Copyright © 2018 International Journal of Cyber Criminology – ISSN: 0973-5089
January – June 2018. Vol. 12(1): 230–254. DOI: 10.5281/zenodo.1467901
Publisher & Editor-in-Chief – K. Jaishankar / Open Access (Authors / Readers No Pay Journal).

The Rise of Chinese Cyber Warriors: Towards a Theoretical Model of Online Hacktivism

Craig Webber[1]
The University of Southampton, United Kingdom

Michael Yip[2]
Independent Researcher, United Kingdom

Abstract

China is frequently reported as the source of many transnational cyber-attacks. Yet, there have been very few studies on the people behind such attacks. In this paper, we have studied some of the reasons behind the rise of a specific form of hacking: hacktivism emanating from China. Using various criminological theories, as well as political and sociological approaches, a novel theoretical framework behind Chinese hacktivism is proposed in this paper. This is supported by an empirical analysis that was carried out on the membership growth patterns of online Chinese hacktivist forums and the observed patterns are used to support the proposed framework.

Keywords: General Strain Theory, Hacktivism, Cybercrime, National Humiliation, Ressentiment, Relative Deprivation, China.

Introduction

The richness of the cyber world of deviance has resulted in new forms of crime emerging, and the merging of traditional and digital phenomena. Hacktivism is a relatively recent addition to this area in which hacking converges with political activism to create the neologism hacktivism (Denning, 2001, p. 263). The term hacktivism has been widely credited to Jason Sack in an article written about the artist Shu Lea Cheang in InfoNation in 1995. Hacktivism takes political demonstration onto the internet and it often emulates activities seen in the non-digital world[3] (Karatzogianni, 2015). However, increasingly it is able to extend the kinds of demonstration typical of traditional attacks (Caldwell, 2015).

[1] Associate Professor of Criminology, Criminology and Psychology Programme Lead, The University of Southampton, Highfield, Burgess Road, SO16 1BJ, United Kingdom. Email: C.Webber@soton.ac.uk
[2] Email: michael.yip.research@gmail.com
[3] However, see Webber and Yip (2012) for a discussion about how many forms of cybercrime rely on the 'drifting' between the online/offline and physical/digital realms.

For example, virtual sit-ins, or Distributed Denial of Service attacks (DDoS),[4] echo traditional forms of protest by preventing the target engaging in their usual activity, while web defacement replicates political slogans defacing buildings. But, the internet removes friction and allows for activities to take place without the need to be physically present at the scene of the attack (Negroponte, 1996; Turkel, 1995/1997). This allows for the escalation of attacks, so that infiltrating networks and destroying or copying databases is made far easier whenever and wherever the target is located. Ultimately, the aim of hacktivism is to make a political statement through a combination of embarrassment, disruption and damage to reputations.

The word hacktivism was created at about the same time as Manuel Castells' *The Rise of the Network Society* was published. Castells suggested that the 'network self', a new social identity forged from the networked society, was an apolitical individual and those who are disconnected join criminal networks or withdraw into fundamentalism (Castells, 1996/2000).However, the hacktivist seems to be a strange hybrid, politically aware and networked, sometimes fundamentalist and surfing around the edges of criminality conducting a form of electronic civil disobedience (Goode, 2015; Fuchs, 2014; Manion & Goodrum, 2000). It has become even more newsworthy since a loose knit group of politically motivated hackers called "Anonymous" launched a series of high profile cyber-attacks against companies who had cut off services to Wikileaks due to the intense pressure from the US government. These "hacktivists" called their series of attacks "Operation Payback". This caught the attention of the media who followed the event with increasing interest and hyperbole (Karatzogianni, 2015).

Variations on the themes have since become the most powerful political and social policy issue of the early 21st Century. Walking a fine line between political espionage and citizen activism, several key incidents have had a profound effect on the shape and possible direction of international relations. The Chelsea Manning leak of sensitive military data and their subsequent publication on Wikileaks in 2010 demonstrated the reach and depth of the security services into the very networks and systems that make up the Internet. Edward Snowden extended this insight by leaking data to various newspapers in 2013. Then came the revelation that Russia was engaging in political manipulation through the social media-enabled targeting of voters with 'fake news' designed to undermine the Democratic candidate, Hilary Clinton, and support the Republican candidate Donald Trump. It is unclear if the Russians were fully aware of the potential outcome of them successfully manipulating the outcome of the US Election.

Popular discourse about all forms of hacking, from the news media to the entertainment media, tends towards the extreme end of the spectrum. This has resulted in suggestions of a cyber-war and cyber-geddon,[5]&[6] with state-sponsorship often seen as propelling the activity at enemy infrastructures with the result that this has done more to mystify than clarify (Jewkes, 2011; Webber & Vass, 2010; Wall, 2008; 2010; Maguire, 2007). Lucas (2017) has proposed the notion that hacktivism, and hacking more generally, can be

[4]DDoS (Distributed Denial of Service) is a type of network-based attack with the aim of overloading a targeted machine, thus preventing it from carrying out its normal duties.

[5]http://www.guardian.co.uk/technology/2012/apr/16/militarisation-of-cyberspace-power-struggle

[6] Watts, S. (2012). "Call for cyber-war 'peacekeepers' force". Available at: http://news.bbc.co.uk/1/hi/programmes/newsnight/9687338.stm.

likened to the notion of soft power. Using the term 'soft-war', here hacktivism is another mechanism that states may use to persuade, encourage or belittle an enemy without the use of military hardware.

Perhaps these headlines are needed to jolt the public's consciousness into making more educated choices when they click on links or download software that could turn their laptop into a "zombie machine"[7] in a botnet,[8] which is then used to unknowingly enact DDoS attacks, one of the most popular forms of attacks used by hackers and hacktivists (Deseriis, 2017). Alternatively, the Internet has become one of the most intrusive surveillance tools ever created, providing governments and corporations with the power to store data about our lifestyles and movements through the web and through the physical environment via smartphones and GPS (Shalhoub-Kevorkian, 2012). In this paper, a more balanced view is taken by examining hacktivist groups from China in some detail as well as the political and social contexts that provide the foundation for the activity. Hacktivism is a subject which has been under researched academically and there has been an over-reliance placed on the knowledge "shared" by the various stakeholders[9] who have a vested interest in boosting demand for their products and services. Therefore, the aim in this paper is to study the key characteristics of a specific form of hacktivism, both theoretically and empirically.

The Criminological Significance of Hacktivism

The first issue that needs to be addressed is, what is the criminological significance of hacktivism? There have been several studies, books and articles written on the subject of cybercrime, hacking and cyber terrorism (Van Hardeveld, Webber, & O'Hara, 2017; Jewkes, 2002; Jordan & Taylor, 2004; Maguire, 2007; Wall, 2008, Yar, 2006, Taylor, 1999; 2001; 2005). Yet, there have been very few distinctly criminological studies of hacktivism (notable exceptions are: Holt, Freilich & Chermak, 2017; Bodford & Kwan, 2018). Where criminology looks at cybercrime it tends to treat it as a form of media and utilises traditional approaches to the study of the crime/media interface such as routine activities theory or rational choice theory. Hacktivism might not be seen by many criminologists as a major social problem because the attacks are generally against websites comprised of digital components that might be of more interest to a computer scientist or security experts (Chander, 2016). However, as noted above, many popular discourses have elevated such issues into a serious social problem akin to a moral panic whereby the event is shrouded in mystique and danger unlike anything seen before (Young, 1971; Cohen, 1972/2002; Garland, 2008). But, more than just a reiteration of a moral panic, hacktivism of all varieties is also a genuinely new and unique form of deviance, even if it shares some characteristics with more traditional forms of activity (Tanczer, 2016; Yar, 2005). It is not just an old form of crime forgotten through historical amnesia (see eg., Pearson, 1983; 1994).

[7] A "zombie machine" refers to a computer which is under the control of another remote user without the acknowledgement of the owner.

[8] A botnet is a network of compromised machines usually under the control of a remote user.

[9] Gray, P. (2011). "Exposing Norton's cybercrime scare campaign". Available at: http://www.brisbanetimes.com.au/it-pro/security-it/exposing-nortons-cybercrime-scare-campaign-20110921-1kkip.html.

