‘What was the nature of the security threat that WikiLeaks presented to the US in 2010?’

Genevieve Morrow
Bachelor of Arts in Politics and International Studies

This thesis presented for the completion of an Honours degree in Security, Terrorism and Counterterrorism Studies at Murdoch University, 2012.

This thesis is an account of the student’s own research.

Thanks to Professor Sam Makinda who supervised my thesis.
Abstract

The disclosures made by WikiLeaks in 2010 were a polarising issue. Julian Assange, the organisation’s spokesperson was called a “terrorist” but at the same time, comments such as ‘this is nothing we didn’t already know’, or that the disclosures were merely ‘embarrassing’ were also made. How can it be both? A critical, constructivist analysis and in particular the Copenhagen School’s theory of securitisation is used to examine how the main actors sought to securitise the issues and the other actor. In this analysis, identity, values and norms, as well as the audience play a role in how security is determined. WikiLeaks attempted to securitise US foreign policy, providing the US with an unorthodox enemy. The US, with more resources and power, endeavoured to securitise the threat made by WikiLeaks by maximising the discourse of danger, that of ‘cyber threat’, to capitalise on a sense of fear that equates the potential of the Internet with WMDs. A successful securitisation allows the securitising actor to introduce emergency or exceptional measures (such as surveillance or a ‘pause’ on human rights) that would not be acceptable under normal circumstances. In 2010, the powerful images of terrorism and prospective WMDs were still resonant in an insecure United States after the 9/11 attacks. These images assisted in the securitisation of WikiLeaks and in the further introduction of extraordinary measures, including the regulation of on-line information and the re-engineering of the architecture of the Internet. The securitisation of on-line information and a re-engineering of Internet architecture also allows a tangible shift in sovereignty in a period of globalisation where borders tend to be perceived as open.
# Contents

Title page 1  
Abstract 2  
Copyright Acknowledgement 3  
Contents 4  

1.  
Aims and Hypothesis 5  
Conceptual Framework 6  
The Method of Analysis 9  
The Main Actors 9  
WikiLeaks Identity and Values 10  
Leaks and Method 12  
The ‘Collateral Murder’ Footage 13  
‘Afghan War Logs’ 14  
‘Iraq War Logs’ 15  
‘Cablegate’ 15  
Security Context in the United States in 2010 16  

2.  
WikiLeaks Framing of Itself and Events 20  
The Apache Footage Analysed as an Exercise in Framing 21  
Suggestions Made by the WikiLeaks Framing 24  
Response to the WikiLeaks Framing 25  
Why Were the Disclosures Securitised? 30  
‘Cyber Threat’ 34  

3.  
Securitisation Success: Audience and Platforms 39  
Was WikiLeaks Attempt at Securitisation Successful? 40  
Did the United States Successfully Securitise WikiLeaks? 46  
Linking Information, Cyberspace, Sovereignty and the Securitisation of WikiLeaks 48  
Concluding Remarks 53  

Bibliography 57
CHAPTER 1

Aims and Hypothesis

The disclosures made by WikiLeaks in 2010 were a polarising issue and have stimulated much debate. Julian Assange, WikiLeaks figurehead was named as a terrorist in the media by authority figures in the United States, a significant characterisation, while at the same time, the disclosures were also said to be ‘nothing we didn’t already know’. The aim of this thesis is to analyse the background that led to this characterisation of ‘terrorist’, and the processes used by both actors, the United States (‘US’) and WikiLeaks, to promote their agenda in contrast with the other.

Several questions are asked throughout the thesis, endeavouring to build a case that answers the question: ‘What was the nature of the security threat that WikiLeaks presented to the US in 2010?’

In focusing on this question, a series of issues are addressed. The first chapter introduces the main actors and the features of their narratives and contexts. The constructivist framework of securitisation is also introduced. The second chapter moves to the substantive aspects of the thesis, using the theory of securitisation to assess the question: If the reactions to the disclosures ranged across a continuum from ‘embarrassing’ and ‘nothing new’ to gravely serious, how and why were they framed as an ‘existential threat’ by the securitisation process? Chapter three discusses globalisation, information and sovereignty as they are implicated in the drive to establish cyber legislation that would
protect against cyber threat and incidents that include those like the WikiLeaks disclosures. The concluding chapter also assesses the success of the securitisation process attempted by both actors.

**Conceptual Framework**

The conceptual framework is based on critical and constructivist theories. This approach allows a direct examination of the events and the issues that influence security rather than an abstract approach that engages with universal definitions (McDonald 2008, 65). The theory of securitisation, as proposed by Buzan, Waever, and de Wilde in *Security* (1998), provides the methodological boundaries of much of the analysis.

Critical theory asserts the understanding that security discourse is socially and politically constructed and as such is not value neutral or objective (Alvarez 2006, 65; McDonald 2008, 65). Constructivism in International Relations theory has several variants. In this thesis, constructivism is taken to indicate a critical approach that considers security to be a social construction, where identities, values and norms are constantly produced and reproduced (Eriksson and Giacomello 2006, 233). These elements form the basis of actions and interests (Reus-Smit 2009, 212). Security, power, identity, values and norms are not primordial, natural or assumed in a constructivist analysis, as opposed to how they would be considered in a traditional, neo-realist Waltzian analysis. Further to this, security is not determined solely by material structures or by elites but is mutually constituted between agents and structures, and between the audience and authorities (Reus-Smit 2009, 216). Compared to more traditional analyses,
This type of analysis provides a more nuanced assessment of the dynamics of security, political power and change that looks beyond material forces (MacDonald 2008, 64).

The underpinnings of critical and constructivist thought can be applied via the concept of ‘framing’. “Framing is one of those heuristic concepts people employ to make sense of the complex world they live in […] where meaning implies not only what is at issue, but also what is to be done” (Eriksson 2001, 211). Vultee explains framing as interaction between sender and receiver, where cues are exchanged as to the meaning of an event or issue, with sender and receiver each learning from the other over time (2007, 79). However, while framing is potentially a strong rhetorical device, it is not deterministic and there is room for agency. Framing prioritises certain information over others therefore promoting a particular evaluation or solution and making it difficult for contradictory evidence to enter the debate (Vultee 2007, 23).

‘Securitisation’ is one type of framing. A brief introduction will be made in chapter one as the theory is discussed in more detail in the following chapters. Securitisation is a social and political process. Ultimately, it suggests that the issue, which does not have to traditionally be considered a ‘security’ issue (for example, climate change and the environment can become a security threat), is being highlighted as more important than all others because our very survival depends upon its successful resolution.
Simply put, an actor who has a degree of authority (although it does not necessarily have to be ‘official authority’) performs a ‘speech act’ in which they declare an issue or event to be a security threat (Buzan et al. 1998, chapter 2). The speech act uses relevant (and oftentimes) dramatic language that seeks to create consensus by portraying the issue as an extraordinary and existential threat (Buzan et al. 1998, 26). The ‘threat’ does not have to be an existential threat; rather it just has to be constructed as such. This gives the issue very high priority on the political agenda, thereby allowing unusual or extraordinary means to be taken to remedy the situation.

The audience must, however, accept the authority of the speaker and the argument that ‘this is a security issue of the utmost importance’ for the issue to have legitimacy. In the public domain, this acceptance process does not necessarily occur without debate, often the authority must argue its case and in this way, the audience and the authority negotiate security. It is an intersubjective process rather than elites simply declaring ‘this is the threat, this is how we will respond’; rather securitisation is a site of contestation between audience and authority, and a negotiation of what is acceptable in order to deal with a serious hazard.

Only when the audience accepts it as necessary is securitisation successful; prior to this point of acceptance the process can only be called a securitisation move. Once there is enough resonance in the audience to accept the speaker’s authority and preference, a platform is established. From this platform, emergency or unusual measures, such as a missile attack, sanctions,
surveillance or dramatic legislative change, can be taken. Without the existential threat having been defined by the speaker, these actions could not otherwise be adopted (Buzan et al. 1998, 25).

The Method of Analysis

Buzan et al. suggest the way to study securitisation is to study discourse and political constellations (1998, 25). Discourse analysis allows contextual elements to be included in the overall analysis, as well as specific actors and their behaviours. The method employed to examine the discourse is a textual analysis of the disclosures by WikiLeaks in 2010 and the response of those authorised to speak on behalf of the US. The security discourse that developed around the disclosures is examined to determine how identity, values and norms contributed to events. By studying primary sources, speech acts can be determined and its arguments and process assessed. Examining rhetoric is central in this analysis as it is the starting point in the securitisation process and becomes pivotal in determining ‘what is security’. Other primary and secondary sources are engaged with to examine the process of securitisation specific to this case study.

