“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
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.
This series of events has been selected because it demonstrates a number of features that have been increasingly associated with contemporary cyber conflict. It has also been called, somewhat loosely, the first visible cyber war. Because of these features this set of events provides insight for thinking about cyber conflict more broadly. The conflict has involved non-state actors and the ‘weapon of choice’ appears to be distributed denial of service attacks (DDoS). However looking at the events from a holistic perspective that includes political, legal and symbolic aspects suggests a more complicated reading.

In late November 2010 the whistle-blowing and journalism organisation WikiLeaks started to make publicly available 251,287 secret cables from United States diplomats dated between 1966 and 2010. It’s rationale for doing so was that:

“This document release reveals the contradictions between the US’s public persona and what it says behind closed doors – and shows that if citizens in a democracy want their governments to reflect their wishes, they should ask to see what’s going on behind the scenes.” (http://wikileaks.org/cablegate.html)

The ‘cables’ are messages sent back to the US from 274 different embassies. As such they cover the gamut of diplomatic activity from mundane reporting little different to reading a local newspaper, to controversial and secret topics. The document release was rapidly condemned by the US government. Over the following days, quite a range of actors became involved in this at quite high tempo.

Much of the reporting in the technical media focused upon a series of electronic attacks and the movement of the WikiLeaks website between various hosting services. Shortly after the cable release WikiLeaks’ website came under two denial of service attacks, seemingly from a US ‘patriotic hacker’, which forced it offline. Additionally the Chinese government blocked access to WikiLeaks from within China. The attacks forced WikiLeaks to move from servers in France to two Amazon cloud servers on the 29th. Amazon then removed WikiLeaks from its S3 server in the US stating a terms of service violation (Amazon Web Services, 2010). The Berkman Center report on civil society and human rights groups that are the target of denial of service attacks suggests making hosting arrangements closer to the ‘core’ of the internet to benefit from the capacity and resilience of major service providers, and finding internet service providers who will commit not to remove controversial content unless required to be law (Zukerman, Roberts, McGrady, York, & Palfrey, 2010, p. 5). This seems to be the motivation for moving to cloud servers, but was in this case ineffective due to the unwillingness of such a provider to host. Shortly after everyDNS.net killed the wikileaks.org address, forcing a move to the Swiss registered wikileaks.ch. After this WikiLeaks is hosted by Swedish company Ban-hof AB which excited the media by being inside a bomb shelter and have a distinctly ‘James Bond villain’ aesthetic. This demonstrates the important role that infrastructure providers play in any form of online politics. Ethan Zukerman terms this capacity ‘intermediary censorship’, which is becoming increasingly important as many web users publish content on servers that they themselves do not control. He argues that protection of online speech requires online service providers to affirm a role as ‘free speech providers’ alongside the clarification of applicable laws and regulation (Zukerman, 2010, p. 72). He cites Wendy Seltzer’s argument that the economics of web hosting place large incentives to remove content that might result in litigation, and little incentive to support free speech or encourage content owners to aggressively defend their rights (Seltzer, 2009).

On the evening of the 3rd December PayPal stopped processing donations to WikiLeaks stating a violation of acceptable use policy and that it considered WikiLeaks to have violated its service agreement on encouraging, promoting, facilitating and instructing others in illegal activity (“PayPal statement regarding WikiLeaks”, 2010). It was followed on the 7th by Mastercard and Visa Europe who also stopped processing payments. Visa Europe Ltd blocked donations
to WikiLeaks and Sunshine Press (the associated fundraising organisation) from December 8th pending an investigation into the nature of WikiLeaks business and if it contravened Visa’s operation conditions. The internal investigation is ongoing, and payments have not been resumed (“No proof WikiLeaks”, 2011). WikiLeaks has repeatedly contended that it does not solicit leaks, but rather acts simply as a channel for whistle blowers with material they feel the need to make public. WikiLeaks has lodged complaint regarding the matter with the European Commission arguing that the combined networks of VISA Europe and Mastercard cover 96% of payment card market in Europe and violate European anti-trust rules (http://wikileaks.org/Banking-Blockade.html). In addition they also released a parody Mastercard advert (http://vimeo.com/wikileaks/masterleaks).

