new media & society

London, Thousand Oaks, CA and New Delhi
Vol7(5):595–597 [DOI: 10.1177/1461444805056007]

EDITORIAL

Editorial: introduction to hacking and hacktivism

David J. Gunkel
Northern Illinois University, USA

The activity of hacking constitutes one of the more contested and misunderstood aspects of network culture. Initially the word denoted a kind of obsessive commitment to creative and innovative computer programming, especially the re-engineering of systems that pushed the relatively new technology of the computer in interesting directions which were oftentimes not anticipated or recognized by their designers. For this reason, hackers have been celebrated as the heroes of the computer revolution, the visionaries of the internet and the principle architects of cybersociety. However, shortly thereafter the word came to be employed to name various forms of computer crime, network intrusion and even cyberterrorism. Under this denotation, hackers have been routinely characterized as a threat to network security and are determined to constitute one of the more pernicious problems faced by societies which are becoming increasingly dependent on new media and digital information systems. Recently, this ominous image of the hacker itself has been re-engineered into what many find to be an unlikely but potent hybrid of computer technology and social activism. 'Hacktivism', as it is called, draws on the creative use of computer technology for the purposes of facilitating online protests, performing civil disobedience in cyberspace and disrupting the flow of information by deliberately intervening in the networks of global capital.

This special section of *New Media & Society* investigates the contended and contested meaning of hacking and hacktivism. The three articles that comprise it re-evaluate the history and social significance of hacking, trace the complex genealogy that connects earlier generations of hackers to the recent development of hacktivism and investigate some of the mechanisms of resistance that have been employed by hackers and hacktivists to intervene in social networks which have become increasingly obsessed with

security and secrecy. However, what connects these three articles to each other is not simply the common subject of hacking and hacktivism but a shared concern with the conceptual system that, for better or worse, already structures the way in which this subject matter has been identified, defined and interrogated. This deeper, epistemological connection is evident in the three intertwining threads that run through the materials assembled here.

First, the polysemia of 'hacking' pulls the term in what appears to be opposite directions, resulting in a set of different and seemingly irreducible characterizations. In this way, the significance of hacking, as with most assessments of computer technology, has been shaped and defined by a system of antinomies or binary oppositions. Is hacking an activity that is good or bad? Are hackers the heroes or villains of cyberspace? Are hacktivists mere adolescent pranksters or socially conscious gadflies with administrator access? All three authors share a concern with, a suspicion about and an attempt to think outside the network of binary distinctions that have organized the understanding and evaluation of this subject matter. In particular, they resist the propensity to locate hacking on one side of the debate or the other and demonstrate how the practices of hacking already interrupt such binary thinking. To put it in somewhat blunt philosophical terms, the articles that follow do not try to position hacking and hacktivism somewhere on the scale of good and bad, but demonstrate how these complex operations open such ethical systems to what is (to borrow from Friedrich Nietzsche) beyond the simple opposition of good and evil.

Second, in seeking to intervene in the binary oppositions that structure inquiry, the articles do not simply address hacking as an object but are themselves involved with and subject to hacking. That is, they are not just examinations of hacking but, insofar as they seek to question and even re-engineer the terms that structure such examination, are also actively engaged in hacking the operating system of our thinking. In this way then, each article not only investigates hacking and hacktivism but also enacts and exemplifies them. Considered rhetorically, this approach has both advantages and difficulties. It is advantageous, because such writing embodies in its own practices what it addresses. To put it in colloquial terms, it 'does what it says and says what it does'. It is difficult insofar as this kind of textual operation necessitates careful attention by both writer and reader to the performative aspect of the text. Such writing, for example, cannot be read simply for 'what it says' but must also be interpreted for what it does, comparing what is articulated to the performance of its articulation.

Third, the goal of this undertaking is not simply technical or intellectual prowess. As with hacktivism, all three articles share an interest in critical resistance that is motivated by a social and political agenda. In hacking the binary oppositions that already program the terms and conditions of the debate, these articles purposefully resist the 'either/or' decisions that one

finds in so much of the literature addressing this subject matter. This is done not simply to 'mess with' the established systems and protocols, but to question the infrastructures of power that already inform and legitimize these institutions. In 'messing with' the logic that has defined this terrain, the authors question the limited options that restrict our evaluation of this complex social phenomena and, perhaps more importantly, inquire about who gets to define the terms, who controls the debate and what interests are served.

In the end, this special section does not promise anything approaching a definitive answer or an ultimate solution to the questions concerning hacking and hacktivism. Instead it merely suggests that the questions by which to ascertain the significance of this subject matter have yet to be adequately identified. The problem with our understanding of hacking and hacktivism is not a lack of answers: it is a by-product of far too many answers that have been provided in response to the wrong kind of queries. The articles that are collected here demonstrate that hacking and hacktivism cannot be questioned by simply applying the usual categories, but can be investigated only by simultaneously allowing the object of inquiry to question and re-engineer the methods of the investigation.