Even though the targets tend to be big corporations such as banks or government agencies, this is precisely why hacktivism is of interest, especially to critical criminologists who recall the magical transformations of youth subcultural crime into statements of political resistance in the 1970's (eg. Hall & Jefferson, 1976).Until recently, the hacker who infiltrates systems for profit, or the carder who deals in stolen or fake credit cards, was the most common cybercriminal, responsible for the majority of all data breaches. However, that is no longer the case. According to a survey carried out by Verizon, hacktivism accounted for 58% of all data breaches in 2011. Hacktivism had not been identified as being behind any data breaches since the survey began in 2004 (Verizon, 2012).[10] In the UK, since 2016, computer misuse and other forms of cybercrime have been added to the Crime Survey for England and Wales (Crime Survey for England and Wales 2017). It showed that a large number of people are experiencing cybercrime of various forms. Although hacktivism is not a separate category in the CSEW, the increasing awareness that cybercrime is now more prevalent than the traditional crimes that criminologists had been studying will be increasingly reflected in the empirical data.

The second issue to address is, what can criminologists offer and how can criminological theory help to understand this activity? Criminology is very good at presenting ideas and theories about hard to reach groups. One such example, and simultaneously a theoretical position that we want to explore, is an article by Robert Agnew where he applied general strain theory (GST) to terrorism in order to test the fit of a theory that derives from criminology to a phenomenon that had not been subjected to such analysis before (2010; see also Agnew, 2012 for a similar analysis of climate change as strain to crime).

Reflections on General Strain Theory and Merton's Social Structure and Anomie: Bridging the Micro and Macro

General strain theory is a social psychological adaptation of Merton's social structure and anomie theory (Agnew, 1992; Merton, 1938). Merton's work, and the strain paradigm more generally, is especially useful to this account because we will go on to discuss the way that an ideology of Chinese patriotism echoes Merton's concerns in mid-Twentieth century America. Specifically, the 'Chinese dream' is to put an end to the humiliation experienced during the "100 years of national humiliation" and "Rejuvenating China (zhengxing zhonghua)" (Wang, 2008, p. 794). In this paper, Agnew's three types of strain are explored in the context of the web and our focus on Chinese hacktivists. The first type of strain, 'strain as the failure to achieve positively valued goals' is related mostly to the work of Merton, A. K. Cohen and Cloward and Ohlin, and which some have referred to as relative deprivation (Lea, 1992).This is explored through a revaluation of the work of W. G. Runciman (Runciman, 1966; Webber, 2007a). The second type of strain, 'strain as the removal of positively valued stimuli' will be explored using the concept of *ressentiment* and humiliation. The final type, 'strain as the presentation of negative stimuli' is discussed through an outline of the historical and cultural context through which hacktivism developed in China. Using this context, strain is the inability to protest due to the overly restrictive State controls on

[10]See also: http://www.guardian.co.uk/technology/2012/mar/22/hacking-anonymous; http://www.bbc.co.uk/news/technology-17428618

public demonstrations. We seek to provide a more sociological and political/cultural account to stand alongside Agnew's more social psychological orientation. It is a useful theory to consider when exploring hacktivism because it synthesises many different theories and suggests that crime occurs not only through the blocking of pathways to positively valued goals, but also the 'inability to escape legally from painful situations' (Agnew, 1992, p. 50).

However, it is necessary to add an element to the approach because it does not adequately capture the way that crime, or in this case hacktivism, is mediated through the unique environment of the web. By focusing on the way that *individual* responses to strains are mediated by different variables that explain the variation in reactions, the account cannot do justice to the way that blogs, forums, and cultural and subcultural variables create a sense of *social* identity. Moreover, the General Strain theory is a theory about criminal responses. If a value-neutral view of hacktivism is taken, does it still work? In other words, if we were to view hacktivism as the expression of legitimate grievances through political demonstrations, is a theory of crime suitable? Clearly, this is a criminological conundrum since hacktivism is a criminal offence in most countries. But, it is also a means to a political end (Manion & Goodrum, 2000).

Consequently, there is an added element in this paper that is often ignored or rendered opaque in the general strain theory literature, namely the political and historical variables. Lastly, changes in technologies, in this case, the availability of the Internet and the World Wide Web (WWW) in China, is also considered a significant variable for the emergence of Chinese hacktivism. Internet forums or Bulletin Board Systems (BBS) are some of the earliest online social networking tools available to Internet users and it continues to be popular among the Chinese users, with approximately 148 million users in 2010 (CNNIC 2011[11]), a 26.6% growth from 2009. As will be shown later in this paper, Internet forums are the primary communication tool used by Chinese hacktivist groups. From a criminological perspective, this is significant because the association with like-minded others helps to reinforce behaviour and ideologies, a key component to Akers' social learning theory (Burgess & Akers, 1966; Akers, 1977; 1998; Akers, Krohn, Lanza-Kaduce & Radosevich, 1979).

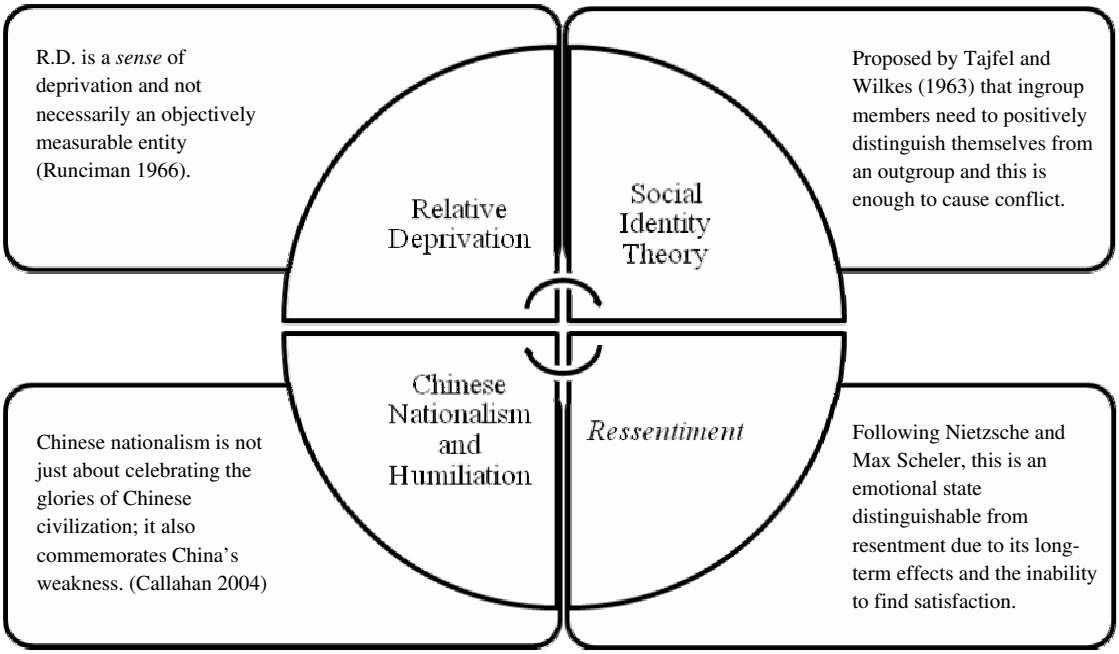
There are a number of reasons for this,[12] but the most important is that we have access to blogs, forums, and data such as membership levels and website usage trends. We do not have access to the hacktivists themselves so there is a need to focus on the macro-level data at the expense of micro. General strain theory has mainly been tested on youth delinquency due to the availability of data and despite Agnew's recent discussion of terrorism and climate change, empirical data on hacktivism has yet to be accumulated even to the limited extent that has been accrued around terrorism. Therefore, it is not possible to do more than speculate about their psychological make-up or personal biographies. Nevertheless, the analysis of this data is a useful and fascinating insight into the reasons behind this particular form of hacktivism.

[11]http://www1.cnnic.cn

[12]There is not space here to go into a discussion of the pros and cons of individual versus social accounts. We take the view that a theoretical synthesis is the most productive way forward, given certain conditions, see for example Webber 2010; 2007a; Jefferson 2002.