The Main Actors

The two main actors under analysis in this thesis are firstly, the US government and those authorised to speak on its behalf, and secondly, the WikiLeaks organisation and its spokesperson, Julian Assange. As shall be shown, ‘the audience’, or those who ‘tune in’ or participate in the debate and discussion in the public domain are also important actors in the progression of the issue as a
security issue. In the following section, WikiLeaks and the US are introduced, along with an outline of the disclosures made. Concluding this chapter is a discussion about the security context of the US at the time the disclosures were made in 2010.

WikiLeaks Identity and Values

WikiLeaks (and its sources) is comprised of many individuals, some of whom remain out of the public discourse on WikiLeaks, leaving founder Julian Assange as their spokesperson and the public personification of the organisation. This section endeavours to summarise the public profile of Assange and WikiLeaks for further critique and analysis. The information used to form the basis of the analysis is taken from a series of primary sources including essays written by Assange, interviews, and information taken from the WikiLeaks website.

In 2006, Julian Assange wrote an essay entitled *Conspiracy as Governance* in which he was critical of corruption. Setting the tone for the later philosophy of the Wikileaks organisation, in a footnote he writes:

> Every time we witness an act that we feel to be unjust and do not act we become a party to injustice. Those who are repeatedly passive in the face of injustice soon find their character corroded into servility. Most witnessed acts of injustice are associated with bad governance, since when governance is good, unanswered injustice is rare. By the progressive diminution of a people’s character, the impact of reported, but unanswered injustice is far greater than it may initially seem. Modern
communications states [sic] through their scale, homogeneity and excesses provide their populace with an unprecedented deluge of witnessed, but seemingly unanswerable injustices.

The description on its website\(^1\) and indeed interviews with Assange, positions WikiLeaks as political activists, representing idealised Western liberal values of human rights, democracy, justice, freedom, and personal empowerment. The website describes WikiLeaks as a “not-for-profit media organisation” which provides an anonymous drop box for willing sources (wikileaks.org/about). Its stated goal is to “bring important news and information to the public” whose means are electronic and its sources and activities global (wikileaks.org/about). Wikileaks states its “broader principles are based on the defence of freedom of speech and media publishing, the improvement of our common historic record and the support of the rights of all people to create new history”. The page cites the *Universal Declaration of Human Rights* with particular reference to *Article 19* that covers journalists and volunteers, and proclaims “we are fearless in our efforts to get the unvarnished truth out to the public”. The web site continues:

> [P]ublishing improves transparency, [creating] a better society for all people. Better scrutiny leads to reduced corruption and stronger democracies […] A healthy, vibrant and inquisitive journalistic media plays a vital role in achieving these goals. We are part of that media.

\(^1\) It is noted that this website has been edited since the organisation’s inception in 2007 but it is unknown exactly what was changed, or when.
It suggests that the traditional media are less willing to ask hard questions and are less independent than they could be and the role that WikiLeaks plays is one of ‘watchdog’. Assange has been quoted as saying that WikiLeaks “goal [is] to create a more just society” (Chua-Eoan 2010). On its website, WikiLeaks suggests that it is not just members of a society that should watch their own governments but members of the global community should also observe leaders of other countries (wikileaks.org/about). Perhaps in recognition to what WikiLeaks would hope to be a large section of their audience, it appeals to liberal traditions of the US, quoting Thomas Jefferson, “the price of freedom is eternal vigilance” (wikileaks.org/about).

**Leaks and Method**

The 2010 leaks were a distinct shift from the previous activities of the web site, which had stated aims of targeting authoritarian governments of Russia, China and sub-Saharan Africa (Ellington 2011, 3). The site had pursued disclosures related to the corruption of the Daniel arap Moi Kenyan government; the Icelandic banking scandal; and rice-deal corruption in East Timor amongst others. By volume though, the disclosures regarding US defence and diplomacy were the largest and became the disclosures that thrust WikiLeaks into prominence. On the targeting of the US, Assange has said, “we don’t have targets […] other than organisations that use secrecy to conceal unjust behaviour, that’s created a general target” (Chua-Eoan 2010,). Further to this, WikiLeaks would be unable to publish disclosures about governments, institutions or individuals without having first received that information from a source.
As an on-line organisation, WikiLeaks had a high level of dependency on digital technology for information gathering and dissemination. WikiLeaks and ‘cyber space’ are inextricably linked; without the Internet, WikiLeaks becomes a hypothetical entity. In 2010, WikiLeaks partnered with traditional media organisations and set timing embargoes to ensure all newspapers would publish simultaneously. Media partners included The New York Times, Der Spiegel, The Guardian, Le Monde, and El Pais. WikiLeaks had no editorial control over what the media outlets would choose to publish from the data files, or how the outlets would choose to interpret the information (Davies 2010, par 18). WikiLeaks published the documents on its website with additional commentary and interpretation some time after the initial disclosures were published by the traditional media partners.

This was not an unproblematic process. WikiLeaks was criticised for publishing documents of the ‘Afghan War Logs’ without redactions of up to 100 informant’s names (Jaffe and Partlow 2010). The organisation was to later change its approach and operate under a method of ‘harm minimisation’ by the time the ‘Iraq War Logs’ were released. Further to this, WikiLeaks and Assange had several legal disputes to resolve, including Assange being implicated in a criminal matter in Sweden but as of October 2012, had not been charged.

The ‘Collateral Murder’ Footage

Wikileaks released two videos of ‘crosshair’ footage taken from a US Army AH-64 Apache helicopter, filmed during an encounter between the Apache and ‘insurgents’ in New Baghdad, Iraq in 2007. WikiLeaks established the domain
name collateralmurder.com and the footage was posted on this web site. A
transcript of the radio transmissions between US Army personnel was published
by WikiLeaks (collateralmurder.com/en/transcript.html). The shorter of the two
edits is almost eighteen minutes long and has subtitles, apparently added by
WikiLeaks, and the longer video is thirty-nine minutes and is uncaptioned. The
subtitled, shorter-length footage appears as a grainy black and white, when the
original vision seen by the Apache gunner would have been colour, that is,
there is reference made to blue trucks (at 05.21 mark, collateralmurder.com/en/transcript.html). Some quality may have been lost as
the footage was de-encrypted by WikiLeaks.

‘Afghan War Logs’
The Afghan War Logs were released in July 2010 and consisted of documents
that were written between January 2004 and December 2009. Ninety thousand
pages of field reports outlining growing Taliban strength; the problematic nature
of Pakistan and its assistance to the Taliban; and previously unreported civilian
casualties are included in the data (Ellington 2011, 4). The logs “painted a
picture of war different to the one described by ISAF [International Security
Assistance Force]” and suggested little progress had been made since 2004
(Munn 2010, par 7). The various media partners focused on their own analysis
of the documents. The New York Times tended to focus on the sense of failure
and the relationship the US had with Pakistan while The Guardian focused
more on human rights abuses and extra-judiciary killings (Munn 2010, par 8-9).
The logs do not, however, reveal strategic analysis of the Pentagon, the State
Department or the intelligence agencies (Rogers 2010, par 2) but critics suggest
WikiLeaks lacked an appreciation for the complexities on the ground (Tiffen 2011, 6) and, as mentioned earlier, neglected to redact some informant’s names.

‘Iraq War Logs’

In October 2010, Wikileaks released what became known as the Iraq War Logs. The complete logs had 392,000 documents that showed military communications records and field reports (Tiffen 2010, 1). The New York Times suggested the logs showed “no earthshaking revelations, but they offer insight, texture and context from the people actually fighting the war” (no name 2010, par 2). The power of Improvised Explosive Devices (‘IEDs’) in asymmetrical warfare; previously under reported civilian deaths; and human rights abuses were revealed by these disclosures. According to the logs, investigations into Iraq-on-Iraq human rights failings were not conducted (Leigh 2010).

‘Cablegate’

In what became known as ‘Cablegate’, over 251,000 confidential communications between US Embassies and the State Department in Washington DC were slowly released starting in November 2010 by WikiLeaks and their media partners. The dates of the cables were from 1966 to the end of February 2010. WikiLeaks claim the cables show the contradiction between public persona and hidden deals of governments that were not in the public interest (wikileaks.org/Cablegate.html#). None were top secret; half were unclassified; 11,000 were secret (six per cent); and 9,000 were marked ‘noform’
(no foreign nationals were intended to see it) (Ellington 2011, 5). It is estimated that three million people had access to those same documents (Borger and Leigh 2010, par 6).

**Security Context of United States in 2010**

In 2010 when Wikileaks made the disclosures, the US was already in a heightened security state and had a degree of relative instability. Ten years of the “war on terror” following the attacks of September 11, 2001 (‘9/11’), two controversial and expensive wars in Iraq and Afghanistan, and the economic recession that began in 2008, contributed to this relative instability and insecurity. This insecurity played a role in the way the US responded to the disclosures. In this section, the background to the elevated threat perception the US was experiencing in 2010 is examined.