Declaring its support for WikiLeaks campaign for transparency and free speech, and high critical of those organisations that had suspended their interactions with the organisation, the internet collective ‘Anonymous’ redirected its Operation Payback away from the Motion Picture Associate of America (MPAA) and International Federation of the Phonographic Industry (Zukerman et al., 2010, p. 6) towards the groups and corporations they see as opponents of WikiLeaks. Anonymous had previously also taken action against the Church of Scientology. Anonymous has demonstrated a relatively high level of technical capacity as well as knowledge of its targets. Using a distributed denial of services attack (DDoS) co-ordinated using the ‘Low Orbit Ion Cannon (LOIC)’ software, Anonymous attacked PayPal on December 6th and Mastercard on December 8th. Other recent Anonymous targets include protests against Wall Street, and electronic actions against the Bay Area Rapid Transit (BART) Police in San Francisco in response to the Police shutting down mobile phone coverage within the transit system during a protest over a police shooting.

An Anonymous press release suggested a number of tactics in addition to DDoS attacks: a boycott of PayPal, to spread and mirror the leaked diplomatic cables, form a ‘human DNS’ system to make them impossible to censor, to voting for WikiLeaks founder Julian Assange on Time Magazine’s person of the year list to increase public exposure. It also advocates posting on ‘critical hubs of information distribution’ to ‘make sure everyone you know is aware of what is happening’. Offline strategies included printing out and distributing locally relevant cables, complaints to local members of parliament or political figures, and conventional protest (marches, petitions, etc.). Operations Payback and Avenge Assange interweave online strategies and actions into protest and political action. This is not inherently surprising because the online environment is one of the ‘places’ where people enact politics, economics, communicate with peers and get information. That political communication and protest activity move here too is to be expected.

The ‘Low Orbit Ion Cannon’ software does not disguise IP addresses and potentially leaves users open to tracking. On the morning of January 28th 2011, three teenagers and two adults were arrested in the UK under the Computer Misuse Act 1990 for their alleged involvement in Operation Payback (BBC, 2011). A press release from ANON OPS responding to this interpreted the arrests as a sign that the UK government does not understand the ‘present-day political and technological reality’ but also as a declaration of war by the UK government against Anonymous (Anonymous, 2010). In coordinated activity, the FBI executed more that forty search warrants across the USA, whilst issuing its own press release reminding the public that participating in a DDoS is illegal and punishable with ten years imprisonment (“Search Warrants Executed”, 2011). This should raise some caution towards the assumption that cyber attacks are generally anonymous and un-attributable, despite relatively serious attempts to ensure operational security by particular ‘Anons’.

As of August 2011 Anonymous claimed that both Anonymous IRC servers and WikiLeaks were under constant denial of service attacks from the same botnet sources. WikiLeaks apparently requested the police investigation of
these attacks, but this has not been forthcoming. Anonymous has stated it will respond to these attacks, regardless if they originate with a state government or with individuals (AnonOps Communications 2011).

3. LANGUAGE AND SECURITIZATION

There are two levels of analysis here – the first is the relatively simply question that asks ‘is the conflict between Anonymous and service providers, in support of WikiLeaks, a cyber war?’ The answer to which is rapidly negative. However, this question reveals a second deeper set of questions about the process of naming and defining a cyber war; a process that involves language and the politics of securitization.

‘Cyber war’ currently has no objective definition against which we can assess an event or series of events and make a clear assessment if these events count as cyber war or not. There are a set of usually offered reasons why such a definition is absent. These revolve around antagonistic relations between states unwilling to settle on a definition which would either curtail their ability to act in this domain, or require them to take particular action that they wish to avoid. For example, in the context of multilateral or collective defence agreements. Also, in the historical absence of anything universally recognised as a cyber war, comparison is complex.

However the absence of a clear definition has more substantial epistemological underpinnings. If we spend some time examining cyberwar’s antecedent and related concept, that of war itself, we can find a similar contested understanding. Fierke (2007, p. 34) describes security as an essentially contested concept and we can extrapolate a similar understanding of war. The criteria for an essentially contested concept is that a concept must have value associated with it, be internally complex, part of a broad conceptual landscape and have relatively open rules of application, so that users can interpret the concept differently in response to different real world events (Gallie, 1955). Typical examples in political theory would be ‘justice’ or ‘equality’, meaningful terms around which political ideologies are structured, and which are used to make political claims.