Innovation and Blocks to the Chinese Dream? Towards a Theoretical Model of Chinese Hacktivism

Figure 1. Theoretical Framework for Patriotic Chinese Hacktivism



In this section theoretical ideas are presented that help to explain some of the unique characteristics of hacktivism emanating from China (see Figure 1 for an overview). This section starts by outlining the social and political context for the theoretical discussion that follows. The Tiananmen Square protest in 1989 was followed by the imposition of further restrictions on public demonstrations by the Chinese Communist Party (CCP) (Hughes, 2000). Shortly afterwards the state launched a nationwide patriotic education campaign to more fully embed the ideology of the CCP (Callahan, 2004; Wang, 2008). However, this had the contradictory effect of arousing nationalistic pride based on a sense of humiliation over past harms against China, whilst simultaneously limiting the means to express it. We will elaborate on this later. Consequently, it is our contention that hacktivism in the Chinese context derives from a complex social and emotional mix of factors. At the emotional level, the feelings derive from a position that is more than just resentment. It will be argued that humiliation is one of the key variables, but it is an enduring sense of humiliation as opposed to the usual definition of the emotion as short-lived. Many scholars have linked this to the reasons for mass protest and collective action (Lacey, 2011; Jasper, 2011; Wang, 2008; Gurr, 1970). Here, the same is suggested for Chinese hacktivism. Humiliation can only occur where there is an out-group that is thought to perceive us in a negative way. Consequently, a theory of in-group/out-group comparisons is presented from a social psychological perspective that accounts for group interactions and identifications. The paper will go on to show how these have been linked to theories of relative deprivation (Webber, 2007a). Chinese hacktivism will also be located within a longer term emotional state that has been described by the term *ressentiment*.

Failure to Attain a Positive Sense of Self: Relative Deprivation, Ressentiment, Social Identity and National Humiliation

1. Relative Deprivation and the Creation of Enemies

Agnew's first form of strain refers to the inability to attain positively valued stimuli, such as self-esteem. However, this is rarely linked to a theory of motivation. What makes Merton's innovator choose to innovate in the first place? This is an emotionally charged decision. Although Merton's theory of anomie, and the tradition of subcultural theory based on it (Merton, 1938; Cohen, 1955; Cloward & Ohlin, 1960), is deemed by some to be a form of relative deprivation (Lea & Young, 1984/1993), it has been argued that we need to look at another theorist, W.G. Runciman, for a more useful account of relative deprivation and group or national conflict (Webber, 2007a).The concept of relative deprivation has appeared in many guises and has enjoyed mixed fortunes since W.G. Runciman's book, *Relative Deprivation and Social Justice* appeared in 1966. This was one of the fullest accounts of the concept up to that time. The following is a summary of the key idea:

> If A, who does not have something but wants it, compares himself to B, who does have it, then A is 'relatively deprived' with reference to B. Similarly, if A's expectations are higher than B's, or if he was better off than B in the past, he may when similarly placed to B feel relatively deprived by comparison with him (Runciman, 1966, p. 10)

Importantly, relative deprivation bridges the gap between objective, even structural, forms of deprivation (absolute deprivation) and the subjective, or agent-level, experience of deprivation. This is important because of the way that the Chinese hacktivists in this study elicit a strong patriotic connection to China. In left realism, relative deprivation is a cause of crime (Lea & Young, 1984/1993). However, it has been argued that it should instead be seen as the outcome of comparative processes (Webber, 2007a). In this way, and in a similar way to the concept of *ressentiment,* it is a negative emotion, not a structural and objective entity such as absolute deprivation. As Runciman suggests;

> Relative deprivation should always be understood to mean a *sense* of deprivation; a person who is 'relatively deprived' need not be 'objectively' deprived in the more usual sense that he (sic.) is demonstrably lacking something (Runciman, 1966, p. 10-11, *emphasis in original*).

Relative deprivation is, therefore, the emotional response to negative comparisons of self (egoistic relative deprivation), or group (fraternalistic relative deprivation) to comparative out-groups. Unlike the 'relative deprivation causes crime' argument seen in left realism, this account allows for ambiguous, even counter-intuitive, responses to comparative evaluations (Lea & Young, 1984/1993). Consequently, relative deprivation is not a *cause*, but a *tendency* towards criminal, or in this case political deviance. This fits in with Agnew's GST whereby traditional strain theory over-predicted crime amongst those sharing the same strains. This is not to say that there are no discernible patterns among those who respond negatively to comparisons with significant out-groups. Strong in-group identifications can have powerful effects, especially when they have been developed over a period of time. The historical sense of humiliation is weak in the concept of relative deprivation, but *ressentiment* captures this factor well.

2. Ressentiment as Persistent Deprivation

In a recent article, Agnew has argued that it is necessary to understand the temporal condition of causal variables (Agnew, 2011). We need to understand that different variables can affect people over different lengths of time. The concept of relative deprivation does have this element in its formulation by Runciman. His book and the survey that forms its core data asked questions about the sense of deprivation over a period of time (Runciman, 1966). Nevertheless, the sense of deprivation and resentment that can occur over many years, even decades, is still only tacitly discussed. In contrast, Nietzsche's concept of *ressentiment,* elaborated and extended by Max Scheler (1915/1998), refers to an incurable and persistent emotion characterised by hate and despising of selected out-groups based on a sense of one's own inferiority. This feeling is one that can be felt at an individual level, as well as at a national or cultural level. An entire nation can be said to suffer *ressentiment*. In Scheler's discussion, *ressentiment* results in an impotent inability to physically and verbally express the feeling. Whereas resentment is usually fleeting and transitory, *ressentiment* lingers often without relief; a form of resignation (Meltzer & Musolf, 2002). It is historical relative deprivation. This sense of an inability to express one's frustration at an enemy is a key outcome, it is argued, of the Chinese government's national education strategy after Tiananmen. An ideology of humiliation to inspire State-sanctioned progress in the economic, cultural or sporting spheres is contrasted with an inability to express anger at enemies from outside China. However, Meltzer & Musolf (2002) have argued that a sense of impotency may characterise *ressentiment,* but it is not inevitable.

> Rather than a necessarily durable state, *ressentiment*-related passivity may at times become a lengthy, dynamic, *transitional* stage between treatment defined as wrongful and retaliation or rectification. That is, ressentient individuals or groups may come to define the inducing agent as either intolerable or no longer overpowering and, therefore, susceptible to acts of revenge or revolt (Musolf & Meltzer 2002, p. 250-251, *emphasis in original*)

It is the perception that something can be done that may result in individual or collective action. Perhaps the key additional criminological input of the work of Cloward and Ohlin (1960) can help us understand how, with the right opportunities, collective action to overcome and mitigate the feelings of impotent *ressentiment* can be achieved. Elaborating Robert Merton's idea that crime occurs in those who accept the American dream but reject the legitimate means to reach that goal, Cloward and Ohlin added the argument that access to illegitimate opportunities was also necessary to engage in specific criminal acts. Hacktivism is very different from the types of criminal activity Cloward and Ohlin describe. But the notion that certain crimes can only take place if we have access to the right opportunities for their commission is pertinent here. The availability of the internet, the forums and blogs that disseminate the hacktivist discourse and the restrictions placed on public protest in China has all increased the opportunity for computer-mediated protest. In addition, the sense of *ressentiment* is increased through dissemination and reinforcement on these forums (Akers, 1998). Less clear are the social psychological dynamics of these groups. It is this issue that is tackled in the next section.

3. Social Identity Theory and Relative Deprivation

It has been argued that relative deprivation, and other negative outcomes of individual and group comparisons such as *ressentiment*, can be included within the social psychological approach known as social identity theory (Webber, 2007a, 2010; Mummendey, Kessler, Klink, & Mielke, 1999). The social psychologist, Henri Tajfel, put forward the suggestion, based on his group experiments, that intergroup conflict could occur without competition for resources (Tajfel & Wilkes, 1963). Identification with a group was sufficient to create conflict if comparison with another group took place. This was because a social group had the need to positively distinguish itself from what became known as the out-group (Tajfel & Turner, 1979). People needed to create or maintain a positive social identity. More recently, this approach has become more sophisticated by moving out of small group experimental studies, to look at groups undergoing real social upheaval, such as during the negotiations in the decade prior to the handover of Hong Kong to China in 1997 (Bond & Hewstone, 1988; see also Reicher, 1987; 1996). What these studies demonstrate is that in order to understand crime or hacktivism it is necessary to understand the networks and social context in which people operate (see also Hobbs, 1997 for a review of the literature; Canter & Alison, 2000). In particular, it has been argued that;

> [I]ndividuals' identification with the relevant group predicts collective action. This is particularly the case when the group's identity is *politicized* because politicized identities are normatively geared toward collective action (Van Zomeren, Postmes, & Spears, 2012, p. 3).

Linking this to the discussion of *ressentiment,* and the elaboration by Musolf and Meltzer, and the feelings of *ressentiment* that are encouraged by the Chinese government's use of National Humiliation as a motivating force, coupled with the opportunity afforded by the spread of the Web to mitigate these feelings of humiliation through hacktivism, all helps to explain the rise of this activity.