As will be shown by a brief analysis of National Security Strategies and a National Defense Strategy, the type of threats the US was bracing against did not significantly change in the years between 2000 and 2010. However, precise threats such as specific terrorist organisation (for example, Al Qaeda or Al Shabaab) did enter the security agenda but the overall type of threat remained consistent. By showing the consistency of what the US perceived to be threatening, a further discussion is enabled in later chapters that demonstrates threat perception is a vital element to securitisation. That is, while a threat can be immediate and spontaneous, the information that provides the background to why an issue can be a threat is often established over time. This is particularly the case in ‘cyber threat’, where its threat profile does not
suddenly appear at its zenith but has been considered in policy circles and public consciousness for several years, even decades. These points will be elucidated in greater detail in the following chapters but for now, a chronological and brief assessment of the security context of the US is examined.

The Clinton Administration’s National Security Strategy of 2000 (‘NSS 2000’) prioritises vigilance against the procurement of weapons of mass destruction (‘WMDs’) by enemies; cyber attacks against critical infrastructure; terrorism; adjusting border protection in a globalised world; and the protection of human rights as the primary security interests of the US (2000, preface). No mention is made of a specific enemy that the US is engaged with in the long term. US leadership is acknowledged and heavily emphasised and alliances and international cooperation are underscored in order to achieve US goals (2000, preface). The excellent position of US prosperity is highlighted (2000, preface), as is the promotion of US national interest abroad and advancing the values of the US (2000, preface). Democracy, human rights and capitalism are recognised as key values (2000, preface). These values are reflected throughout all the National Security Strategy statements.

The themes from the National Defence Strategy of 2005 (‘NDS 2005’) are similar. The heightened level of threat is evident in the first line of Defence Secretary Donald Rumsfeld’s forward to the NDS, “we live in a time of unconventional challenges and strategic uncertainty” but the US remains an “unusually powerful player in world affairs” (2005, iii).
The *National Security Strategy* of 2006 (‘NSS 2006’) emphasises the values of freedom, democracy and human dignity (2006, i). Economic prosperity and the promotion of it overseas are also highlighted (2006, 1). Notable threats are WMDs; global terrorism; opposition to democracy and human dignity; and tyrannical and oppressive foreign governments (2006, 1). The word ‘cyber’ is mentioned only once (2006, 44) in the context of a potential weapon a non-state actor may use against the US and Internet technology is alluded to in a non-specific way. However, during his administration, George W Bush did sign Executive Order 13,228 enabling an Office of Cyberdefense to be formed (Dunn Cavelty 2008, 26) and the hazard associated with digital technologies remained very high on the threat agenda.

The Obama Administration’s *National Security Strategy* of 2010 (‘NSS 2010’) also features the opportunity and threats of globalisation but vows America will continue to shape the world (2010, 41). The economy is highlighted as a threat to US stability but views promotion of its values as the way for America to express its power. The main threats as per the NSS 2010 come from WMDs; terrorism; cyberspace; reliance on fossil fuels; climate change and potential health pandemics (2010, 1-6).

Further to these statements of what are perceived to be the primary threats to the US, the budget regarding national security can also demonstrate the level of threat the US perceived in the period leading up to and including the WikiLeaks disclosures. In 2010, the US spent 42.8% of the total world military expenditure (SIPRI 2011). According to a Congressional Research Service Report, in the
decade after 2001, the United States Congress had approved a total of $1.283 trillion for military operations in Iraq and Afghanistan (Belasco 2011). Other sources place the projected expenditure on a greater expanse of national security programs, including Homeland Security, nuclear arsenal maintenance (via the Department of Energy), Pentagon spending (including its base budget plus war spending), and Department of State for one year (FY2013) at an estimate of around a trillion dollars, meaning a quarter of every tax dollar spent goes towards national security (Hellman and Kramer 2012, par 21). The threat level is considered so substantial and defence so important that in May 2012, the House of Representatives passed a Bill that protected the defence budget from being cut and that the budget reductions instead should be taken from social welfare programs such as Medicaid and food stamps (Hellman and Kramer 2012, par 22).

What can be ascertained in these figures and statements about the high level of threat perception of the US leading up to 2010? Firstly, the documents show the importance of US identity and values. That is, the importance of US leadership, power, democracy, prosperity, freedom and human rights and the promotion of those values abroad. Secondly, the style of threat did not largely change in the decade prior to 2010; most of the threats mentioned in 2000 were echoed throughout the first decade of the new century in official policy statements. Notably, amongst the primary threats was the cyber-threat, significant in its placement next to WMDs as one of the most, if not the most substantial hazard to the US.
CHAPTER 2

Chapter one considered the narratives that WikiLeaks and the US each promoted, and recognised that the US was experiencing a period of relative instability in 2010. Chapter two looks closely at the securitisation and framing processes by each actor. The impact of the discursive context that links WikiLeaks to what is understood to be ‘cyber threat’ is also examined.

WikiLeaks Framing of Itself and Events

WikiLeaks fostered its identity as political activists by framing its disclosures in a very specific way: that the disclosures were in the best interests of democracy (wikileaks.org/about). Each of the four disclosures was not randomly selected but deliberately chosen to create impact in accordance with WikiLeaks agenda. Its promotional material suggests it advocates ‘scientific journalism’, where the readers can access the original data and make up their own minds about the information (Assange 2010, par 6). The implication of the word ‘scientific’ is that the information available is sterile, technical and precise, and therefore unquestionable. The expression ‘scientific journalism’ is selected to support WikiLeaks argument and refute any framing in opposition. It fits neatly in with its framing and reinforces the public persona of WikiLeaks as activists for truth and justice.

The United Kingdom, the US, Spain, and Germany had all taken part in the conflicts in Iraq and Afghanistan and had diplomatic cables related to their countries published. Conceivably, this is a strategic move to capitalise on
discontent within these countries for the Iraq and Afghanistan conflicts and US foreign policy more generally. The timing of the disclosures, between April and December, as well as the slow release of documents relating to each leak extended the temporal impact of the information. WikiLeaks did relinquish some of its framing control to other media organisations such as The Guardian and The New York Times, but this does not necessarily indicate a reduction in the power of the framing process. Indeed, a high level of exposure and drama can promote a successful securitisation process (Dunn Cavelty 2008, 23). WikiLeaks was not seeking a neutral outcome; it was seeking to promote its agenda, and selected the timing of events and the topic areas accordingly.

The Apache Footage Analysed as an Exercise in Framing

All four disclosures frame events in a particular way, encouraging a specific discourse, that is, one that challenges the authority and legitimacy of the US. The Apache footage will be used as an example to demonstrate elements of the framing process.

The domain name ‘collateralmurder.com’ is suggestive - a play on words of the term ‘collateral damage’, a euphemism referring to civilian fatalities. The quote from Orwell that precedes the footage, “Political language is designed to make lies sound truthful and murder respectable, and to give the appearance of solidity to pure wind” (collateralmurder.com) capitalises on the connotations associated with Orwell, that is, for example 1984 and ‘Big Brother’. Following this, a photograph of the son of one of the dead is accompanied with a description of their family; references to the positive nature and chivalrous
character of the Reuters photographer are made in subtitle; as is a public statement made by a spokesman for the US Army, who explains the event, which after viewing the video appears to be misleading.

The actual footage has not yet commenced but already the staging is emotional and political. These are clearly intended to influence the audience in an emotional way – the audience is more than likely not to know what a real war scene looks or sounds like but may be more familiar with movie-style or video-game war scenes. The viewer’s lack of experience in a real war situation potentially shocks the viewer as they witness a real war scene where several people die. In this way, WikiLeaks frames the material as a very personal Armageddon-style event that surprises and shocks the viewer. Benjamin and Sontag (in Dartnell 2003, 487) suggest that subtitling of video adds narrative that enhances interpretation. In this way, WikiLeaks guides the viewer to an emotional or shocking interpretation of the footage.

The controversy of the footage is based on several elements. Subjectively it could be suggested that it appears as if all who are shot and killed are unarmed but the gunner in the Apache claims to see AK-47s and a Rocket Propelled Grenade (‘RPG’) launcher. Two long lens cameras are mistaken for weapons. Subsequently, it is found out the two individuals carrying cameras are Reuters News employees, one a driver and the other a photographer. None of the group, around eight in total appear to be acting in a menacing way. The Apache gunner requests permission to engage and after some cannon fire, it is clear most are dead and the banter that ensues between the US Army
personnel is obviously not intended to be heard by anyone outside of the situation; it contains laughter, congratulations and swearing in regards to the dead individuals. A wounded man drags himself away and the radio-voice asks him rhetorically to pick up a weapon so he can re-engage. A short time later a van arrives and several men get out to assist the wounded man. No weapons are evident but upon closer inspection, two children are visible in the passenger-side window. The wounded man is carried to the van. The gunner requests permission to open fire and after some discussion on whether the injured are being collected, permission is granted to re-engage with cannon fire and all are killed except the children who sustain serious injuries. The van driver is criticised, “that’s what you get when you bring your children to war” (collateralmurder.com/en/transcript.html).

