“This is Not a Cyber War, it’s a...?”: Wikileaks, Anonymous and the Politics of Hegemony

David Barnard-Wills, Cranfield University, UK

ABSTRACT

This paper is a political theory analysis using the conflict, attacks, and ‘hactivism’ surrounding the WikiLeaks organisation following diplomatic cable releases as a case study to demonstrate the complexity of contemporary cyber conflict. This complexity is reflected in the motivations, identities, and values of a multiplicity of (often non-state) actors. Termed ‘the first visible cyber war’ this conflict (having already drawn in states, media organisations, banks and payments companies, and loose coalitions of individuals) is one where traditional metaphors of war occlude as much as they reveal. International relations and critical security studies have developed a range of approaches to international conflict that focus on identities, values, and normative frameworks. Securitization, hegemony, and democratic demands offer a productive way of understanding cyber conflict. Distributed denial of service attacks are interpreted as an attempt to establish a dominant discursive position and to construct a coalition around political issues.

Keywords: Cyber Conflict, Cyberwar, International Relations, Language, WikiLeaks

1. INTRODUCTION

“We open governments.” – WikiLeaks

“If you want to start a revolution, feel free to use my mask.” – AnonOps

This paper performs a political theory analysis using the conflict, attacks and hactivism surrounding the recent publication of US diplomatic cables by the WikiLeaks organisation as a case study to demonstrate the inherent complexity of contemporary cyber conflict. The theory of securitization is used to demonstrate the politics inherent in the act of labelling a conflict ‘war’ and how this applies to the cyber environment. The paper also makes use of Antonio Gramsci’s concept of Hegemony, and Ernesto Laclau’s concept of democratic demands. These models allow us to examine the contested construction of meaning and norms in cyber conflict, a contestation which applies to the very terminology of the discussion. As a struggle for hegemony rather than a ‘war’, we can understand that hegemony is never total, nor permanent. The cyber conflict is not ‘won’ but instead something that is perpetually

DOI: 10.4018/ijcwt.2011010102
worked out. In his famous cyberpunk novel *Neuromancer*, William Gibson described the net as a ‘Consensual Hallucination’. However, drawing upon theories of the contestation of meaning, combined with the case study of politically motivated communicative conflict, suggests that the shared environment is far from consensual and there are competing politics about the directions in which it should develop.

Analyses of Cyberwar threaten to gravitate towards two poles, one arising from International Relations security studies and the second from information security (Nissenbaum, 2005). The first of these draws primarily upon ‘realist’ International Relations analysis, the functions and strategic needs of states in an anarchic world system. A typical example might be Joseph Nye’s ‘Cyber Power’ (Nye, 2010). These accounts generally attempt to incorporate ‘cyber’ either as a space of conflict (Barnard-Wills & Ashenden, in press) or a tool for various actors already active in international politics. The second performs a technological analysis of particular network level activity, attempts to locate and assess particular cyber attacks and determine effective countermeasures. An example of the second would be Project Grey Goose (2008). The account of international security politics in such accounts is often theoretically and conceptually shallow, and makes simplifying assumptions about the effects of technological processes on broader social structures. The argument is made that both of these perspectives lack an understanding of norms, identities and values that play an important part in understanding cyber conflict and that simply taking a middle path between the two poles perpetuates this problem. This paper therefore provides an analysis drawing upon critical security studies perspectives (securitization) and a post-structural theory of the formation of group identities (hegemony and democratic demands).

Critical security studies is a developing set of perspectives within International Relations security studies. Traditional strategic perspectives (often termed ‘Realism’ within the discipline) are based upon certain foundational rules. States are the primary, or even sole, important actor in international relations. There is always an enemy, but the identity of this enemy is not particularly important for understanding the function of the inter-state system. Conflict is the motivating force in international affairs, and the model assumes that states have permanent interests (Coker, 2009, p. 131). Following Cox’s insight that ‘Theory is always for somebody and for some purpose’ (Cox, 1981) traditional Security Studies can be seen as developing from Strategic Studies in the West during the cold war in an attempt to answer the problem of why states go to war, and to study the threat and use of military force (Peoples & Vaughan-Williams, 2009, p. 19). Its key concerns were with nuclear deterrents and the movements of state-based armies.

Karen Fierke suggests that due to attempts to develop new approaches and answers, and the rejection of the idea that states have universal and transitive interests and behaviours, critical security studies has arguably been more in line with a changing world than its mainstream counterparts (Fierke, 2007, p. 27). Sensitivity towards identity and interests is more appropriate than a theory which assumes an unchanging security environment over time (Fierke, 2007, p. 28). Furthermore, the Realist perspective primarily concerns itself with the interests of states and as such is poorly calibrated for understanding the actions of sub-state or non-state actors (Peoples & Vaughan-Williams, 2009, p. 20), precisely those that can become involved in cyber conflict. Norms, values, and identities are often missing or discounted alongside an objectivist ontology that assumes a pre-constituted international world prior to the political activity of actors. Wedding this perspective to technological media does not advance our understanding particularly far.

2. THE ‘CYBERWAR’?

This section of the paper sets out a brief overview of the events following the WikiLeaks ‘Cablegate’ release of US diplomatic cables.