Political language is not simply descriptive but also evaluative. To term something a ‘war’ or not, is not just to describe, but also to judge (Jackson, 2005, p. 23). To accept an account of an essentially contested concept is to also accept political activity in line with that commitment (Fierke, 2007, p. 34). Bobbitt argues that the entire system of laws of war is predicated in part upon the definition of warfare (Bobbitt, 2008, p. 455). War is a human social artefact (Fierke, 2007, p. 57), but one that is potentially at odds with other human ends. The search for definitions and check lists is missing the contested and politicised nature of language and the penetration of the definitional exercise by securitization moves. Language should also be understood as performative, in that speaking in a certain way makes certain things true.

Labelling a set of events as ‘war’ is a clear example of a securitizing move. A theoretical concept initially developed by the Copenhagen school in international relations, ‘securitization’ does not mean ‘to make something more secure’ but rather to define something as needing to be secured (Buzan, Waever, & de Wilde, 1998, p. 36). Conventionally the referent object of this securitization is the nation state, a political regime or ‘the people’. The concept of national security assumes that the nation state has to survive and it is therefore necessary for the state to maintain armies, produce weapons and seek out intelligence (Peoples & Vaughan-Williams, 2009, p. 76).

Normal politics (at least for liberal democracies) is characterised by haggling and contestation, by multiple actors and agencies with varying priorities as well as resources. Successfully securitizing an issue removes it from this melee and justifies prioritising it over other issues (Fierke, 2007, p. 108). When an issue is successfully presented as an existential security threat, then it legitimates exceptional politi-
cal measures (Peoples & Vaughan-Williams, 2009, p. 76).

Labelling as war is not simplistic however. There are important questions as to who is labelling. Certain actors will be more effective at labelling issues as security issues than others. This relies upon their credibility and right to speak to relevant audiences. A securitizing actor requires enough social and political capital to convince their audience of the existential threat. This authority currently appears to emerge from the two poles of cyber security, state security actors and computer security actors, with their own forms of securitization. Certain issues are also easier than others to securitize, given their historical associations with existential violence (Peoples & Vaughan-Williams, 2009, p. 79).

The Cyber environment is relatively new in this in that it really does not have a history of violence, not in the same way as massed tanks on an international border. Therefore the use of the term ‘war’ is a bridging metaphor to more familiar linguistic descriptions of physical conflict. The concept of ‘information warfare’ is a similar securitizing move, applying military metaphors to industry and commerce (Munroe, 2005). Nissenbaum has already highlighted the problems of dominating Information security through a political frame (Nissenbaum, 2005, p. 73) and war can be understood as the paradigmatic form of the political state frame - given the state’s claim to monopoly on the legitimate use of violence. Given the traditionally depoliticised nature of information technology language, technological actors involved in producing software, hardware, providing infrastructural services and others may have particular influence in the way that cyber securitization moves are articulated, accepted or rejected.

A different name for the same set of events may generate both different perceptions of those events, emotional and affective responses to those events and political and strategic responses to them. Jackson (2005, p. 23) provides the example of a protest, the description of which as a ‘generally ordered protest’ or an ‘anarchist riot’ would affect the way that police forces respond to future demonstrations.

Labelling a series of actions and events as cyberwar therefore suggests a particular set of responses. This is not deterministic, and there is scope for individual or group agency. However, particular discourses – ways of making sense of the world – and particular categorisations construct particular responses as rational and others as nonsensical. The labelling of DDoS attacks as a type of war, brings with it a historical set of associations, a set of assumptions about the appropriate way to deal with those problems, and the appropriate agencies for engaging with them. ‘War’ is traditionally the preserve of military agencies, and responses include the use of force. Peoples and Vaughn-Williams argue that the key insight of the securitization model is that security is not always a ‘good thing’:

“Securitization of an issue brings with it a particular type of emergency politics where the space (and time) allowed for deliberation, participation and bargaining is necessarily constricted and brings into play a particular militarised mode of thinking.” (Peoples & Vaughan-Williams, 2009, p. 83)

For example, treating the teenagers arrested for participating in LOIC attacks as warfighters would be hugely problematic. The work done by the metaphor of war in the ‘war on terror’ has been well covered. Jackson identifies the importance of language for legitimating and enacting political violence.