It is the selection of scenes and the continuity of the footage that emphasise a particular framing of events – these people did die, that is factual, but the circumstances are less obvious to the viewer than we immediately understand. From the framing of the Apache video, it can be recognised that elements are chosen and promoted within a discourse to highlight or exaggerate some effects or components. There are two versions of the footage and critics suggest the shorter version lacks context (Hasian 2012, 192).

Space constraints do not permit extensive analysis of the footage but amongst the critics of the actions of the soldiers are suggestions that the soldiers ignored long-standing military norms, and the 2007 rules of engagement were not adhered to; the helicopter was not under fire, proportionate action was not
taken and the unarmed wounded were fired upon (Khatchadourian in Hasian 2012, 197).

Other critics who support the actions taken by the Army have suggested that the larger context is not shown by the shorter of the two WikiLeaks videos (Hasian 2012, 192) and the Apache had been engaged in a fire fight with insurgents prior to this engagement, leading the crew to believe this group was involved in that encounter. Other criticisms suggest that the social agency of the Apache crew that implied they were “unthinking brutal warriors” is over-emphasised, and that it confirmed negative stereotypes of adrenalin-filled soldiers who lose control during battle (Hasian 2012, 194).

**Suggestions Made by the WikiLeaks Framing**

WikiLeaks promotes its actions in a way that suggests it is speaking for a broad generic justice, representative of the utilitarian ‘greater good’. These intentions are made clear when Assange and WikiLeaks speak of justice and transparent democracies (see wikileaks.org/about). In this way, Wikileaks conflates its agenda with the global good, without recognition that its actions may be destructive in ways it has not intended and are therefore left external to its framing of the disclosures. The disclosures are clear however, in that they seek to specifically target and counter US security discourse and US foreign policy.

Through the disclosures, WikiLeaks criticised the actions of the US. The values promoted in the NSS 2000, 2006, 2010 and NDS 2005 represent the consistent
and fundamental pillars of US identity. These are democracy, human rights, freedom, prosperity, US leadership, and the promotion of these values internationally. The very clear suggestion made by Wikileaks and the disclosures was that the US was not administering democracy correctly; that the human rights it promoted were not standardised human rights but were conditional; international law in the forms of jus ad bellum and jus in bello were provisional; and the Apache video implied that the US could not perform ‘legitimate’ violence correctly.

This is a dramatic framing of events by WikiLeaks and it is argued it is an attempted securitisation. The media are actors who are able to make securitisation moves through the speech act that announces ‘security’ is occurring (Buzan et al. 1998, 88-89). Using information produced by the US itself, WikiLeaks is suggesting the US and its actions are existential threats. They are challenging the regular security order in a radical fashion. The process of securitisation beyond the ‘securitisation move’ and its success in relation to both actors is discussed further in chapter three.

**Response to the WikiLeaks Framing**

Several public statements were made in response to the leaks by high-ranking political figures and media commentators in an attempt to re-frame the issue to suit the security discourse of the US. According to Buzan et al., a ‘securitisation move’ occurs when a high-ranking official, academic or media organisation perform a speech act, that is, makes a rhetorical claim that the threat faced is a very serious one and ‘if we don’t deal with it now then we won’t be here
tomorrow to deal with it our way’ (1998, 25). Reflecting again on the securitisation definition in chapter one, this securitisation move is not however, complete; it is only when the audience accepts it as such that it moves across the threshold and becomes a successful securitisation.

It is worth pausing to consider the notion of ‘existential threat’. The threat posed by WikiLeaks was not the typical, traditional threat against a country’s sovereignty with a physical device or battalions of soldiers that was customary in the post-Westphalian era. This threat had several elements that made it unorthodox. Conventional notions of existential threat involve a relatively straightforward classification: a total, irreversible physical annihilation of a population or state.

Buzan, Waever and de Wilde’s conception of securitisation provides guidelines for what types of security threats could be perceived and constructed as ‘existential’. Different ‘sectors’ (for example, economic, military, political) have differing core elements that, under threat, are considered to be existential elements. They suggest a state has three components: idea, physical base and institutions. Threatening any of these components can be construed as an existential threat (Buzan et al. 1998, chapter 7). Physical threat includes a direct threat to sovereignty. Even a minor violation of the sovereign space is a serious threat to the state because the borders signify the bounds of the state and are considered absolute (1998, 150). Further to this, political institutions are built on the ideas and identity of the state, therefore, “[b]y threatening these ideas, one can threaten the stability of the political order” (1998, 150). Buzan,
Waever and de Wilde also suggest each securitisation should be considered in its own temporal and political context (1998, 24), indicating, for example, that an existential threat to a fragile state does not necessarily translate to an existential threat to a powerful state.

According to this conception, WikiLeaks has harshly critiqued the idea of the US and its identity, values and norms and therefore its authority and legitimacy. This line of thinking could be further strengthened by considering the medium of the threat, the Internet, as an infringement into sovereign space (via the undefined borders of ‘cyber space’). The weapon WikiLeaks used was information that was authored by the US itself. By threatening US sovereign (cyber-) space, and challenging the idea and values of the US, WikiLeaks were then constructed as an existential threat, thereby justifying any response the US deemed necessary. Declaring existential threat and the resulting security response are powerful proclamations, perhaps amongst the most powerful a state can make.

Returning to the responses to the disclosures by public figures who had a level of authority (either official or otherwise), the rhetoric had strong defensive and attacking tones. Sarah Palin, former Vice Presidential nominee suggested Julian Assange qualified for the same treatment that Al Qaeda received (Palin 2010, par 2), and his extrajudicial killing was suggested by several figures in the media (for example see Kuhner 2010). Outside of the US, Italian Foreign Minister, Franco Frattini proclaimed the diplomatic cable leaks as “the 9/11 of diplomacy” (Neuman 2010, par 30). Hillary Clinton, Secretary of State, made a
statement that included the following: “[T]his disclosure is not just an attack on America’s foreign policy interests. It is an attack on the international community – the alliances and partnerships, the conversations and negotiations, that safeguard global security and advance economic prosperity” (Rodham Clinton 2010, par 3). Mitch McConnell, who was the then Republican leader of the Senate; Newt Gingrich, former Speaker of the House; Rick Santorum, a Senator from Pennsylvania; and Vice President Joe Biden all publicly called Julian Assange either a high tech, or information “terrorist” (McConnell 2010; Gingrich 2010; Grier 2010; Biden 2010).

All of these comments suggest a dramatic interpretation of the actions of WikiLeaks and Assange. The responses outlined here had the clear implication that Assange and WikiLeaks were enemies. Naming an individual as a terrorist in a heightened security environment was not an act of random semantics.

Identifying an opponent as a terrorist works to delegitimize that opponent’s political goals and thus to move the contest away from the gray areas of political contestation, and by implication political responsibility, and toward the black-and-white world of the existential threat that is fundamental to securitization theory (Vundee 2007, 14).

Terrorism is a concept well understood by the American public (and the US allies) and is one of the strongest danger images possible in the western world (Jackson 2004, 5). “Terrorism” and its connotations signalled the extreme importance in security terms to what Assange and WikiLeaks meant to the US.
Hence, for high-ranking officials to name Assange a terrorist meant a multitude of things automatically. Terrorists are “evil”, “traitors”, murderers who will not be negotiated with, and the US will not stop until they are defeated (Bush 2001). Terrorists in the decade prior to the disclosures were relentlessly pursued, and in the quest for the defeat of terrorism, international norms and institutions that governed sovereignty and human rights were violated (Makinda 2003). Seeking out terrorists is a matter US foreign policy engages with in earnest.

To understand what a threat means to a country, its cultural, social and political history must be considered in context with the threat (Kumar 2010, 165). US identity had suffered a serious setback after the terrorist attacks of 9/11 and the decade that followed involved on-going efforts to re-produce and stabilise US values and identity both domestically and internationally. The disclosures challenged the values that the US sought to secure after the instability related to the 9/11 attacks and the economic recession that followed later in the decade. Therefore, the comments made in public by individuals such as Biden and Clinton were not just signals that the US disapproved of the actions but that WikiLeaks and Assange were firmly embedded in the category of exceptional and important enemy, an ‘enemy of the state’ (Dorling 2012). This, in turn, allows the US to pursue the offenders and their means in the manner it deems appropriate.

