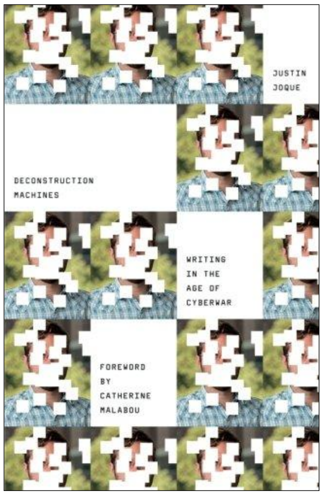
International Journal of Communication 13(2019), Book Review 5579–5582 1932–8036/2019BKR0009

Justin Joque, **Deconstruction Machines: Writing in the Age of Cyberwar**, Minneapolis, MN: University of Minnesota Press, 2018, 248 pp., $27.00 (paperback).

Reviewed by
Luca Follis
Lancaster University, UK



Cyberwar operates in the space between the known and the unknown. It has an intractable legal status (is it an act of war or not?), but it also defies factual confirmation (was this an actual attack or a bug in computer code?), to say nothing of the problems with its attribution (was this an incursion by a nation-state, a criminal gang, or some other third party?). The geopolitical significance of this new modality of conflict has been well charted by a number of recent books on the subject (e.g., Buchanan, 2017; Kello, 2017; Rid, 2013). Yet ***Deconstruction Machines: Writing in the Age of Cyberwar*** argues that these surface tensions are not just indicative of how networked technologies transform the strategic capacities of nation states. Rather, they are reflective of a deeper, ontological insecurity in computer code and the networked computer systems it underwrites.

Justin Joque argues that cyberwar is a mode of writing that subverts the logical and linguistic systems that underpin computer programs from within; it militarizes deconstruction and brings the battle deep into the constituent fabric of everyday life. It is not just that the depth of code (its complexity, context, and piecemeal assemblage over decades by multiple writers) necessarily defies authorial intent, exposes it to vulnerability, and eludes complete control. Not even that the discovery and use of a vulnerability in it would seemingly confirm that someone, at some point in the future, will use it again. Rather that, like any text or form of writing, computer code always carries within it a sort of "autodeconstruction immanent to the logic of the program" (p. 76). In other words, cyberwar's militarized deconstruction inevitably sets in motion a set of counterforces and a moment when that very same force will be leveled against itself.

As might be expected, the discussion draws heavily on the work of Derrida, Deleuze, Foucault, Lacan, and Malabou, illustrating how their writings elucidate what is at stake in cyberwar while at the same time showing how cyberwar confirms the insights of postmodern theory. It is a theoretically demanding (and at times circuitously longwinded) read, which nonetheless manages to couple stimulating conceptual insight with a detailed technical overview of key themes (e.g., cryptography, cybernetics) and events in the history of cybersecurity.

According to Jocque, cyberwar operates at multiple levels: It targets strategic nodes based upon when and where they are located within networks, but also seeks to actively exploit the full scope of global data (and physical) flows. Chapter 1 applies this insight to a range of familiar events. The early Russian excursion into U.S. computer networks in the late nineties (Moonlight Maze) and Russia's cyber campaign against Estonia are situated alongside Stuxnet (which infected Iran's nuclear processing facilities) and Operation Orchard—where an Israeli fighter jet bombed a Syrian nuclear installation and escaped undetected because of a “backdoor” in the computer chips running the radar system. These examples do more than emphasize the insecurity of the code, networks, and global supply chains technology relies on; they identify the increasingly varied and heterogeneous set of domains and spaces where cyberwar is waged.

Channeling Deleuze and Guattari, *Deconstruction Machines* argues that cyberwar blocks (striates) the unimpeded flow of data by disconnecting its targets from global networks (e.g., Estonia), but it also smooths network pathways and “frees” data flows to optimize the exfiltration of sensitive information (e.g., Moonlight Maze). Finally, it also reconfigures how space, location, and time function in networks by turning them into attack vectors. For example, even speed (often understood in terms of a near-instant attack capability) gains strategic value in terms of its differentials: The Stuxnet virus was partially successful in evading detection and remaining localized in Iran because of its very slow infection rate. Joque’s point here is that we are very far from the terrain of war as conventionally understood. Instead, we are confronted with a high-dimensional battlefront, which manifests itself through an open and expansive set of potential conflicts where attacks unfold at multiple levels (technological, temporal, geographic, metaphysical) sometimes contemporaneously.

