CRIMINALIZING YOUTH POLITICS¹

Judith Bessant²

Abstract: The present article aims to analyze the contemporary political theories which affirm that the use of the new media - mainly the internet - for politics online would replace more traditional means of democratic participation. Its scope is understanding the political motivations of the individuals - primarily the youth - involved in these direct actions like the use of DDoS, and also its criminalization by the State, indispensable to the understanding this new form of political activism.

1

Keywords: Slacktivism; DDoS; Hacktivism; Cyberpolitics; Democratic Participation.

1. Introduction

A large and growing body of research and theory testifies, young people drawing on digital media have mobilized support for democratic principles like freedom of speech and assembly and for institutions like free elections since the early twenty first century. New media has been used in direct political action like Distributed Denial of Service activities. The new media have also been used by organizations like Wikileaks to publish unprecedented amounts of intelligence data and diplomatic documents which revealed the illegal conduct of many western governments. Digital media has been central to movements like the anti-Austerity campaigns in Europe (2008+), the global Occupy movement (2009+) and prodemocracy movements driving the 'Arab Spring' (2010+). In response, many governments including those identifying as liberal democratic have moved to criminalize these forms of dissent.

Against the criticism that online political action (eg 'slacktivism') is replacing more traditional forms of political action, I argue here that new media involving activities like those just mentioned augment and enhance political participation and the public sphere. While digitally based action can create its own discrete forms of activism it is also often a component of actions involving off-line action, thereby integrating online and offline activities.

1 Paper submitted and acknowledged in November 1st 2016.

2 Professor, RMIT School of Global, Urban and Social Studies (Melbourne, Australia). PhD, La Trobe University.

2. A Sense Of The Problem

To appreciate efforts by governments and other organizations to criminalize or regulate various forms of political activity, I offer a brief survey of the context. This is not to presume that criminalization of dissent is a new phenomenon, indeed it has a long history. It does however appear to be intensifying and involves increasing numbers of young people.

A scholarly consensus exists that the past few decades have seen dramatic increases in popular anxiety about crime and official reactions to that concern (GARLAND, 2001). Opinion polls indicate that crime is the source of considerable fears and 'law 'n order' has become a staple in most election campaigns across the globe. Western governments everywhere became purveyors of 'risk governance', evident in their increased use of surveillance technologies, the deployment of more police and calls for a more punitive approaches to 'offenders' (CARLEN, 2009).

It is possible to be precise about when popular concern over terrorism and security began and when governments started introducing measures ostensibly designed to protect their citizenry. The 11 September 2001 was when we began living with 'a permanent fear of terrorism' (AOUDE, 2002). Those attacks unleashed an American-led 'war on terror' urged on by political posturing and calls for sacrifice to ensure national security.

As a result, many western states began shifting the balance towards security at the expense of civil liberties and human rights. As HOGG notes, legal academics and lawyers were 'deeply' concerned about the fate of the rule of law and liberal democratic institutions in the 'war on terror' (2007, p.84). Hocking similarly observed, developments since 2001 in western democratic states of counter-terrorist law and policy have allowed 'for the preemptive control of political conflict and dissent, which may or may not protect individual citizens but which certainly protects the state itself' (2003, p.371).

Against this backdrop we saw the increased criminalization of traditional political protests or public assembly in democracies like the UK and USA which included the regular use of 'anti-terror' legislation. In this context the potential of a 'threat' 'justified' use of mass police action and anti-personnel weapons against civilians.

In Australia the Australian Defence Legislation Amendment (Aid to Civilian Authorities) Act 2000 became a benchmark for dealing with protestors. Similar amendments in other countries saw increases state powers to search, seizure and detain without a warrant or formal arrest. In 2010 the G20 'March for Justice Toronto', Canada saw a 10,000 strong police contingent corral protestors into confined spaces where they were contained for hours

(SALTER, 2011, p. 211-238). They were tactics repeated in the UK against students protesting education funding cuts and other "austerity" measures.

Animal and environmental groups faced court as some corporations intensified their efforts to criminalize dissent. Meanwhile specific groups and individuals are described as 'domestic terrorists' and 'eco-terrorists', language embedded in legislation like the US Patriot Act. Similarly young satirists, like the Spaniard, Facu Diaz, are charged with breaches of anti-terrorist laws and breaching the 'glorification of terrorism laws' for mocking the government (BERRERDA, 2015).

As revelations by whistleblower Snowden indicate, some governments led by the US extend the scope of their electronic surveillance to track all citizens on the premise we are potential criminals or terrorists. Since 9/11 many governments expanded their already extensive surveillance technologies to retain and analyze mega-data without the regulation implicit in judicial warrants.