Paradoxically, to others, the leaks were “embarrassing but not damaging” (Mackey 2011, par 1) or “nothing new” (for example see Oppel 2011; McFarland 2010). Robert Gates, then Defense Secretary, wrote on August 16
2010, “the review to date has not revealed any sensitive intelligence sources and methods compromised by this disclosure” (Mackey 2011, par 6). These sorts of comments reveal the array of possibilities available to individuals who have access to media exposure or are high-ranking bureaucrats whose opinions influence discourse. Here, it should be noted that the media play a significant role in the perpetuation of security discourse messages that are promoted by those in authority (Vundee 2007) and as such ‘chose’ which stories to highlight and promote, either Gates’ response or a continuation of the more dramatic narrative. Both comments can be reported in the media but it tends to be the dramatic frames that the audience engage with and these frames sell newspapers (Dunn Cavelty 2008, 23). Buzan et al. suggest, “Actors can choose to handle a major challenge in other ways and thus not securitise it. The use of a specific conceptualization is always a choice” (1998, 32). If there is a range of ways powerful actors can respond to an issue and the reactions to the disclosures stretched across a continuum from ‘embarrassing’ and ‘nothing new’ to gravely serious, how and why were they framed as ‘existential’ via the securitisation process?

**Why Were the Disclosures Securitised?**

In order to answer the question of why the WikiLeaks disclosures were securitised, we must consider what framing and securitisation permit. Firstly, identities and values can be reasserted and re-created allowing the central political institutions and the national or collective narrative to be strengthened. Secondly, framing allows a temporal extension of previously promoted security discourses and their accompaniments. That is, certain types of security can
maintain position and support on the political agenda. Thirdly, ‘every day’, standard politics can be suspended and unusual measures can be introduced that would not otherwise be permitted (Buzan et al. 1998, 25). In order to address the above question of ‘why were the WikiLeaks disclosures securitised’, all of these elements must be considered.

Firstly, identity, values, and security discourses can be analysed critically to see how the threat discourse surrounding WikiLeaks is contextualised. Constructivist theory considers the state to be a construction and an idea, and its primary task is to secure this idea (Alvarez 2006, 65). Traditional approaches to security assume a ‘threat’ is self-evident and relatively unproblematic, able to be measured objectively, and usually arising from a state actor or a defined group (Dunn Cavelty 2008, 21; Eriksson and Noreen 2002, 1; Alvarez 2006, 65). In a critical approach, a ‘threat’ is not self-evident, natural or organic (Buzan et al. 1998, 204). Security and threat are context-specific social constructions (McDonald 2007, 67) - threat is a political construction that, to borrow from Robert Cox, ‘is always for someone and for some purpose’ (emphasis in original 1981, 128).

Discourses of danger are not organic or ‘common sense’. Fear is a real emotion and is necessary for survival. The impressions that emerge from a graphic terrorist attack provoke anxieties and visceral responses that no degree of rationalising can overcome (Jackson 2004, 2). However, these images and fears are used to reinforce a selected set of ideas, ignoring others that suggest alternatives to fear. Multiplicities of real dangers exist in the world but the ones
that are highlighted and interpreted as a ‘true danger’ or existential threat are politically mediated and determined (Jackson 2004, 3). This is not to say that those that are determined as threats are not a threat, rather their seriousness is sometimes over-emphasised and misconstrued.

Often this will occur to the detriment of other threats that are ‘more’ existential such as, for example, the large number of deaths from preventable malaria in sub-Saharan Africa - large budgets are allocated in political ways rather than according to threats that have been qualified through empirical research (Lawson 2011). Powerful actors largely determine security agendas and threats, and ‘danger’ is named and interpreted within a discursive context (Eriksson and Noreen 2002, 21). Meanings are assigned to events and these meanings are prone to alteration over time to suit a political agenda (Jackson 2004, 2). Alvarez suggests that ‘security discourses might need to be understood as the states constant reproduction of danger rather than as the states response to danger’, and the state has the role of simultaneously naming danger and providing itself as the solution (emphasis added, 2006, 75). Buzan suggests that total security is not possible, not because threats are endless but because achieving complete security would make the state redundant (in Alvarez 2006, 67).

Constructed identities, values and narratives create communities that define a collective ‘us’. The collective ‘us’ is not possible however, without the opposing, constructed ‘them’ or ‘other’. The borders that sovereignty suggests provide a line between the two groups, producing insiders and outsiders, allowing a neat
but mythical differentiation – these groups and their identities are under constant re-production, transformation and contestation, are never complete and as such are inherently unstable (Nayak and Malone 2009; Campbell 1998). Nevertheless, collective identities and values are powerful social constructions upon which security discourses are built and maintained.

Discourses of danger are also important by reinforcing the mythical who ‘we’ should be, for example, ‘that is not the American way’, and as such limit dissent outside of norms. During a time of conflict or perceived threat, redefining and reinforcing collective identities, values and normative behaviour is much easier as people tend to unify in the face of danger (Jackson 2004, 13). Discourses of danger tend to encourage individuals to self-censor, as they do not want to be excluded from the norm or the collective that represents ‘us’. Campbell suggests the US has successfully used conflict and danger to re-define itself multiple times since foundation (Campbell 1998, 170). In the case of WikiLeaks, the US audience is reminded via the securitisation speech act of what are acceptable behavioural norms. ‘Patriots’ do not dissent - as was suggested by the notion Assange was treasonous (Palin 2010 FB), disregarding the fact he held Australian citizenship, and therefore could not be a patriot, but the implication is clear – acting outside these defined norms and challenging the values of the US is seditious. Thus, it allows individuals and groups to express their patriotism by aligning with the US. It has been suggested corporations such as Bank of America, Visa, MasterCard and PayPal expressed such patriotism by refusing donations to WikiLeaks be delivered through their
channels, while simultaneously allowing donations to the Ku Klux Klan (Paypal 2010; wikileaks.org/banking-blockade; Waever and Adams 2010).

‘Cyber Threat’

The central discourse of danger that relates to Wikileaks is the narrative of ‘cyber threat’. The term ‘cyber threat’ does not relate to a specific threat, rather it is a term commonly employed to encompass any and all threats related to the Internet. This often results in clichés and technical imprecision (Dunn Cavelty 2007, 20; Eriksson 2001, 214). ‘Cyber threat’ tends to be a reference to crime, mischief or terrorist activity by state and sub-state groups on the Internet. There are other constructions of ‘cyber threat’ but they are beyond the scope of this thesis. The relative newness of the discourse surrounding cyber threat has resulted in imprecise meanings where a range of criminal activity from web site defacement to the theft of fighter jet blueprints by a state actor are conflated into the same category (Dunn Cavelty 2008, 22). The Internet is (incorrectly) perceived to be a borderless and uncontrollable space, replete with uncertainties and as Herrera suggests, the perception of the Internet is such that it seems to be a great no place, with different rules, different threats, and there is nothing much the regular geographical and political world can do about it (2007, 67-72).

There are other factors that contribute to the threat perception of the Internet. The rapid development of technology couples with the high level of reliance on technology and with the fear of ‘the machines’ – machines and technology that are out of control, as suggested in popular culture by movies such as Moon,

The threat associated with the Internet suggest terror and loss can come from any or many geographical locations, it does not need a large budget, and importantly, is usually anonymous in nature (Lawson 2011, 11; Dunn Cavelty 2009, 217; Herrera 2007, 71). Since the 1990s, terms such as ‘cyber war’, ‘electronic Pearl Harbour’ (Eriksson and Giacomello 2006, 226) and ‘cyber-Katrina’ (Walt 2010a; Lawson 2011, 21) have sat alongside images of lone actors with keyboards who, it was intimated, could use any or all of those keyboards like bombs (Dunn Cavelty 2008, 19). Conflating WMDs with cyber threat is common (for example see Poulsen 2007). However, it is argued by some, including a report sponsored by the Organisation for Economic Co-operation and Development (‘OECD’) that catastrophic, existential-type threat is largely overstated (Dartnell 2003, 480; Dunn Cavelty 2008, 20; Eriksson and Giacomello 2006, 226; Dunn Cavelty 2010, 187; Stewart and Mueller 2011; Lawson 2011).

Nevertheless, while part of this thesis is a critique of the over-statement of the Internet as a (medium for) threat, it would be remiss to suggest that no hazard exists. Incidents such as denial-of-service attacks, web site defacement, hacking, and theft of digital property, are reportedly widespread and used in a
variety of circumstances (Sommer and Brown 2011, 6). These attacks tend to be against symbols and images, and the major impact tends to be humiliation and the feeling of vulnerability rather than a genuine existential threat (Eriksson and Giacomello 2006, 234). Dunn Cavelty adds to this by proposing that cyber attacks result in inconvenience and financial loss in the form of property rights infringements or lost revenue and do not result in the doomsday scenarios proposed or the loss of life that is commonly proposed (Dunn Cavelty 2008, 20). The so-called ‘millennium bug’ or ‘Y2K bug’ were dramatised and framed as substantial threats. It was suggested the Y2K bug would potentially cause nuclear meltdowns, catastrophe, and significant loss of life. There was some damage done by the Y2K bug but it was significantly less than what it was framed as (Eriksson 2001, 218).

