruction perspective provides a fresh look at this relationship. Geospatiality is again considered, this time through the lens of deconstruction. This leads to a discussion on the future of identity and authentication, where aspects of public-key cryptography are considered. The chapter concludes with a discussion on "a global situation confronted with a horrifying mutually assured deconstruction" (p. 109).

The third chapter, "Distributed Denial of Service," delves further into the concept of sovereignty in cyberspace, as is alluded to in the first chapter. Both the sovereignty of the individual and the sovereignty of the state are considered. Sovereignty is assessed through the lens of the politics of cryptography, in particular a dual-nature of cryptography as a tool for liberation as well as a tool for control. In a similar vein, the linkages between transparency and antigovernmentality are considered. In contrast to previous chapters where the philosophies of Derrida dominated, Deleuzian concepts come through strongly, and the views of Julian Assange (WikiLeaks) are noticeably interwoven with the discussion.

The discussion evolves into one on the enablement of citizens to oppose state power through digital technology in the fourth chapter, "Spear Phishing." The activities of the hacktivist group Anonymous, as would be expected, appears early on in the discussion, along with the concept of data leaks in politics in "transparency and the politics of knowledge" (p. 154). Derrida's philosophies make a return to be considered in this context, and the chapter concludes by discussing the ability of networked subjects to rebel against the state as a cyberwar.

The conclusion, "Firmware Vulnerabilities," includes the activities of a sophisticated threat actor known as the Equation Group with particular reference to their attacks that exploited the firmware (very low-level code used to control machines) of computer hard drives. The thematic concepts covered in the previous chapters are coalesced into a strong discussion on deconstruction, and how cyberwar is a form of writing and logic attacking its own underlying writing and logic. Throughout the book there is an element implying that cyberwar will, in essence, prevent itself due to its own nature, following Rid (2013), whose views were acknowledged in the introduction.

A number of important concepts and examples related to cyberwar were absent in the book. While there was some history on the concept of cyberwar, strongly related concepts such as command and control warfare, information warfare, electronic warfare, or revolution in military affairs would give the concept of cyberwarfare more context and focus throughout the book. None of the military strategists advocating cyberwarfare or doctrine documents were considered. The Russian involvement in Ukraine and the annexation of Crimea is an excellent example of how cyberwar concepts can be used as part of a bigger picture.

Despite the possible omissions mentioned above, *Deconstruction Machines: Writing in the Age of Cyberwar* remains a thought-provoking work. It provides a uniquely philosophical discussion not only on cyberwar but also on the underlying structure of computers and the Internet, which for some are a constant companion.

References

Arquilla, J., & Ronfeldt, D. (1993). Cyberwar is coming! *Comparative Strategy, 12*(2), 141–165.

Arquilla, J., & Ronfeldt, D. (2001). *Networks and netwars: The future of terror, crime, and militancy*. Santa Monica, CA: RAND Corporation.

Carr, J. (2012). *Inside cyber warfare* (2nd ed.). Sebastopol, CA: O'Reilly.

Huhtinen, A., Hirvela, A., & Kangasmaa, T. (2014). The opportunities of national cyber strategy and social media in the rhizome networks. *International Journal of Cyber Warfare and Terrorism, 4*(2), 22–34.

Rid, T. (2013). *Cyberwar will not take place*. Oxford, UK: Oxford University Press.

Schmitt, M. N. (2013). *Tallinn manual: On the international law applicable to cyber warfare*. Cambridge, UK: Cambridge University Press.

Schmitt, M. N. (2017). *Tallinn manual 2.0: On the international law applicable to cyber operations*. Cambridge, UK: Cambridge University Press.