4. Humiliation without relief: Nationalism, Patriotism and Hacktivism

Agnew suggests that two forms of strain differ from the traditional Mertonian account. One is the removal of positive stimuli; the other is the presentation of negative stimuli. Humiliation and shame are powerful emotions. In the Chinese context, they are integral to this account. Moreover, the 'inability to escape legally from painful situations', Agnew's account of the presentation of negative stimuli, is also fundamentally implicated in the rise of Chinese hacktivists (Agnew, 1992, p. 50). In *Crime, Shame and Reintegration* Braithwaite argues that in countries that have an effective form of shaming, a re-integrative rather than stigmatizing form, crime rates tend to be low (1989; 1993).

What effect, then, might a national education programme have on creating a sense of patriotic humiliation and shame?[13] And how might this sense of shame be overcome? These are some of the issues that will be explored in this section. Over the last two

[13]There is much discussion over whether or not shame and humiliation are interchangeable (see for example Callahan 2004). Shame tends to be something we want to apologise for, whereas to be humiliated is something that is done to us as an individual or group and about which we do not feel we need to apologise. But, here we will use both terms since the point of the hacktivist's attacks is to restore what they see as national pride in the face of the government's failure to act. It is a sense of shame at being in the humiliating position of weakness.

centuries, national humiliation propaganda has proven to be a very effective, if not the most effective tool for the purpose of national unification and recovery in different locations. Abraham Lincoln declared a "National Humiliation Day" to unify the country during the American Civil War. Gandhi used the same strategy to unify India to rise against the British imperialists in 1919. In China, Mao used it to establish the People's Republic of China and offered a national salvation by telling the world "Ours will no longer be a nation subject to insult and humiliation" (Callahan, 2004, p. 203). Then in the 1980s, the Chinese Communist Party (CCP) faced the "three belief crises": crisis of faith in socialism, Marxism and the party itself. This gradually led to an increasing demand for Western-style democracy which resulted in the Tiananmen movement in 1989. The shocked Chinese rulers perceived the cause to be the lack of ideological and political education and as a result, a patriotic education campaign was launched in 1991 (Wang, 2008, p. 800).

Initially, the patriotic education campaign was limited to youth education and it was implemented from kindergartens to universities. According to Zhao (1998,p. 292), "…by May 1994, more than 95% of primary and middle school students in Beijing were organized to watch the patriotic films recommended by the State Education Commission". However, the campaign gradually targeted almost everyone including soldiers, farmers and workers. As Callahan (2004) has summarised, Chinese nationalism is;

> [N]ot just about celebrating the glories of Chinese civilization; it also commemorates China's weakness. This negative image comes out most directly in the discourse of China's Century of National Humiliation. Chinese books on the topic generally tell the tale of China going from being at the centre of the world to being the Sick Man of Asia after the Opium War (1840) only to rise again with the Communist Revolution (1949)...The discourse of national humiliation shows how China's insecurities are not just material, a matter of catching up to the West militarily and economically, but symbolic. Indeed, one of the goals of Chinese foreign policy has been to 'cleanse National Humiliation'. (p. 202)

Indeed, the most relevant part of this patriotic education campaign to hacktivism is the ways in which the campaign "took every opportunity to instigate nationalist resentment against foreign pressures" (Zhao, 1998, p. 297). The aim is to convince the youths that hostile international forces are doing all they can to undermine China's quest to dominance once again. To achieve this goal, the patriotic education campaign was "designed to present the Chinese youth with detailed information about China's traumatic and humiliating experience in the face of Western and Japanese incursion" (Wang, 2008, p.791). This political creation of a sense of historical relative deprivation towards foreign forces, which we argue is *ressentiment,* through national education programmes, and the coincidence in timing with the availability of the Internet in the mid-90s are what the authors believe to be the fundamental factors behind Chinese hacktivism. In effect the CCP created some of the conditions for a collective form of re-integrative shaming, creating a sense of national shame but with a focus on collective responsibility to overcome it (Braithwaite, 1989; Callahan, 2004). However, the CCP provided few means to express grievances in public (Lacy, 2011).

The first major instance of an eruption of this politically constructed *ressentiment* is evident from Hughes' paper (2000) in which he reports the reactions to the Indonesian riots against ethnic Chinese in May 1998 and examines how the Internet was used to

mediate information about the events happening in Indonesia. His paper shows that there was a strong reluctance from the Chinese state to act over the May 1998 Indonesian riots in which many Chinese women were reportedly gang raped and murdered. The state banned student protests in China because; "[T]he ban should be understood in the context of the clamp-down on independent political activity in the capital that had been in place since the Tiananmen Massacre of 4 June 1989" (Hughes, 2000, p.201). This officially shuts out the traditional physical ways in which the Chinese citizens could voice their anger over political matters. Perhaps most important of all is the paradoxical situation that the Chinese state have found themselves in. On the one hand, they actively promote nationalism to unite the country. Yet, in the political arena, they cannot allow protest in response to political events because any form of protest would subject the state to criticisms and ultimately threaten its legitimacy to rule. As Hughes (2000) observes there is an;

> …increasing need for the state to align itself with the nationalistic outbursts that are becoming a regular occurrence in cyberspace. That the PRC state has found itself increasingly held hostage to an ideology that it has itself encouraged since the Tiananmen Massacre was evident when the authorities found themselves having to provide buses to ship demonstrators to the anti-NATO demonstrations held after the Belgrade bombing. (p. 206)

Hughes provides a valuable insight into what drove the Chinese hacktivists, which we argue to be "the generation of patriotic education", to respond since these are the very first examples of Chinese hacktivism. It is these early examples which helped create their symbolic status as patriotic cyber citizen-warriors. In other words, the internet is a relatively safe place for the Chinese government to allow the expression of anger and which would not provoke the same kind of mass physical political movement as happened at Tiananmen and elsewhere in China during 1989. Hacktivism safely vents the *ressentiment* of national humiliation encouraged by the Chinese government through the patriotic education programme.

So how did the practice of hacktivism spread in China? As noted, Internet forums continue to be a popular social networking tool among the Chinese Web users. Chinese hacktivist groups also use Internet forums as their primary communication tool due to their widespread popularity. Using Akers' social learning theory, it can be demonstrated that an Internet forum facilitates several key components of the learning process behind Chinese hacktivism. Firstly, a forum provides a permanent virtual space for users to find and become *associated* with like-minded others. A forum also facilitates interactions among members with open and private communication channels. This is important because according to Akers (1977);

> most of the learning relevant to deviant behaviour is the result of social interactions or exchange in which the words, responses, presence, and behaviour of other persons make reinforcers available, and provide the setting for reinforcement or are the behaviour reinforcers. (p. 47)

In other words, the forum serves as a place for existing members to consolidate their values and to justify their actions. Second, the forum provides a place for the group to showcase their work to the general public. This has the effect of attracting public attention

and support for the work the existing members are doing, which is also a type of reinforcement. This showcasing also helps to attract new members as the forum essentially attaches a community of supporters to the hacktivism cause, thus giving it a positive definition (Akers et al., 1979, p. 637). Thirdly, the forum serves as a command centre in which preliminary actions can be coordinated and private discussions can be arranged. In general, an Internet forum gives a hacktivist group permanency and the ability to grow. It also represents the lifetime of the group as the posts are recorded.

Before we move on, one possible point of criticism of this approach is that it does not account for hacktivism as a form of challenge, of excitement, or of an escape from boredom, as criminologists such as Jeff Ferrell and others from the cultural criminology tradition might suggest (Ferrell, Hayward & Young, 2008; Webber, 2007b; Young, 2011). It is acknowledged that this is an integral part of the overall picture. But for now, there are clear patterns in the operation of this form of hacktivism that we wish to explore. In the remainder of this paper, we present empirical findings from hacktivist forums to support the argument presented above.

The Rise of the Chinese Cyber Warriors: Cyber Innovation to Overcome Shame and Humiliation

The aim of the following is to examine the potential links between membership growth patterns of the hacktivist online forums and the timing of significant political events in order to find empirical support for the position proposed in this paper. It is argued that the lack of freedom for physical protests has driven some Chinese people to express their emotions online. Consequently, it is then logical to hypothesise that in the event of a major political event that has sparked public outcry, hacktivist groups should experience a surge in membership growth and the hacktivist attacks will focus on specific targets (see also Shalhoub-Kevorkian, 2012). Further, the benefit of using membership data is that it reflects the mass incidental response to specific political events in a holistic manner which cannot be captured so well using qualitative data. What makes hacktivist forums a particularly appropriate source of data for this study, and specifically the trends in membership, is that one does not need to be a member to read or access the majority of forum contents. Therefore, for those who flock to the websites just to read the forum posts in response to publicity and hype from the media, they could do so without being a member. This implies that by becoming a member of a hacktivist forum, one is indicating the desire to be associated with the group's purpose and a willingness to be involved in the group's activities, be it just discussions on the forum or to participate in cyber-attacks. Moreover, one must be a member of the forum in order to participate in attacks. Therefore in this study, we argue that a rise in forum membership would also lead to a rise in the number of hacktivists who would eventually participate in cyber-attacks.