It is difficult for the layperson to be able to judge the seriousness of what cyber threat may entail and they tend to surrender their understandings of the issue to stakeholders, experts and government. The jargon relating to the expertise of the technology is understood well by very few. Lack of access to the reality of the threat is further curtailed as the statistics of the actual damage done is kept classified (Walt 2010b). Security discourses cultivate and institutionalise stakeholders who naturally develop a vested interest in preserving threat perception (Jackson 2004, 14) and ‘cyber threat’ is no exception. These stakeholders vary from bureaucrats within the government security apparatus, to private sector security developers and providers, to researchers who receive funding or grants that rely on the continuation of threat. This opens the ‘floodgates’ for all types of threat exaggerations whether threats are
substantiated or not (Dunn Cavelty 2007, 37). All of these above-mentioned factors contribute to the manufacture of uncertainty – uncertainty that is not objectively measured yet subjectively felt which reinforces the sensation of potential threat.

From a historical perspective, the threat of the Internet did not emerge spontaneously. The Reagan administration was the first to legislate for computer security (Dunn Cavelty 2008, 24). According to Eriksson, several factors contributed to the rise of the cyber world as a security threat. The resolution of the Cold War allowed a new security policy window to open; the rapid development of information technology (‘IT’) carried with it expectation and fear; and information, which has always been a core element of military affairs, was embraced by the military as a security issue because IT can be used as part of an advancing technology of warfare (2001, 219). The threat of the cyber world remained steady and high on the security agenda through the 1990s. Central Intelligence Agency Director John Deutch in 1996, and all US Presidents since Bill Clinton have placed ‘cyber threat’ at the very top of threats to the US, next to WMDs (Dunn Cavelty 2008, 25; NSS 2000; NSS 2006; NSS 2010). The events of 9/11 saw a further elevation of the threat that could emerge via the Internet, and policy and legislation in the US was altered accordingly (Herrera 2007, 77).

WikiLeaks and its use of information via the medium of the Internet is inextricably linked with the discourse of danger that is known as ‘cyber threat’. Assange is the personification of that threat, constructed as a dangerous former
hacker who is taking on the US single-handedly, his intimidation of the US, its sovereignty, its values and identity with a threat so grave, may mean that ‘if we don’t deal with WikiLeaks in a particular way, we will not be free tomorrow to deal with it the way we need to’. This is the constructed securitisation of the WikiLeaks disclosures.

The US experienced a period of relative instability and insecurity after the attacks of 9/11 and the economic recession beginning in 2008. These events challenged US identity and values grounded in democracy, human rights, freedom, prosperity, US leadership, and the promotion of these values internationally. The framing of WikiLeaks disclosures suggested that information is the weapon and the Internet is the delivery device. Securitisation suggests that a successful framing of events will lead to measures that permit extraordinary measures to be taken in order to address the threat, and prevent such matters from occurring again.
CHAPTER 3

Chapters one and two have shown that both WikiLeaks and the US have attempted to frame and securitise specific issues according to their own agendas. As an on-line organisation, WikiLeaks has been conflated with the discourse of danger that has been developing alongside the rise of IT, that of ‘cyber threat’. Cyber threat is however, a discursive tool that vaguely and inadequately refers to the rise of powerful and unpredictable machines that are as dangerous as WMDs. Endeavouring to reinforce and stabilise US identity and values, the US attempted to securitise WikiLeaks, its actions, information and the Internet. Chapter three discusses this in greater detail, evaluating the success of the securitisation process by both actors, and situates globalisation and international sovereignty in the issue.

Securitisation Success: Audience and Platforms

In the previous chapter, securitising ‘moves’ were discussed in regards to the speech act. The role of the audience is unique in the securitisation approach: the audience engages with the speaker to decide if the issue is a serious threat (Buzan et al. 1998, 29-33). Security is not solely discussed amongst elites for their determination of threat, rather it is the intersubjective nature of the relationship between audience and authority that determines if an issue is a serious danger or not. The acceptance by the audience is not necessarily by easy passage; deliberation and debate may often occur in the public domain that involves the case put forward by the securitising actor (Buzan et al. 1998, 25). Further to this, there is no guarantee that a speech act or the securitising
move will be accepted as security, even in polities that are authoritarian (Buzan et al. 1998, 31). In accepting the threat as existential, Buzan Waever and de Wilde add,

[W]e do not push the demand so high as to say that an emergency measure *has* to be adopted, only that the existential threat has to be argued and just gain enough resonance for a platform to be made from which it is possible to legitimise emergency measures or other steps that would not have been possible had the discourse not taken the form of existential threat, point of no return or necessity (emphasis added 1998, 25).

McDonald (2008, 75) suggests that the notion of ‘audience’ is problematic in the theory of securitisation and wonders who the audience is and how can it be defined. This does present some issues as will be discussed further. However, keeping in mind Buzan et al.’s suggestion that the securitisation theory is not an attempt at a purely objective method but is rather an overall consideration of a process, and the lack of a precisely defined audience can be overcome. While the audience is a critical element for the overall success of a securitisation, there are several other components in the process that enable a successful securitisation.

**Was WikiLeaks Attempt at Securitisation Successful?**

In examining Wikileaks framing of events, could it be determined that it has been successful in its attempts to securitise US foreign policy as per Buzan et al.’s criteria? Firstly, the (presumed) goals of WikiLeaks should be
reconsidered. The disclosures in 2010 offered a harsh critique of US foreign policy; democracy, human rights, international law, US identity and values, and the state’s legitimate exercising of violence were all called into question. The critique that was undertaken appeared to be open-ended and did not provide ‘solutions’ or a projected outcome of its own. In a state-centric securitisation, actions such as war, sanctions, policy or legislative changes are within the state’s power. WikiLeaks itself did not have the resources to initiate these types of actions against any state, law, or policy; rather the promotion of a counter discourse to US foreign policy appears to be the end in itself.

While there is some contention over whether WikiLeaks can be considered journalists or not (see Peters 2011, 667; Thomas 2011), WikiLeaks can arguably be considered a part of the media or publishers within the model of ‘new media’. The media is able to act as a securitising actor but it usually follows an authority’s lead (Vultee 2007, 21), making the speech act supported by WikiLeaks, that is, ‘US foreign policy is an existential threat’, an unusual but not impossible speech act. News articles questioning the morality of war-like actions, or investigative stories that reveal human rights abuses are not uncommon in the media but attempts to de-legitimise and de-stabilise a nation-state on a large scale through media are unusual. The state is the usual securitising actor because historically, it has the processes and power that favour its position as such. However, securitisation theory suggests that in principle, the role of the securitising actor is not pre-determined and does not have to be state-centric as is suggested by traditional International Relations theory (Buzan et al. 1998, 31, 37).
How does the role of the media, the security speaker and the audience apply to the case of Wikileaks? Traditional media outlets such as The Guardian and The New York Times assisted in positioning the disclosures into a place where they could ‘speak security’. While WikiLeaks, as has been demonstrated, framed and provided a discourse to interpret the disclosures, it could not be the speaker of security as it did not have the authority or social capital. Rather, the speakers of security in this case are, ironically, the original authors of the documents and footage, the US government and their representatives. If the audience accepts that the disclosures were not significantly altered, and the audience could apply their own meaningful interpretation, the content could be interpreted as a significant and existential threat. The speaker was the US government by proxy, an authoritative speaker, where the US seemed to provide evidence against itself, even if WikiLeaks had heuristically framed it. WikiLeaks and other traditional media organisations, therefore, participated in the securitisation but the speaker was the US government by a type of paradoxical proxy. While this is an unconventional way to securitise an issue, it is not outside the thresholds that Buzan, Waever and de Wilde (1998) discuss.

The acceptance of the threat as existential by the audience is difficult as the defining of ‘audience’ is subjective and open to interpretation. A well-designed study to measure audience acceptance of existential threat is beyond the scope of this thesis. Anecdotally, some suggestion of audience acceptance could be garnered from blogs or commentary on the issue, or from surveys that measure audience perceptions of Assange or WikiLeaks but the limitations must be noted – they are informal and only a guide. In Australia, UMR Research polled
1000 people in mid-December 2010 and found 51 per cent to support the release of the documents while 25 per cent opposed it (Lester 2011). This makes the suggestion that the disclosures were considered acceptable in December 2010 but it does not provide a clear analysis on changes of perceptions over time or that specifically, existential threat was perceived.