“Wars cannot be fought without the willing participation of large numbers of individuals from across the social spectrum. Enlisting such support requires altering the perception of individuals to comprehend the need for employing force, structuring their cognition so it appears as a reasonable and logical course of action and arousing them emotionally so they will participate or at least acquiesce to violence.” (Jackson, 2005, pp. 23-24)

We can also suggest the prefix ‘cyber’ is also doing some securitizing work. This prefix
is an evocative placeholder for more prosaic terminology, evoking a novel, high-tempo and technological otherworld. For Coker, war seems to have escaped the narrow parameters it was located within during the twentieth century. Not because of any inherent expansion, but because of the extension of ‘security’, the dominant ‘grammar of violence’ of our age across the variety of social life (Coker, 2009, p. 62). For Hansen and Nissenbaum (2009), ‘technification’ is a particular form of securitization where an issue is constructed as reliant upon expert technical knowledge, and therefore a politically neutral.

Talk of cyberwar is part of a rhetorical chain that prepares the ground for ‘violence’ in cyberspace and support for this action. Securitization theory suggests the importance of ‘desecuritization’ or retrieving the normality of politics (Huysmans, 1998, p. 576), bringing issues back into the normal ‘haggling’ of contested politics (Buzan et al., 1998, p. 29). This does however make some assumptions about the way ‘normal’ politics operates through mechanisms of limited conflict. It is precisely this dynamic, through which language constructs perceptions and affects political attachments to which we now turn, driven by critical security studies, this time with the focus on identity and motivations for Anonymous. Though this the way that a non-war conflict serves to construct identities for participants.

4. ANONYMOUS IDENTITIES, VALUES AND DEMANDS

The 2006 US Quadrennial Defense Review argued that traditional inter-state threats were giving way to decentralised network threats emerging from non-state actors, and that the spectrum of irregular conflict was expanding. Coker argues this perception of threats arising from unknown and unknowable non-state actors has penetrated across the way the West thinks about conflict (Coker, 2009, p. ix). It is easy to see how from certain perspectives Anonymous could be seen to fit within this paradigm. Anonymous appears decentralised, ambiguous, non-state and not motivated by traditional concerns of international relations. It is also harnessing modern information technology for its political activity and to support its decentralised organisation. It fits with a perception of modern hazards as differing from the past—they cannot be conveniently or simply delineated in time and space (Coker, 2009, p. 70).

It also fits with the concern regarding the apparent proliferation of ‘patriotic hackers’. Much attention has been paid to an apparent developing trend, in which popular cyber campaigns mirror political, economic or military conflicts in cyberspace, primarily conducted by ‘cyber militia’ (Ottis, 2010b, p. 1). Estonia in 2007 and Georgia in 2008 are seen as the paradigmatic examples of this type of activity, with a focus upon militia either directed by a state, or self-organising along line that parallel state interests. Activity by these militia is considered problematic because they are often anonymous (small ‘a’) and their association to a state is hard to ascertain. Comparing such militia to ‘farmers with laptops’ Ottis provides a breakdown of the minimum resources and skills required to conduct an effective cyber campaign, and finds very low barriers to action, especially for manual or voluntary botnets for distributed denial of service attacks (Ottis, 2010a). However he does suggests that a requirement for a successful cyber campaign is that some members must have a deeper understanding of cyber activity. This appears to be the case based upon the information made available on those arrested for involvement with Anonymous DDoS attacks.

However not all participants in cyber conflict are driven by nationalist affiliation, nor by association with existing political organisations—even decentralised ones. We can relate this activity to a process of identity formation associated with a collective horizon of values and perceived interests. The self-proclaimed intentions and motivations of groups such as Anonymous, as diverse as they are, should be taken seriously in any coherent analysis of their activity. Identity should be understood
as an ongoing continual process rather than a settled descriptor or essential unchanging aspect. For Fierke identity is a social category that incorporates the self-ascribed identity that the individual actor gives themselves, but also the definitions one ascribes to others and have ascribed upon them (Fierke, 2007, p. 76). Identity is therefore fundamentally relational.