Data sources and data analysis

Since the purpose of this study is to examine hacktivism, it was decided that online hacktivist forums (or Bulletin Board Systems, BBS) would be suitable and without 'off-line' access to those undertaking hacktivism directly. There are several practical and ethical issues that need to be addressed with such data on the Web. This is related to whether or not it is freely published and so an open source of data, the means for its interpretation and analysis, and more importantly with regard to blogs and BBS, the age of the person doing the posting (Battles, 2010; Hine, 2000; 2005; Markham & Baym, 2009; Wakeford, 2000).

In order to minimise ethical issues it was decided to limit the sources of data to quantitative material and forum posts that have been published more widely in traditional media sources. There are two further problems with this data. Firstly, the source of data is critical. The Internet Archive[14] [15]is one of most complete Internet archives available and is a great source of data when studying old web pages, especially those from domains which no longer exist[16]. All data presented in this study is captured from the Internet Archive by querying the domain names of the hacktivist forums listed in table 1.

Table 1. List of famous hacktivist groups

Name	Founder	Domain name	Duration
Green Army	"Goodwill"	isbase.net	1998-2000
China Eagle Union	Wan Tao	chinawill.com, chinaeagle.org	2000-2005
H.U.C. (1st generation)	"lion"	cnhonker.com, cnhonker.net cnhonker.org	2000-2004
H.U.C. (2nd Generation)	"Binger[17]"	chinahonker.com	2005
H.U.C. (3rd Generation)	"Lyon"	honker.net	2010 - present
H.U.C. (3rd Generation)	"Binger"	cnhonkerarmy.com	2010 - present

With regards to the timing of political events, this study uses information primarily from news articles from both the Western and Chinese news agencies, in particular, the timeline of major events in China published by the BBC[18]. Secondly, as shown in table 1, there have been quite a number of hacktivist groups which have been formed and disbanded since 1998 (Henderson, 2007). Therefore, there was a need to select our target groups. Several factors were considered.

Availability of data: the Green Army would be the most ideal subject as they were the earliest group of hacktivists (Henderson, 2007). Unfortunately, the earliest date of data offered by the Internet Archive only dates back to 4th Feb 2001, which is after the group is believed to have disbanded. Thus, the Green Army could not be chosen as a test subject.

The relevance of the group: considering the age of the group, the China Eagle Union would be an ideal alternative to the Green Army. However, the presentation of the group gives no clear indications about their scope of activities. In other words, there is no clear indication whether the group was a pure hacktivist organisation.

[15]The Internet Archive: http://web.archive.org

[16]China's equivalent of the Internet Archive, the Web Infomall: http://www.infomall.cn. Unfortunately, during this study, the Web Infomall was inaccessible for unknown reasons.

[17]Phonetic translation of the hacker's user name "冰儿"

[18]http://news.bbc.co.uk/1/hi/world/asia-pacific/country_profiles/1288392.stm

On the other hand, the relevance of the Honker Union of China (H. U. C.) is clear. The H. U. C. was first created by a famous Chinese hacktivist known as "lion" in late 2000(Henderson, 2007). It is clear that this is a hacktivist group purely dedicated to protecting China because they refer to themselves as the "honkers", which is a transliteration for the Chinese words with the meaning "red hackers", where red is the national colour. Furthermore, the group also has a strict code of conduct[19] which includes the following rules:

- Love your country
- Strictly forbid attacks against any legitimate institutes within the country
- Treat other honkers as your colleagues and share your knowledge
- Uniformly defend the country and respond to defiant acts by foreign countries

Members of the H. U. C. are encouraged to adhere to those rules by the different generations[20] of H. U. C., which are listed in table 1. Therefore, this study focuses on the membership growth over the first decade of the 2000's of the different generations of the H. U. C. from 2001 to 2010.

Hacktivist Forum Membership Growth

In this section, the membership growth patterns of each generation of the H. U. C. are presented and correlated with the timing of key political events which occurred in China.

a. First generation of H.U.C. (2001- 2004)

As already mentioned, there are three generations of the H. U. C. and the first generation was created by "lion" in 2000. Unfortunately, membership data for the group in 2000 is not available on the Internet Archive and data for 2001 is relatively incomplete.

From figure 2, it can be seen the group's membership had a relatively steady growth from January to April and a slight increase before a sudden surge in mid-June which continued beyond July. More precisely, between 15th June 2001 and 23rd June 2001, it was found that the groups' membership surged from 9814 to 16099 and from then on, the growth rate became much sharper than before. The question is what triggered this surge in membership? The authors attribute some of the reasons behind the increase in growth to a major international incident. In early April 2001, a U.S. spy plane collided with a Chinese fighter which killed the Chinese pilot. This sparked outrage across China and subsequently, this led to a hacker war[21] between U.S. hackers and the Honker Union of China. This was widely reported on the news and on 6th May, the popular news portal sina.com published an interview[22] with "lion". The authors believe that this is the key moment for the honkers as it was the first time they became known to the general public and that this is the moment when the label "honkers" became associated with online proactive patriots. Significantly, this increase in awareness led to a membership growth. Clearly, these are people who are aware of hacktivism, and are sufficiently motivated to

[19]http://replay.web.archive.org/20010405092345/http://www.cnhonker.com/cnhonker.htm
[20]http://cnhonkerarmy.com/purpose.htm
[21]http://news.bbc.co.uk/1/hi/world/asia-pacific/1322839.stm
[22]http://tech.sina.com.cn/i/c/65747.shtml

either join, or partake in hacktivist attacks. It is beyond the scope of the present study to outline the demographic characteristics and motivations of these members.

Figure 2. Membership growth of H. U. C. (2001)

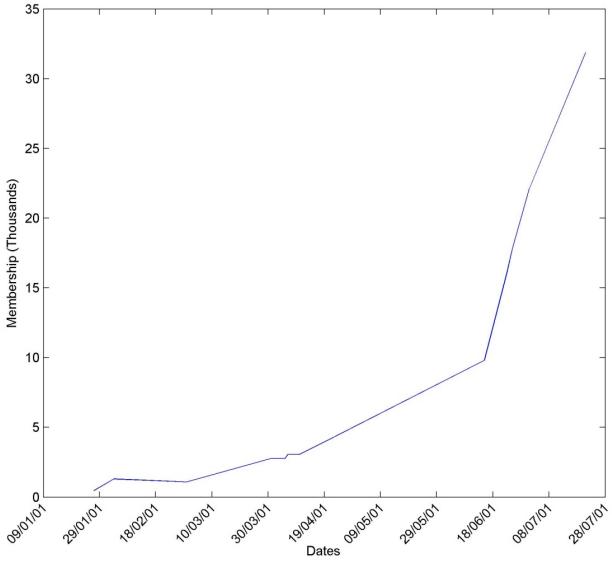
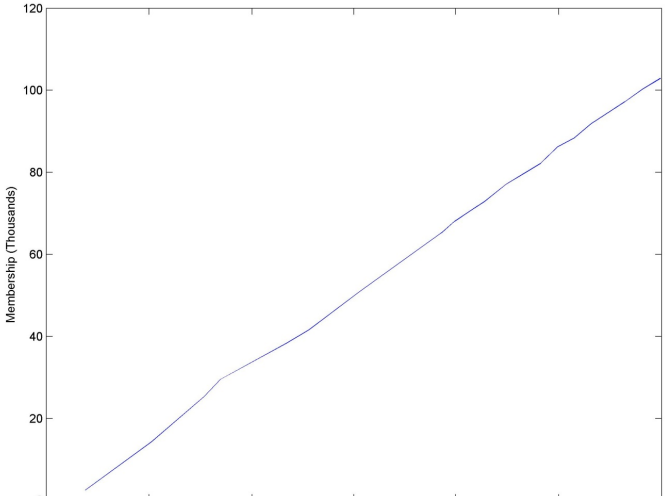