Chapter 2 focuses on cyberwar as a form of writing that valorizes certain texts and meanings while working to undermine and deconstruct others. For Joque, this form of deconstruction is an attack not just on computer systems but a more expansive threat leveled at all symbolic systems. Cyberwar moves between metaphysical, communicational, social, and physical systems, operating across networks and seeking to rewrite and undermine them from within. Here Joque draws on the War Machine model to argue that, as it is played out across these heterogeneous spaces and systems, deconstruction works to uncage hierarchies and unleash meaning at the same time as it corrupts, destroys, and infects those very same systems (on whose stability our own existence increasingly depends).

Chapter 3 provides an oblique take on sovereignty. Cyberwar functions outside of the traditional time and space of war, and it targets the macroscopic and microscopic facets of our technological systems. Because of this, *Deconstruction Machines* argues that we need to understand cyberwar not just as a conflict between states (as the International Relations literature would argue) but also as a conflict between states and their populations. And here once again we are confronted with the tension between cyberwar’s drive to exploit the connections and interactions that emerge in the informational and physical infrastructure of global flows and the very complexity of these systems, which provides both the basis of their insecurity and the gradient of resistance to state control.

He illustrates this point with a brief history of the struggles over public access to cryptography and the multidecade attempts by the National Security Agency to dominate the process. Between World War II and the 1970s, the U.S. government (through the NSA) was able to maintain a high degree of control over information and knowledge surrounding advanced ciphers, yet this gradually shifted as public and university access to computers grew and the computer industry began adopting cryptography in their products. Ultimately, over the space of thirty years, the domination of cryptography by a set of secret government systems gave way to a new mathematically driven public science open to all. The point here is that despite the NSA’s attempts to keep the technology they invented secret, as well as their attempts to engineer within subsequent standards backdoor access, the sheer complexity of the cryptographic systems; the network flows they were meant to encrypt; and the broad range of technical, scientific and economic interests that coalesced around the project worked against government control.

In the struggles over cryptography, we see a familiar dynamic play out: The state develops a technology of control that it then seeks to undermine and disrupt because it becomes a vehicle for others to resist state control and even turn against the state (e.g., The Onion Router). According to Joque, this is because cryptography is positioned between the War Machine and the state; it is necessary for any semblance of digital citizenship and grass roots organization, but it is also fundamental to any notion of cyber security. The above scenario reframes the aporias of sovereignty for the digital age: "The whole requires cryptography to function in a digital world, but the individual's access to cryptography threatens the whole" (p. 124).

Chapter 4 considers the possibility for resistance and its subversion within this new world of conflict. This is perhaps the most engaging section of the book, as it convincingly brings together the theoretical strands and insights of previous chapters. According to Joque, the problem of agency under the specter of cyber war is twofold. There is the very real possibility of cooption and infection by the state war machine (cyberwar also targets the individual as an object of control), but there is also the more elusive realization that the sheer complexity of the systems and temporalities one is trying to influence and act within defy a straightforward and linear intentionality. Joque illustrates this point with the example of Anonymous's various operations and contrasts this with the eventual revelation that the Anonymous and LulzSec-affiliated hacker, Sabu (Hector Xavier Monsegur), was an FBI informant and operative.

What is striking in Joque's retelling of this affair is not that Sabu chose to become a government informant once he was arrested by authorities—after all this is a relatively common, even expectable outcome. What is striking rather is that under the FBI's direction, Sabu and his collaborators hacked into scores of foreign government websites in countries like Turkey, Brazil, and Syria; they broke into the private intelligence firm Stratfor, exfiltrated the credit card information of its subscribers, downloaded their email spools (which were subsequently passed to WikiLeaks), and wiped their servers.

Moreover, Sabu's tweets and public pronouncements were brazen and insurrectionary, reveling in their outlaw status and open defiance of the state. In this scenario, it is unclear and difficult to determine who is coopted by who (Sabu? The FBI? Anonymous?), who is directing whom, and who ultimately realizes their objectives? Perhaps fittingly, despite the oft-stated capacity of networked technology to disrupt existent power relations, it also invariably scrambles the logic and trajectory of resistance. As Joque puts it:

> If the state is so quick to turn against itself and its allies, appropriating political resistance to a variety of still unclear ends, it becomes increasingly complicated to resist such a system, let alone to evaluate the efficacy of any resistance. (p. 154)

References

Buchanan, B. (2017). *The cybersecurity dilemma: Hacking, trust and fear between nations.* Oxford, UK: Oxford University Press.

Kello, L. (2017). *The virtual weapon and international order*. New Haven, CT: Yale University Press.

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