Anonymous describes itself as ‘not a group, but rather an internet gathering’ (ANONOPS press release), but this is itself problematic. There is no membership structure, no officers, designated representatives or legal existence. One can join simply by claiming so (or even by identifying with Anonymous). Being on certain forums will make you more aware of what it is doing and able to participate in its functions. However one can speak for Anonymous by simply doing so (and in a sense, every Anon forum post does so), although how seriously this is taken by a range of interested actors will vary. One is a member of Anonymous simply to the extent that one recognises oneself as a member of Anonymous. Whilst spokespeople for Anonymous have communicated with mainstream media (for example ‘Coldblood’ was interviewed on the BBC Radio 4 ‘Today’ programme) this language mirrors that used in other protest movements. Students in Paris in 1968, and anti-globalisation activists in the late 1990s both regularly stated that their representatives were only spokespeople, not leaders.

This draws upon a consensus/participation model, in which if an identifying individual doesn’t like a particular action, they can simply not participate in this action without any in-group consequences. Nor is Anonymous without internal discussion. For example the use of denial of service attacks has not been without its internal criticism and caution has been expressed that continued DDoS attacks will promote a public backlash (Keane, 2011). Lulzsec, the hacker group claiming responsibility for a number of high profile attacks and exposing a number of security vulnerabilities can be thought of as an offshoot of Anonymous due to divergent methodologies and goals.

An Anonymous press release discusses the group’s relationship with WikiLeaks and argues that the association is primarily a shared set of ethics, norms and political goals. Primarily an open internet and anti-censorship.

“WeWhile we don’t have much of an affiliation with WikiLeaks, we fight for the same reasons. We want transparency and we counter censorship. The attempts to silence WikiLeaks are long strides closer to a world where we cannot say what we think and are unable to express our opinions and ideas.” (http://pandalabs.pandasecurity.com)

The extent to which the members are known to each other is open to question. Ottis discussed cyber militia with relatively loose ties, which require them to communicate online. Anonymous, and its origins in 4Chan arguably have a different relationship. To talk, as Ottis does, of ‘real life’ connections is to miss the point somewhat, and negate the importance of online created and lived identities. Ottis suggests that this lack of ‘real world’ connections creates a particular vulnerability to information operations techniques (Ottis, 2010b, p. 2). However some connections in these online environments can be very deep, very detailed and very meaningful. Of course, other connections can be very ephemeral. It is hard however to disentangle the two from an external perspective.

The linked concepts of hegemony and democratic demands provide us with potential analytical purchase upon the anonymous cyber attacks. The Marxist philosopher and social theorist Antonio Gramsci’s (1891-1937) theory of hegemony was part of an attempt to overcome the economic determinism of Marxist thought. Rather than being determined by the economic substructure, explanations of social change were instead to be found in the relatively autonomous realm of ideas and ideology. This was to emphasise the role of collective human agency and choice. Hegemony is the ability to gain control of ideas that manipulate social consciousness. Rather than being solely determined from above, this was ‘a negotiation between
the dominant and controlled class over what
the latter will accept to believe and what they
will not swallow’ (Woodfin & Zarate, 2004, p.
123), and as such was an ongoing process. In
trying to explain the uneven and unsuccessful
nature of socialist revolution across Europe
in the early 20th century, Gramsci suggested
that revolution can only take place if there is a
genuine alternative worldview accepted by the
widest range of exploited social groups.

According to Torfing, Gramsci use the
concept of hegemony to explain the contingent
articulation of a plurality of identities into a
collective identity capable of bringing about a
particular social order (Torfing, 1999, p. 102). A
discourse or identity is hegemonic to the extent
that it becomes a dominant horizon of social
organisation or that it redefines the terms of
political debate. Hegemony is an articulatory
practice – it is meaningful, and occurs through
language. This is predicated upon a notion of
collective identities that are not reducible to
economic or national structures, and a notion of
politics that takes place within a conflicted terrain
of power and resistance (Torfing, 1999, p. 101).