Figure 3. Membership growth of cnhonker.com (2003-2004)

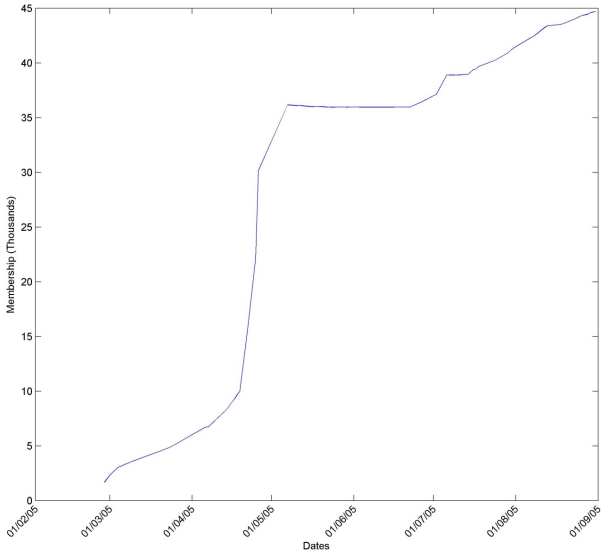


Then on 20th June 2001, Taiwan test-fired the Patriot anti-missile defence system while in the same month, China held a military exercise simulating island invasions. There was a growing concern that China would invade Taiwan. It is argued that this tension added further to the *ressentiment* already built up in the Chinese people during the conflict with the U.S. With the knowledge of such groups now in the public domain, people were able

to express their sense of frustration through membership of these forums. This allowed them to take a proactive approach towards political matters. Oddly, the group was temporarily closed between the end of 2002 and early 2003 but was re-launched from May 2003 to end of 2004. The interesting aspect of this second launch of the H. U. C. by "lion" is that unlike in 2001, the membership growth of the group remained relatively steady throughout 2003 - 2004, as represented by the straight line graph shown in figure 3.

The relatively steady and slower growth during the period from 2003 to 2004 can be explained by the fact that China's foreign relations were relatively stable and that domestic events dominated the period, including the Sars virus outbreak and the first Chinese moon landing. On 31st Dec 2004, "lion" disbanded the H. U. C. and this was the end of the first generation.

Figure 4. Membership growth of chinahonker.com



b. Second generation of H.U.C. (2005)

Soon after "lion" disbanded the first generation of the H.U.C., it was then regrouped by another person known as "Binger" in early 2005. The membership growth of this group is shown in figure 4.

As evident from figure 4, this second generation experienced a sudden surge in membership in April. In detail, the membership surged from 9945 on 19th Apr 2005 to 30151 on 26th Apr 2005, a 203% increase in 17 days. Therefore, it has been shown that there was a sudden increase in forum membership from mid-April to late April. The authors believe that there were two reasons for this. Firstly, there was a mass outcry happening at the time over the Japanese Education Ministry's attempt to omit the atrocities committed by the Japanese Imperial Army in WWII from textbooks. Secondly, on 22nd April, a popular multimedia online portal, qq.com reported[23] that the H. U. C. had in fact already regrouped after its disbandment at the end of 2004.Therefore, it is the

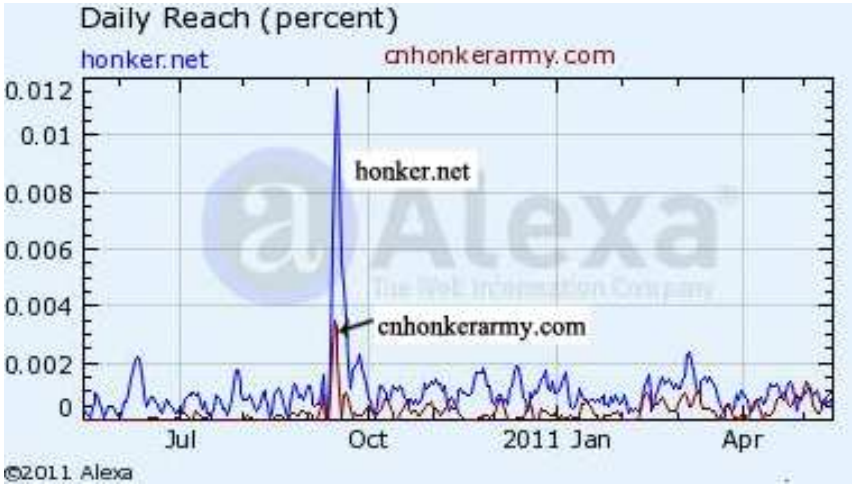
[23]http://tech.qq.com/a/20050422/000071.htm

authors' belief that the surge is attributable to the strong reawakening of *ressentiment* over Japan at the time. The news of the regroup drove those in need of expressing their emotions to the H. U. C. as they already knew about the group's proactive patriotism from 2001.Shortly after the incident this generation of the H. U. C. disbanded at the end of August 2004.

c. Third generation of H.U.C. (2010 – present)

In 2010, there were two separate groups claiming to be the Honkers Union of China: honker.net (previous domain name was chinesehonker.org) was launched in June 2009 and cnhonkerarmy.com was launched in June 2010.

Figure 5. Percentage of daily global reach to the forums



[Source: Alexa Internet (www.alexa.com)]

On the 7th September, the Chinese captain of a fishing trawler was detained by the Japanese navy near the Diaoyu Islands. This caused a public outcry in China. The authors hypothesised that this event should also lead to a surge in membership for the two hacktivist forums. Unfortunately, the Internet Archive could not provide the archived pages for either of the forums and so the authors had no choice but to turn to Alexa,[24] a web traffic monitoring service, and studied the Web traffic data instead. Although it is accepted that data derived from Alexa is not without problems, the patterns observed in this case are so far beyond the norm as to demonstrate a clear trend. The record on the percentage of daily global reach of both forums during the period is shown in figure 5. It is evident from the figure that during mid-September there was an unusually sharp surge in reach for both forums and this surge is found to have coincided with a hacktivist rallying call[25] published on the 11th September 2010 on a forum dedicated to China's fight for sovereignty over the Diaoyu Islands. This rallying call was made by someone proclaiming to be one of the founding members of honker.net and asked people to participate in a forthcoming cyber-attack on Japan planned for the 18th September. 18th

[24] http://www.alexa.com

[25]http://www.cfdd.org.cn/bbs/thread-71680-1-1.html

September 2010 was also the date which marked the 79th anniversary of the "Manchurian Incident" which was said to be staged by the Japanese as the pretext to the invasion of China.

Figure 6. Average time spent on site (minutes) on Chinese hacktivist forums in the last twelve months

[Source: Alexa Internet (www.alexa.com)]

Figure 7. Average daily unique page views per user on Chinese hacktivist sites over the last twelve months

[Source: Alexa Internet (www.alexa.com)]

However, what does this surge in daily reach mean? Figures 6 and 7 present some interesting insights into the sudden surge in daily reach. Although honker.net received the highest surge in traffic, figure 6 shows that it was cnhonkerarmy.com which experienced the highest surge in the average time visitors spent on the site. Similarly, figure 7 shows that it was cnhonkerarmy.com which experienced the highest increase in the number of daily unique page views by the visitors.

Figure 8. Screenshot of a defaced Japanese website published on cnhonkerarmy.com

There are two reasons for honker.net's greater surge in daily reach: firstly, the Web address of the forum was featured on the rallying call. Secondly, on 13th Sept, the founder of honker.net "Lyon" published an official notice saying that the rallying call had nothing to do with honker.net and that he believes such attacks add no value to the country[26]. Subsequently on the 15th September, this notice by "Lyon" featured in the news[27] on sina.com. As honker.net has had such wide media exposure, it is not surprising to find that it had experienced a surge in reach. However, cnhonkerarmy.com did not feature in the media and yet it also experienced a surge in traffic. This indicates that those who were more familiar with hacktivism were also seeking out websites that were not mentioned in the media. Moreover, the surge in the length of time spent on the site and the average number of pages viewed by its visitors as well as the surge in daily reach may be attributed to the fact that cnhonkerarmy.com had announced details of their own set of attacks on Japan, as shown in figure 8.

Therefore, it may be argued that cnhonkerarmy.com's general growth in all three Web traffic benchmarks reflects the users' need to express their emotions by being involved with the hacktivists who are at the "front line" of defending their national identity. This supports Nietzsche and Scheler's view of *ressentiment:*

> [A]s embodying an intense desire for revenge…Both also stressed the inability of those experiencing *ressentiment* to rebel against the agents of their unjust treatment, who are more

[26]http://www.honker.net/News/Notice/2010-09-13/4908.html
[27]http://tech.sina.com.cn/i/2010-09-15/17134659907.shtml

> powerful. Imaginary or symbolic revenge, however, may often take the place of actual retaliation (Meltzer & Musolf, 2002, p. 248).