Outside of the suggestions that one poll can provide, other factors regarding the audience can be considered. The partnerships with traditional media outlets across several regions and languages suggest the audience is vaster than the continental US, opening the issue up to be debated amongst diverse groups with a variety of politics and perspectives. Arguments suggesting the destructive nature of US foreign policy pre-exist the disclosures and this provides a foundation for the meaning and interpretation of the disclosures amongst some of the audience. Within the broader audience, the US government and its political allies are a powerful faction and this will impact upon ‘audience acceptance’. Therefore, ‘the audience’ is not a simple element but it can be assumed a multitude of perspectives exist within it.

If the audience accept the existential nature of the threat, a platform is then established from which emergency measures may or may not be taken (emphasis added, Buzan et al. 1998, 25). It appears as though WikiLeaks is providing a challenge to the US but will not take traditional security actions such as imposing sanctions or declaring war. If, however, the platform is established because it is accepted that an existential threat does exist, other actors may use that platform for their own ends if it can skilfully be appropriated.
Members of the audience that subscribe to the idea that US foreign policy is an existential threat possibly already held that opinion prior to the WikiLeaks disclosures and used the disclosures as evidence to support their point of view. Measuring that portion of the audience is, as already mentioned, challenging, but it might be reasonable to accept that there is a portion of the system-wide audience that accept this to be so considering the negative opinions concerning US foreign policy are held across many identity groups, within both allies and enemies of the US (for an empirical analysis see Katzenstein and Keohane 2007). This is not to suggest the alternative point of view that the US promotes democracy and therefore peace does not exist, rather, it suggests both can exist simultaneously and have platforms and resonance of their own. Contrasting ideologies such as those in the cold war existed simultaneously and were securitised concomitantly so this concurrence does not detract from the possibility that two or more platforms claiming existential threat can co-exist. That the US was the original author of the disclosures is significant; it qualifies the authority of the message within them powerfully. A commanding global actor such as the US has a ready-made audience who listen to its rhetoric.

Buzan et al. do however make the point that attempts to securitise system-wide (that is, globally) are likely to fail (1998, 36-37). WikiLeaks attempted a system-wide securitisation, across multiple regions and identity groups. Large scale, ‘global’ securitisation beyond discrete communities or identity groups is difficult but not impossible. Events that use the majority of the world’s population as a referent object, such as a possible environmental catastrophe due to climate change or the 1914 attempt to mobilise the international working class have
experienced mixed results and tend to work less effectively than middle scale
securitisation but this is not to say that large scale securitisation cannot occur
as circumstances change (Buzan et al. 1998, 36). Middle scale actors such as
the US have a powerful, pre-existing sense of who ‘we’ are, and are able to
muster national identity and resources to confront the actor who claims to
represent a system-wide community (1998, 37). In the cyber context, on-line
political activists tend to have effects that are ‘wide’ rather than ‘deep’ (Dartnell
2003, 495) that are no match long term for the power and adaptability of the
nation state (Shaw 2000, 13). Therefore, while the disclosures perhaps claim to
speak for multitudes of un-named people, across many cultures and regions,
this actually weakens WikiLeaks case in attempting to securitise US foreign
policy; middle scale actors tend to be more defined and able to act against the
system wide attempt, and system wide actors do not tend to have enough
legitimacy to maintain their program.

Here, points and counter points have been presented in order to determine the
success of WikiLeaks securitisation of US foreign policy. If it is accepted as so,
it was performed in an unorthodox manner but still within the methodological
bounds of Buzan, Waever and de Wilde’s theory of securitisation. The main
issue remains with the deliberation of ‘audience’ and therefore has a platform
been established. If it is accepted that there is sufficient evidence to affirm that
a significant portion of the audience acknowledges that US foreign policy was
an existential threat on the basis of the evidence Wikileaks provided in its
disclosures, and hence a platform established, then a case of securitisation has
occurred.
Did the US Successfully Securitise WikiLeaks?

Chapter two discussed in some detail the securitisation of WikiLeaks and Assange, focusing on the characterisation of Julian Assange as a ‘traitor’ and a ‘terrorist’. As was noted, the impact of labelling an individual as a terrorist in that historic and cultural context was profound and clear. The key question then becomes: Were WikiLeaks actions accepted by the audience as an existential threat and hence, was a platform created upon which extraordinary measures could be taken?

The audience in this process was primarily the US domestic audience and secondarily, the allies of the US, internationally. Securing the domestic front is of higher priority because without the integrity of sovereign power domestically, no state is able to defend itself effectively, internationally. As Buzan et al. suggest, it is not that an audience accepts the speech act unconditionally, or without debate, it just must gain enough resonance to be understood as existential. If we once again consider, for example, the reasonably large number of officials and media outlets that supported or carried the speech act, with its powerful message of “Terror”, as well as the large and highly influential financial corporations (Visa, MasterCard, PayPal, Bank Of America) and Internet Service Provider (amazon.com) that categorically and publicly rejected WikiLeaks actions, a picture starts to build that sustains the suggestion that ‘enough resonance’ took place. A survey taken by The Washington Post suggests that 68 per cent of those surveyed believed the disclosures harmed national interest and 59 per cent believed Assange should be arrested (Chaiken 2011). As previously suggested, polls, surveys and anecdotal evidence are
limited in their methodologies but they do provide a suggestion that a portion of
the audience accepts the existential threat argument proposed by the security
speakers. In another study published in 2012, the statement, ‘how worried are
you that you or someone in your family will become a victim of terrorism’ was
rated by 42% of individuals as ‘very or somewhat worried’ (Stewart and Mueller
2011, 108). This can be extrapolated to suggest that the surveyed population
understood what the characterisation of ‘terrorist’ meant and what the
implications of its classification as existential were.

While WikiLeaks did not have the avenues to pursue sanctions, ‘legitimate war’,
diplomatic action or legislative change, the United States did have access to
these and this provides a major difference between the two actors and their
method of securitisation. Potentially, both could securitise and establish a
platform that is based on an existential threat but only the US could take
significant actions based on that platform. While it can be argued that the US
successfully securitised the WikiLeaks issue, there is also a larger context that
suggests it is also still a political ‘work in progress’. This is not unusual in
securitisation, as political issues can be understood as constructions that are
embedded in a larger historical process. However, it is essential the actions
taken against the existential threat must be beyond daily politics and create or
allow the platform for extraordinary action that would not otherwise be
acceptable (Buzan et al. 1998, 21).
Linking Information, Cyberspace, Sovereignty and the Securitisation of WikiLeaks

The securitisation of the disclosures was assisted by two contextual factors. The first is the discourse of danger of ‘cyber threat’ that is inextricably linked to WikiLeaks. The second is the post-9/11 environment that allowed the audience to understand ‘terrorist’ more graphically than prior to the events of 9/11, and created a precedent that, in the minds of the audience, permits the dramatic securing of the nation-state and information as acceptable and at times, highly desirable. Without the prior and comparatively more dramatic events surrounding 9/11, the securitisation of WikiLeaks would have unfolded differently, if at all. At the same time, US values and identity would not, hypothetically, have been as insecure as they were in 2010 if not for the events of 2001. Therefore, it is within the context of 9/11, and the discourse of ‘cyber threat’, the securitisation of the disclosures of 2010 permit a platform, from which the US can pursue these ‘new’ weapons and means – information and cyber space - through a legal and legislative process. Two points can be made here.

Firstly, legislation to control the threat posed by the digital world existed prior to the WikiLeaks threat and WikiLeaks cannot be considered as the initiator for extraordinary action in the realm of cyber legislation. Rather, WikiLeaks allows a continuation and re-magnification of the issues that cyber legislation address. The securitisation of WikiLeaks permits the securing authority to prove its case for cyber legislation by saying, ‘this example shows us we must secure the Internet or national security will be at risk again from terrorists’. This is a
completely undesirable proposition, but also one that is oversimplified. However, it is the platform upon which extraordinary measures can be both recalled and established in their own right.

Secondly, the convening of a grand jury in Virginia (Greenberg 2012) remains a mysterious segment of the entire episode that, if it leads to the prosecution of Assange, it has been speculated will lead to a skirmish between US First Amendment rights and national security issues (Timm 2012). This, at the time of writing, remains a series of ‘ifs’ and ‘maybes’ but this approach to First Amendment rights would have been almost unimaginable without national security issues being over-emphasised and securitised both in a post-9/11 context and in the way the US has framed the WikiLeaks issue. Even if the grand jury amounts to nothing and Assange is not prosecuted, ‘information’, a key resource for the US in globalisation and also as a strongly protected tradition and key value from the US Constitution is being included in the securitisation process.

Information is the weapon of WikiLeaks; it is the substance of the latent battle between First Amendment free speech and publishing rights and national security; and it is the matter that flows in the conduits of cyber space, the space that is being secured by US legislation. As a key value and strongly guarded tradition, no ordinary event would allow First Amendment alteration. Only an important issue, and a long term significant challenge would allow any change or shift to occur – extreme national security risks and threats of terrorists, either fundamentalist or cyber-terrorists are seemingly solid reasons for such a shift.
Further to this, securing cyber space allows for greater control over the
dynamics of globalisation, as well as maintaining jurisdiction of sovereign
space. Securitisation and existential threat are the vehicles that allow dramatic
shifts in policy and legislation to occur.