In relation to Anonymous and WikiLeaks
we can see an attempt to put forward an alternate
world view in an environment where social
consciousness can potentially be both global and
rapid. This world view, in favour of transpar-
ey, institutional accountability and freedom of
speech as important political values, is opposed
against the less explicitly formulated world
view they see in their opponents, a hegemonic
position which normalises state and corporate
deception and secrecy alongside the structural
and tactical manipulation of the communica-
tion environment. These values put forward by
Anonymous are not extrinsic to liberal political
theory, ‘an interest in freedom and openness
belongs to a world of liberal democracies where
these practices are tied to legitimacy’ (Fierke,
2007, p. 80). However, they take on a level of
radicalism due to the nature of these demands.

For Laclau, for a political demand to be
classed as democratic, it must meet two criteria.
Firstly, that it is a demand formulated to the
system by an underdog of some kind. Because
of this it carries an egalitarian dimension.
Secondly, the very emergence of a democratic
demand presupposes some kind of exclusion
or deprivation (Laclau, 2005, p. 125). Laclau’s
analysis of populist reason and the emergence
of collective group identities suggests that it is
the making of demands that cannot be fulfilled
that is necessary for the emerge of shared
collective identities (Laclau, 2005, p. 127).
Laclau’s study is addressed to populist social
movements for example those in East Europe
or Latin America, these shared identities are
often ‘the people’ making a demand for liberty
or equality that cannot be met by the capitalist
state as it is then constituted without radical
changes in social relations and distribution.

For Glynos and Howarth (2010), a demand
is fully political if it publically challenges the
norms of an institution or society. It is radically
political if it challenges a fundamental norm
or practice. Furthermore these demands may
become hegemonic if they are successfully
generalised, so that a range of demands and
grievances are articulated in these same terms
(Glynos & Howarth, 2010, p. 115).

We can identify certain similarities with
collective identities such as that articulated by
Anonymous and other WikiLeaks supporters.
The Anonymous press release sums this up by
saying ‘we are not a group of hackers, we are
average Internet Citizens’ (Anonymous, 2010).
The January 28th press release does however also
refer to Anonymous as ‘the people’ (Anony-
mous, 2010). Any essential characteristics of
membership are effaced in their communication,
which stresses inclusion and ideas. Whilst we
can anticipate some demographic striations (age,
gender, language, etc.) of participants, these
are not seen as important to the communica-
tors themselves. This is not a movement which
fetishises nationality or religion for example,
but rather makes a discursive claim to some
broader collective identity that does not yet
exist, but might be called into being through
political discourse - ‘Internet Citizens’.

We can therefore contextualise Anonymous
as an open expansive movement driven by a set
of values formed around the online environment,
freedom, and lack of censorship. Perceiving WikiLeaks as ideologically aligned, members recognise this value set and identify themselves as member of Anonymous and a wider incipient non-state collective identity as internet citizens. Free speech and transparency are values picked up by a wide range of online and offline actors, as other issues are couched in this terminology. The impossible demands for absolute freedom of speech and transparency solidify the group identity in the face of external contestation. These demands cannot be met without radically transforming institutional and governmental structures, behaviours and ideologies. Their target is not system security, or the website of a banking company, but rather a much broader communicative field, not a power-politics, but a more discursive one – DDoS as communicative act and assertion of nascent political identity.

5. CONCLUSION

It is fairly unproblematic to suggest that the digitally mediated contestation between the hacktivist group Anonymous in support of WikiLeaks and various online payments providers is not an example of war. It is however an example of how complicated a multi-actor international political environment can be and how a traditional state-centric perspective on security is fundamentally flawed in the cyber domain. To this end the paper suggests drawing upon critical security studies perspectives from International Relations and social theory. The Copenhagen school account of the process of securitization allows us to understand the importance of language and speech acts in creating and maintaining a security environment, and suggests caution in the application of the label ‘war’. Secondly, the critical perspective also suggests attention towards the identities, values and processes of group formation which bring together a loose coalition of online actors in support of particular value set and political position. This account is a useful corrective to accounts of ‘patriotic hackers’ or ‘cyber jihad’, and it is hoped that wider adoption of the theoretical tools and perspectives of critical security studies in the field of cyber conflict can allow it to move beyond shallow and empirically lacking models. Accounts that attempt to explain online political activity as some effect of the structure of the communication media miss the important role that the specific politics of communication plays in this context.

REFERENCES


ENDNOTE

1 Internet Relay Chat, the initially preferred method of communication for Anonymous.