Furthermore, figures 6 and 7 also provide crucial insights into the behaviour of the users on hacktivist forums at the time of major political events. The sharp increase in both the average time spent and the average daily unique page views per visitor demonstrate that during a major political event, the members of the hacktivist forums become more active on the forums. Thus, this serves as evidence for Jasper's claim that "(e)motions are part of a flow of action and interaction, not simply the prior motivations to engage or the outcomes that follow' (Jasper, 2011, p.16).

In summary, what this data shows is that the membership surges might be seen as a temporary response to situational incidents, but the events are of historical importance. That is, the event that triggers the surge is something that reactivates the longstanding *ressentiment*, a form of chronic strain that is inculcated by the patriotic national education programme. This is akin to a cavity in a tooth that has been filled, but that will flare with pain if a piece of foil is bitten down on: always there in the background, but triggered by a specific catalyst (Agnew, 1992, pp. 60-61).

Conclusion

This paper takes a novel approach to a phenomenon that has hitherto been rendered as a moral panic, with hacktivists as folk devils intent on global Armageddon. It has been argued that the form that hacktivism takes in China is bounded and shaped by social and historical influences, and these have accelerated since the Tiananmen Square massacre in 1989. These hacktivists regard themselves as defending the nation, but without the formal approval of the state. This is a very different form of hacktivism to Anonymous or LulzSec where each of these groups are not bounded and defined by their national identity. There is a fit with various criminological theories, as well as political and sociological approaches. The political demonstrations against the ruling communist party in 1989 led the government to create a national patriotic education programme highlighting the way that China had suffered national humiliation. This sense of social *ressentiment* becomes piqued when an incident occurs that threatens the national identity. The paradox is that the patriotic education programme encourages in-group solidarity and antipathy towards the out-group, but this can rarely be expressed in demonstrations because the government fears a new Tiananmen.

Hacktivism in China developed at about the same time as the education programme started to be rolled out, and in order to demonstrate that this is not just a coincidence, it has also been shown how activity on hacktivist forums rises and falls during incidents of perceived national threat. Hacktivism therefore becomes a safe outlet to vent patriotic anger, and so this form of public hacktivism is not encouraged by the state, but tolerated. Regardless of the complexities of Chinese cybercrime laws, the fact that the hacktivist forums exist openly and publicly demonstrates this (see Qi, Wang & Xu 2009 for a fuller discussion of Chinese cybercrime legislation).

What this research shows is that there is a need for a unique approach to different forms of hacktivism. The distinctive effect of the national humiliation programme coupled with restrictions on demonstrations is a more complete way to understand this form of behaviour. What we suggest is that this is an approach that supersedes the security-oriented perspective, whereby the security industry takes a top-down approach to risk management.

The perspective we take allows for a fuller understanding, a bottom up approach that reflects on the social, cultural and historical factors that we argue underpin some forms of hacktivism. We believe such an approach allows for the target of an attack to have the ability to better anticipate likely threats. However, what this also allows for is the acknowledgement that some forms of hacktivism reflect legitimate grievances and cannot just be understood at the level of criminal law or computer science. Lastly, hacktivism has developed in other countries that have tried to prevent public demonstrations, such as throughout the middle-east during the uprising of the 'Arab Spring', and between Palestinians and Israelis (Greylogic, 2009; Lacey, 2011). A properly criminological account can present a theoretical synthesis that helps in our understanding of a new and complex form of citizen activism.

Acknowledgement

This research was funded by the Research Councils UK Digital Economy Programme, Web Science Doctoral Training Centre, EP/G036926/1.

References

Agnew, R. (1992). Foundation for a general strain theory of crime and delinquency, *Criminology, 30*(1), 47-87

Agnew, R. (2010). A general strain theory of terrorism. *Theoretical Criminology*, *14*(2), 131-153.

Agnew, R. (2011). Crime and time: The temporal patterning of causal variables. *Theoretical Criminology, 15*(2), 115-139.

Agnew, R. (2012). Dire forecast: A theoretical model of the impact of climate change on crime. *Theoretical Criminology, 16*(1), 21-42.

Akers, R. L. (1977). *Deviant Behavior: A Social Learning Approach* 2nd ed., California: Wadsworth.

Akers, R. L. Krohn, M. D. Lanza-Kaduce, L., & Radosevich, M. (1979). Social Learning and Deviant Behavior: A Specific Test of a General Theory. *American Sociological Review*, *44*(4), 636-655.

Akers, R. L. (1998). *Social Learning and Social Structure: A general theory of crime and deviance,* Boston: Northeastern University Press.

Battles, H. T. (2010). Exploring ethical and methodological issues in internet-based research with adolescents. *International Journal of Qualitative Methods*, *9*, 27-39.

Bodford, J. E., & Kwan V. S. Y. (2018), A Game Theoretical Approach to Hacktivism: Is Attack Likelihood a Product of Risks and Payoffs?. *Cyberpsychology, Behavior, and Social Networking*, *21*(2), 73-77. doi: 10.1089/cyber.2016.0706.

Bond, M. H., & Hewstone, M. (1988). Social identity theory and the perception of intergroup relations in Hong Kong. *International Journal of Intercultural Relations*, *12(*2), 153-170.

Braithwaite, J. (1989). *Crime, Shame and Reintegration,* Oxford: Oxford University Press.

Braithwaite, J.. (1993). Shame and Modernity. *The British Journal of Criminology, 33*(1), 1-18

Burgess, R. L., & Akers, R. L. (1966). A Differential Association-Reinforcement Theory of Criminal Behavior. *Social Problems, 14*, 128-147

Caldwell, T. (2015). Hacktivism goes hardcore. *Network Security, 5*, 12-17.

Callahan, W. A., (2004). National Insecurities: Humiliation , Salvation , and Chinese Nationalism. *Alternatives*, *29*, 199-218.

Canter, D., & Alison, L. (2000). The Social Psychology of Crime: Groups, Teams and Networks. In D. Canter and L. Alison (eds.), *The Social Psychology of Crime: Groups, Teams and Networks* (pp. 3-20). Hampshire, England: Ashgate Publishing.

Castells, M. (1996/2000). *The Information Age: Economy, Society and Culture. Volume 1: The Rise of the Network Society*. Oxford: Blackwell.

Chander, D. (2016). Securing the Anthropocene? International policy experiments in digital hacktivism: A case study of Jakarta. *Security Dialogue, 48*(2), 113-130.

Cloward, R., & Ohlin, L. (1960). *Delinquency and Opportunity* London: Collier-MacMillan.

Cohen, A. (1955). *Delinquent Boys: The Culture of the Gang* New York: Free Press.

Cohen, S. (1972/2002). *Folk Devils and Moral Panics: The Creation of Mods and Rockers*. (3rd Edition with revised Introduction), London: McGibbon and Kee.

Crime Survey for England and Wales (2017). Retrieved from https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingmar2017.

Denning, D. E., (2001). Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing. In J. Arquilla & D. Ronfeldt, (eds.), *Networks and Netwars: The Future of Terror, Crime, and Militancy* (pp. 239-288). Santa Monica: RAND Corporation.

Deseris, M. (2017). Hacktivism: On the Use of Botnets in Cyberattacks. *Theory, Culture and Society, 34*(4), 131-152.

Ferrell, J., Hayward, K., & Young, J. (2008). *Cultural Criminology: An Invitation*. London: Sage

Fuchs, S. (2014). Hacktivism and Contemporary politics. In D. Trottier and S. Fuchs (eds.), *Social Media, Politics and the State: Protests, Revolutions, Riots, Crime and Policing in the Age of Facebook, Twitter and YouTube* (pp. 88-106). London: Routledge.

Garland, D. (2008). On the concept of moral panic, *Crime Media Culture, 4*(1), 9-30.

Greylogic (2009). *Project Grey Goose Phase II Report: The evolving state of cyber warfare*. Retrieved from http://www.scribd.com/doc/13442963/Project-Grey-Goose-Phase-II-Report.

Gurr, T. R. (1970). *Why do Men Rebel?*. Princeton, N.J.: Princeton University Press.

Hall, S., & Jefferson, T. (eds.) (1976). *Resistance through ritual: Youth subcultures in post-war Britain,* London: Unwin Hyman.