3. Liberal Democracies

While there may be little surprise when authoritarian or one-party states criminalize dissent, there is good reason to be surprised when liberal democratic states repress legitimate dissent

Brabazon asks if liberal democracies pride themselves on civil liberties like freedom of association and democratic rights like the right to free and contested elections, 'Why would these states and their decision-makers not welcome social movements and dissent of all kinds as a natural part of the rich fabric of citizen participation in decision-making?' (2006, p. 3). In this article I ask how might scholars in the fields of youth studies and social science generally, understand such criminalizing processes? How should we make sense of moves to criminalize dissent involving young people engaged in new forms of on-line political activity like Distributed Denial of Service activism.

To address these questions I clarity what is meant by 'the political'. I argue, a significant obstacle to inquiring into contemporary youthful politics relates to the ways 'the political' has been understood. Quite divergent assessments of young people's politics exist (MANNING, 2009; FARTHING, 2010; BESSANT 2004 and 2014). Young people tend to be either chastised as apolitical heralding a 'crisis of democracy', or hailed as the progenitors of technologically mediated forms of new politics. This binary reveals differences in how 'the political' is understood.

They are differences that can be conceptualized in a few ways. One way is to focus on

the incapacity of liberalism to apprehend the political (MOUFFE, 2005). For Mouffe proponents of liberal tradition assume that individualism, rationality and pursuit of consensus define the modern practice of politics (2005). That is, liberal accounts of politics expressed in the deliberative democracy tradition rely on restricted framings of the political, ones that omit the value of opposition and dissent, while acting 'as-if' dissent is valued.

My own argument aligns with Ranciere's view that 'the essence of politics is dissensus' (2010 p. 38; MOUFFE, 2005). It is a notion of dissensus understood not simply as conflict between interests, opinions, or 'values', but as a reconfiguration of the status-quo, as a rearrangement of more common experiences or what is sensible and known.³ (RANCIERE, 2010, p. 69).

I begin with a case study to identify a distinctive form of political activism - DDoS then offer a brief account of how youth studies and social science make sense of this politics, then use a heuristic to analyse responses from the state to it, which include the criminalization.

4. Distributed Denial Of Service Action

DDoS is designed to make a computer or network of computers temporarily or indefinitely unavailable. It involves mobilizing numerous computers to target a website at a set time so the site is inundated with traffic until it reaches maximum capacity after which it cannot process requests, or if it can, it does so slowly. Typically this does not compromise the security of files or databases of the site. DDoS are the digital equivalent to traditional protests like sit-ins, that flood a space, create bottlenecks, disrupt or deny access (SAUTER, 2014).

DDoS is used for political protest. It's used by collectives like 'Anonymous' and can involve thousands, even millions of people. Government sites in the USA, Israel, Australia, Tunisia, Uganda, Tunisia, Egypt, Libya and Yemen have been subject to DDoS action as part of anti-government protests. DDoS have been used in anti-Church of Scientology campaigns, and in protests against the CIA and against gaming companies like Sony and Nintendo. LulzSec, Anonymous and others targeted credit and payment companies like PayPal and MasterCard in retaliation to their decision to suspend processing payments to WikiLeaks after WikiLeaks disclosed 'classified documents' to the public. Each of these actions were motivated by interests in securing liberal values like public accountability, freedom of information, speech, and the right to privacy (COLEMAN, 2014).

³ While we cannot live well in states of constant disagreement and there needs to be appropriate limits to pluralism (eg exclusion of fascism), what exists now is too far along the continuum of securing consensus and compliance at the expense of an open society (Unger 2014).

DDoS activism was also used in the USA when the US Congress attempted to enact the *Stop Online Piracy* (SOPA) legislation in 2011-2012. If it had passed it would have expanded the powers of law enforcement by criminalizing certain online activities backed by penalties of up to five years imprisonment. The use of DDoS helped persuade Congress to drop the legislation. DDoS was part of a mass demonstration by approximately 9,000 people who targeted government departments like the FBI and Department of Justice who were supportive of the legislation (BESSANT, 2014).

There are also closely related activities like DNS Zone transfers which re-direct users from one site to another. An example of this took place in 2011 in the wake of the UK News Corporation phone-hacking scandal which saw activists hack the British tabloid's website. *Sun-Herald* readers were directed from the newspaper's website to a mock site which carried a fake headlines announcing that the paper's owner, Rupert Murdock was dead. It produced caused disruption and the temporary closure of the websites for *The Sun*, *The Times*, BSkyB and *News International* (MOSES and GARDINER, 2011).