Attribution and anonymity are key issues in Internet security as has been
mentioned. Without attribution, the enemy in all its forms, from bully to vandal
to spy to thief, cannot be identified and therefore the doctrine of deterrence
cannot successfully be applied (Sommer and Brown 2011, 11). Preventing
action by an unknown actor, or prosecution of the unknown entity is obviously
unyieldingly difficult. The Obama Administration’s *Cyberspace Policy Review*
(2009) dramatically emphasises the ubiquitous Internet as insecure and lacking
resilience, in need of “major advances in security […] or significant change in
how [the Internet] is constructed or operated”, it is desirable to change the
architecture to decrease anonymity, or the US will be highly vulnerable in terms
of economic prosperity and national security (2008, i-vi, 33).

Consequently, Bills recently presented to the US Congress emphasise
decreasing barriers to identification of on-line users (*Cyber Intelligence Sharing
2012 are examples of Bills proposed to Congress, see govtrack.us for more
detail). Propositions like these set aside all previous privacy legislation to allow
for new on-line privacy laws to be enacted (Paul 2012; Shaw 2012). Further to
this, while crimes on-line reflect ‘real world’ instances, for example identity
fraud, bullying and espionage can all be committed both on-line and off, on-line
criminal activity is approached (at least theoretically) by a suspension of the fourth amendment of the US Constitution, that is, the protection against unreasonable search. Of course, proponents suggest that national security is at stake therefore the search is defensible, however, just as warrants are available in the real world for criminal activities, so might they specifically apply in the cyber world, rather than a wholesale suspension of due process as critics suggest these legislations will provide (Shaw 2012).

Redefining the architecture of the Internet to allow identification of users also offers a re-territorialisation of sovereign space (Herrera 2007). This redefining or affirming of sovereign space is desirable in an increasingly globalised world where borders are open and less defined. Cyber regulations such as those mentioned above, also aim to protect the value of prosperity that is of high import to the US (Cyberspace Policy Review 2009, B-1). A significant aspect of the discourse of danger of cyber threat is that unpredictable events ‘will’ occur and an existential threat is inevitable at some point. WikiLeaks, as has been established, is the embodiment of this threat. By securing sovereign space, enemies are kept on the ‘outside’, the inside can be better regulated, and there is a clearer delineation between ‘us’ and ‘them’, allowing identity, values and national narrative to be reinforced and recreated. When discussing the notion of national sovereignty, international society becomes essential because it is the understanding and acceptance of reciprocity that endows the practice of sovereignty with validity.
The Internet is a network of networks across multiple territories (Herrera 2007, 69) and as such, any regulation to identify users will not have the desired efficacy without international regulations. The ‘Convention on Cybercrime’ is an international treaty that requires member countries to regulate domestically for identification of cyber criminals (Council Of Europe, 2001). Both the US and Australia have signed this treaty. However, this is a European-authored treaty and it is likely that the US will prefer to author a treaty themselves and show global leadership on the issue in order to promote their own values, including prosperity and stewardship (Cyberspace Policy Review 2009, iii). Normative change in international society occurs slowly over time – emergency measures as per securitisation can be enacted but substantive normative change occurs more slowly. Herrera suggests that political crises initiate the political momentum for change in technologies and increased regulation (2007, 74). While 9/11 initiated an environment of change in international cyber regulations, the US continues to lead international society in these changes, and shocks or crises like the WikiLeaks disclosures allow further consciousness to shift towards further regulations in the international sphere.

Therefore, while the events of September 2001 initiated a change in security policy including cyber-security policy, the securitisation of WikiLeaks and its characterisation as ‘terrorist’ and a cyber threat allow a deeper embedding of information and the Internet as a security issue. In turn, information and the Internet become weaponry that must be secured by the appropriate authority in order for the nation-state and indeed the global citizenry to be protected from serious threat. While a change was initiated in 2001, it is the further
construction of security issues such as the securitisation of WikiLeaks that allows cyber threat to be viewed as an imperative risk that must be dealt with by extreme measures. Hence, the platform created by the naming of a security threat and the consequential platform allows the US to regulate cyber-space, information, and sovereignty both domestically in the US and internationally.

**Concluding Remarks**

This thesis is not a wholesale rejection of the notion that threat can occur or originate on-line. It is accepted that the Internet is implicated in numerous security issues. However, danger is a subjective emotion (Campbell 1998, 1) and threat perception is often based on emotional responses and dramatic messages not rational cost and benefit analyses. Securitisation capitalises on the drama and the human response to fear, maximising worse case scenarios of the future, of the unknown. To do this, discourses of danger such as the narratives associated with ‘cyber threat’ and ‘terrorist’ are constructed politically and are often over simplified. While there may be various threats that exist on-line, the likelihood of them being altogether existential is perhaps hyperbolic; rather, they are most often inconvenient and sometimes expensive.

Terms like ‘cyber threat’ tend to conflate issues together mixing less serious issues such as web site defacement with more serious issues of espionage (Lawson 2011, 25). Comparing Internet threat to weapons such as WMDs is not helpful and is misleading. Technical and specific terminology and definitions are more useful to correctly address threats rather than using the misunderstood notion of cyber threat with its equation with WMDs in the
legislative process. However, legislation that is technically specific will limit its ‘shelf-life’ and it would need to be amended accordingly on a regular basis (Auerbach and Tien 2012, par 12). It was once thought ‘spam’ would mean the end of email but a specific technical approach meant it could be addressed with an exact tool to filter spam from email accounts (Singel 2010, par 44).

There is no shortage of data available to researchers that would enable them to conduct significant empirical cost benefit analyses to ascertain real threat (Tehan 2012, i). Further to this, threats tend to be localised rather than national or global, countering the suggestion that cyber threat is of pandemic proportions (Sommer and Brown 2011, 5). Re-engineering the architecture of the Internet to allow attribution appears to be a crucial goal in proposed legislation and policy. Some advocates for the US Bill of Rights find this problematic (for example see Lemieux 2012; Paul 2012).

Political rhetoric such as that of securitisation allows easier passage for legislation that would not have been possible prior to successful securitisation. This is not to suggest that a mighty conspiracy is at hand, rather, legislators and their audience do not understand the critical detail and technicalities of the material. No person can be an expert on every legislative issue and the population look to authority figures to make those informed decisions for them. Legislators, it is asserted, genuinely want to maintain their end of the social contract and establish a secure and sovereign nation-state that has a strong identity and set of values. Convincing a group of people they should be scared about a particular issue to the point that it represents an existential threat
reduces resistance to extraordinary measures that reinforce power. In this case, the open borders of globalisation have challenged sovereignty of the US. The architecture and anonymity of the Internet are such that the Internet additionally challenges sovereignty. ‘Enemies’, ‘terrorists’ and threats help define who ‘we’ are. Securitising allows maintenance of these borders and a reconstruction of identity and values that help constitute who ‘us’. Identity, values, norms and national narratives in critical and constructivist theory are vital because not only are they the basis of actions and interests, they create the imagined community that holds a nation together.

A critical, constructivist analysis has permitted an alternative view of the threat WikiLeaks posed to the US in 2010. A critical analysis and an assessment of securitisation allow a deeper analysis of both positions and it is not intended as a moral judgement of who may be right or wrong; neither the US nor WikiLeaks can be considered ‘innocent’ or unproblematic. Both actors attempted a framing or securitisation of the other in order to either shift or maintain power. The relative strength of the US and its defined identity, values and norms allowed it to respond effectively to the ‘threat’ the WikiLeaks disclosures posed, allowing the US to redefine itself at a time of (constructed) threat, reiterating the values of ‘what makes the US exceptional’. Of course, this critical analysis has demonstrated that existential threat is often a construction and for securitisation to be successful, a true threat does not have to exist, rather just perceived to be so. Nevertheless, WikiLeaks did pose a threat that was unique, unorthodox and in some ways, substantial. They reinforced pre-existing ideas that US foreign policy was hypocritical, and ironically, the disclosures used the US’s own
authority to speak. However, the combination of WikiLeaks and the Internet together and its resulting discourse of ‘cyber threat’ misconstrue the threat of WikiLeaks as one that equates with WMDs. The methodological boundaries of Buzan, Waever and de Wilde’s securitisation theory allow the analyst to accept that both actors successfully securitised the other because both could establish a platform that ‘proved’ existential threat. While securitisation is a process embedded in contested political practice, the disclosures of 2010 may have run a large degree of their course but the threat of WikiLeaks and their political agenda remain a threat to the US while the Internet and information remain insecure.
Bibliography


Reus-Smit, Christian. 2009. “Constructivism” In Theories of International


