Chapter 9

The Fight for Cyber Thoreau: Distinguishing Virtual Disobedience from Digital Destruction

Matthew D. Crosston
Bellevue University, USA

ABSTRACT

This analysis sheds light on where cyber disobedience fits in to larger society positively and does not deserve to be summarily thrown in with all types of illegal cyber acts. Making these legal delineations does not solve all of the problems a state will face in the new cyber age. But they will go a long way in helping a democratic state honor its foundation of civil liberties and freedom and avoid becoming a perpetrator of virtual hyperbole and digital panic. In so doing, it guarantees the people greater freedom for themselves while also having greater confidence in the fairness of their own government. This, in place of the chaotic, ambiguous, and uninformed legal and political environment governing cyber action today, would be a dramatic improvement.

DOI: 10.4018/978-1-5225-1938-6.ch009
INTRODUCTION

The intent of this chapter is to re-imagine and apply the term ‘civil disobedience’ to the cyber domain. The full extent of how it can apply will be analyzed in a framework of the evolutionary rights of protest. Traditional civil disobedience is a ‘performance’ via visual and physical mediums, while cyber disobedience is essentially a digital performance with difficulty in attributing true ownership of the act. This is an interesting antithesis to the physical protestor, who uses strategic visibility, threat of arrest, and popular backlash against state behavior as vital aspects of the disobedience. These variables are noticeably absent in cyber disobedience. But this new space also has a low cost of entry and regimes will find it difficult to physically control. Another distinction is how actors intending to cause wide-scale state damage are a very real cyber threat, while cyber disobedience can appear far more menacing than it is in reality. Thus delineating cyber disobedience that does not intend to fundamentally damage the state from cyber-attacks that aspire to is incredibly important but has proven elusive within formal cyber policy. Perhaps the most obvious delineation will be in determining the self-declared intent and motivation of cyber civil disobedience groups, along with their ultimate overall goals.

In some ways this is a completely new application of studies that consider innovation within activism for the purpose of social change. Some initial research has considered the impact of the internet on social activism in recent years. (Earl & Kimport, 2011) But this is the first application of the legal debate across global norms within such research. Newer studies are becoming more and more intrigued by the transnational potentiality of social activism and the impact it can have across state structures. (Ilcan & Lacey, 2013) As will be seen in this chapter, the essence of cyber activism is by default transnational, boundary-absent no less, and thus the arguments being made here should be seen as an important addition to this growing literature. Finally, a third sub-category within the literature is directly benefited by this chapter, namely how social media is used for social change. To date this has been largely used for the analysis of student groups at a youth level. (Velasquez & LaRose, 2015) This chapter’s findings enhance the scope and reach of such literature by expanding the applicability beyond students and youth. Indeed, social media, cyber activism, and societal change will likely only become more prevalent in future studies. Thus, this chapter represents something of the front edge of the coming digital social activism wave.

Some might also find this chapter extremely pertinent to Rawls’ Law of Peoples, which conceptualized a particular liberal understanding of social justice and defined legitimacy in a political sense. The Rawlsian ‘emergency exemption’ got rid of what been a long-standing traditional aspect of jus in bello, that which prohibited the targeting of civilian populations. It has been argued that this view of order posited...
Developing Confidence Building Measures (CBMs) in Cyberspace between Pakistan and India
[www.igi-global.com/chapter/developing-confidence-building-measures-cbms-in-cyberspace-between-pakistan-and-india/133933?camid=4v1a](www.igi-global.com/chapter/developing-confidence-building-measures-cbms-in-cyberspace-between-pakistan-and-india/133933?camid=4v1a)

Logic Tester for the Classification of Cyberterrorism Attacks
[www.igi-global.com/article/logic-tester-for-the-classification-of-cyberterrorism-attacks/135272?camid=4v1a](www.igi-global.com/article/logic-tester-for-the-classification-of-cyberterrorism-attacks/135272?camid=4v1a)