Henderson, S. (2007). *The Dark Visitor*. Lulu Press.

Hine, C. (2000). *Virtual ethnography*. London: Sage Publications.

Hine, C. (2005). *Virtual methods: Issues in social research on the Internet*. Oxford: Berg.

Holt, T. J., Freilich, J. D. & Chermak, S. M. (2017). Exploring the Subculture of Ideologically Motivated Cyber-Attackers. *Journal of Contemporary Criminal Justice. 33*(3) 212–233.

Hughes, C. R., (2000). Nationalism in Chinese cyberspace. *Cambridge Review of International Affairs*, *13*(2), 195-209.

Jasper, J. M. (2011). Emotions and Social Movements: Twenty Years of Theory and Research. *Annual Review of Sociology*, *37*, 285-303.

Jordan, T., & Taylor, P. (2004). *Hacktivism and Cyberwars: Rebels with a cause?* London: Routledge.

Jefferson, T. (2002). 'For a psychosocial criminology'. In K. Carrington and Hogg, R. (eds.), *Critical Criminology: Issues, debates, challenges* (pp. 145-167). Devon: Willan Publishing.

Jewkes, Y. (ed.) (2002). *Dot.cons: Crime, deviance and identity on the Internet.* Cullompton, Devon: Willan.

Jewkes, Y. (2011). *Media and Crime, 2nd Edition,* London: Sage.

Karatzogianni, A. (2015). *Firebrand Waves of Digital Activism 1994-2014: The Rise and Spread of Hacktivism and Cyberconflict.* London: Palgrave MacMillan.

Lacey, D. (2011). The Role of Humiliation in the Palestinian / Israeli Conflict in Gaza. *Psychology*, 4(1), 76-92.

Lea, J. (1992). The Analysis of Crime. In J. Young & R. Matthews (eds.), *Rethinking Criminology: The Realist Debate* (pp. 67-94). London: Sage.

Lea, J., & Young, J. (1984/1993). *What Is To Be Done About Law and Order?* London: Pluto Press.

Lucas, G. (2017). State-Sponsored Hacktivism and the Rise of Soft Power. In M. L. Gross & T. Meisels (eds.), (2017). *Soft War: The Ethics of Unarmed Conflict* (pp. 77-87). Cambridge: Cambridge University Press.

Maguire, M. (2007). *Hypercrime: The New Geometry of Harm.* Abingdon, Oxon: Routledge Cavendish.

Manion, M., & Goodrum, A. (2000). Terrorism or Civil Disobedience: Towards a Hacktivist Ethic. *Computers and Society, 30*(2), 14-19.

Markham, A. N., & Baym, N. K. (2009). *Internet inquiry: Conversations about method* Thousand Oaks: Sage Publications.

Meltzer, B. N., & Musolf, G. R. (2002). Resentment and Ressentiment. *Sociological Inquiry*, *72*(2), 240-255.

Merton, R. K. (1938) Social Structure and Anomie. *American Sociological Review, 3*(5), 672-82.

Mummendey, A., Kessler, T., Klink, A., & Mielke, R. (1999). Strategies to cope with negative social identity: Predictions by social identity theory and relative deprivation theory. *Journal of Personality and Social Psychology, 76*(2), 229-45.

Negroponte, N. (1996). Being Digital, New York: Vintage Books.

Qi, M., Wang, Y., & Xu, R. (2009), Fighting cybercrime: legislation in China, *International Journal of Electronic Security and Digital Forensics, 2*(2), 219-227.

Reicher, S. (1987). Crowd Behaviour as Social Action. In J. C. Turner, M. A. Hogg, P. J. Oakes, S. D. Reicher & M. S. Wetherell (eds.), *Rediscovering the Social Group: A Self-Categorization Theory* (pp. 171-202). Oxford: Blackwell.

Reicher, S. (1996). "The Battle of Westminster": Developing the Social Identity Model of Crowd Behaviour in Order to Explain the Initiation and Development of Collective Conflict. *European Journal of Social Psychology,* 26(11), 115-34.

Runciman, W. G. (1966). *Relative Deprivation and Social Justice.* London: Routledge and Kegan Paul.

Scheler, M. (1915/1998). *Ressentiment.* Milwaukee, Wisconsin: Marquette University Press.

Shalhoub-Kevorkian, N., (2011). E-Resistance and Technological In/Security in Everyday Life, *The British Journal of Criminology*, *52*(1), 55–72.

Tajfel, H., & Turner, J. (1979) An Integrative Theory of Intergroup Conflict. In W.G. Austin & S. Worschel (eds.), *The Social Psychology of Intergroup Relations* (pp. 33-47). Monterey, CA: Brooks/Cole.

Tajfel, H., & Wilkes, A. L., (1963). Classification and Quantitative Judgement. *British Journal of Psychology*, *54*(2), 101-114.

Tanczer, L. M. (2016). Hacktivism and the male-only stereotype. *New Media and Society, 18*(8), 1599-1615.

Taylor, P. (1999). *Hackers: Crime in the Digital Sublime*. London: Routledge.

Taylor, P. A. (2001). Hacktivism: in search of lost ethics? In D. S. Wall (ed.), *Crime and the Internet* (pp. 59-73). London: Routledge,

Taylor, P. A. (2005). From Hackers to Hacktivists: speed bumps on the global superhighway? *New Media and Society,* 7(5), 625-646.

Turkle, S. (1995/1997). Life on the Screen: Identity in the Age of the Internet. New York: Touchstone.

Van Zomeren, M., Postmes, T. & Spears, R. (2011). On convictions collective consequences: Integrating moral conviction with the social identity model of collective action. *British Journal of Social Psychology, 51*(1), 52-71. doi: 10.1111/j.2044-8309.2010.02000.x.

Verizon (2012), *2012 Data Breach Investigation Report.* Retrieved from http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf.

Van Hardeveld, G. J., Webber, C., & O'Hara, K. (2017). Deviating from the cybercriminal script: exploring tools of anonymity (mis)used by carders on cryptomarkets. *American Behavioral Scientist*, *61*(11) 1244-1266.

Wakeford, N. (2000). New Media, New Methodologies: Studying the Web in D. Gauntlett (ed.), *web.studies: Rewiring Media Studies for the Digital Age* (pp. 31-41) London: Arnold,

Wall, D. (2008). Cybercrime and the Culture of Fear: Social science fiction(s) and the production of knowledge about cybercrime. *Information, Communication & Society, 11*, 861-884.

Wall, D. (2010). Criminalising cyberspace: the rise of the Internet as a crime problem in Y. Jewkes & M. Yar (eds.),*The Handbook of Internet Crime* (pp. 88-103). Cullompton, Devon: Willan,

Wang, Z. (2008). National Humiliation, History Education, and the politics of Historical Memory: Patriotic Education Campaign in China. *International Studies Quarterly, 52,* 783-806.

Webber, C., (2007a). Revaluating relative deprivation theory. *Theoretical Criminology*, 11(1), 97-120.

Webber, C. (2007b). Background, Foreground, Foresight: The third dimension of cultural criminology? *Crime Media Culture*, *3*(2), 139-157.

Webber, C. (2010). *Psychology and Crime*. London: Sage.

Webber, C., & Vass, J. (2010). Crime, film and the cybernetic imagination. In Y. Jewkes & M. Yar (eds.), *Handbook of Internet Crime* (pp. 120-144). Devon, UK: Willan.

Webber, C., & Yip, M. (2012). Drifting on and off-line: humanising the cyber criminal, In S. Winlow, & R. Atkinson (Eds.), *New Directions in Crime and Deviancy* (pp. 191-205). Abingdon, GB: Routledge.

Yar, M. (2005). The Novelty of Cybercrime: An Assessment in Light of Routine Activity Theory. *European Journal of Criminology, 2*(4), 407-427.

Yar, M. (2006). *Cybercrime and Society*. London: Sage.

Yip, M., Webber, C., & Shadbolt, N. (2013). Trust among cybercriminals? Carding forums, uncertainty and implications for policing. *Policing and Society*, *23*(4), 516-539.

Young, J. (1971). *The Drugtakers,* London: Paladin

Young, J. (2007). *The Vertigo of Late Modernity*. London: Sage.

Young, J. (2011). *The Criminological Imagination*. Cambridge: Polity Press

Zhao, S., (1998). A state-led nationalism: The patriotic education campaign in post-Tiananmen China. *Communist and Post-Communist Studies*, *31*(3), 287-302.