Actions like these often spill off-line and on to the streets. 'Zombie flash mobs' were part of the anti-Scientology campaign run by Anonymous which saw thousands of people dressed as ghoulish zombies walking or roller-skating along the streets of New York City to occupy the front of the scientology Church on a monthly basis.

When asked about their motivations, activists point to a mix of political reasons. Some refer to the fun involved (the 'lulz'), and the thrill of transgression that comes from 'straddling serious political protest and carnivalesque shenanigans' (COLEMAN, 2014). Many participants are best described as political provocateurs and saboteurs committed to exposing shoddy security systems, racism, and other unfair practices In many case their interest can be traced back to 4chan imageboard launched in 2003 (ibid).

5. Understanding The 'Political' And Young People's Politics

While it is difficult to make too many generalizations about a field as eclectic as 'youth studies', it can be said that mainstream youth studies attempts to offer a 'neutral' and 'objective' research that informs law, policies and programs for young people. The oldest versions of this intellectual practice drew on 'classical sociological-functionalist' social control narratives, presenting 'youth transition models' reliant on successful-failed socialization models which encourage an interest in 'delinquent' and 'criminal' young people. More recently mainstream youth studies embraced a 'risk society discourse' (GIDDENS,

1991; BECK, 1992) and an accompanying 'individualisation thesis' which argues that 'traditional' 'social structures' like gendered expectations about work, family formation or class-based structuring of education and employment have been weakened as we transited from modernity to 'late modernity'.

The result is a equivocal political framework, with the tendency to talk about 'youth at risk' becoming 'the fulcrum of the basic ideological and strategic tensions' that inform youth studies and associated human service practices (POYNTING and WHITE, 2004, p. 40). This is said to produce tensions or uncertainty about whether to support 'social justice' or a 'social control function'. The interest in social justice promotes 'radical forms of advocacy and collective youth empowerment' while a 'social control' function promotes a 'treatment model or conservative advocacy' (POYNTING and WHITE, 2004, p. 40).

The underlying problem becomes clearer when paying attention to how the political is conceived within fields of inquiry into young people politics. As I document here the contradictory stories about young people and politics point to important differences about how we conceptualize the political.

6. Young People As Apolitical

A large body of research indicates that young people are disengaging from political life and civic participation (KIMBERLEE, 2002; HENN at al 2002; HENN et al 2006; ARVANITAKIS and MARREN, 2009). It's a pessimistic, even alarmist account that began emerging in the 1990s which highlights disengagement, declining electoral participation and trends towards 'depoliticization' by many young people. Young people we are told are the most apolitical generation ever and threaten the future of liberal democracy (BAUERLEIN, 2009).

It is an account that often draws on 'risk' discourses (BECK, 1992; GIDDENS, 1991), ideas about 'liquid modernity' (BAUMAN, 2000), the break-down of traditional identities and practices, and 'life-cycles' or what some call changing 'life patterns and personal biography' (MAYER, 2003). It also relies on long-standing problem setting agendas about 'youth deficits' (OSLER and STARKEY, 2006; ARVANITAKIS and MARREN, 2009) and stereotypes of 'youth as trouble and troubled', as a narcissistic generation replete with a sense of 'entitlement' (TWENGE, 2009). Such deficit models are used to explain how 'they' are 'unmotivated and unskilled. This, we are told, is because key social institutions failed to educate, to cultivate the requisite civic dispositions and values. Given this framing, 'the solution' is more civics education designed so 'they' can understand their obligations to vote

and engage civically.

7. Young People As Political

A second and different account of young people's politics recognizes the political engagement of many young people. This account relies on evidence that many young people have clear civic identities and are engaged on-line and off-line (MARTIN, 2012; VROMEN and COLLIN, 2010; XENOS et al, 2014). It identifies civic values, a variety of political activism (BENNETT et al, 2009; WEINSTEIN, 2014; p. 210-233), and pays attention to what is happening digitally as possibly the beginning of significant changes in how we practice and understand politics.

One thing this binary highlights is a problem with the way the political is conceptualized.

It's this binary that overlooks the complexity of young people's relationship with contemporary politics (BESSANT, 2014; MANNING, 2009; FARTHING, 2010). As O'Toole et al., argue, without understanding how young people define 'politics' it is difficult to demonstrate they are disengaged (2003, see also MARTIN, 2012).

For McCaffrie and Marsh:

'a pervasive problem with the mainstream participation literature [is that] a restrictive conception of politics forces a restrictive understanding of participation' (2013, p. 116).

Indeed the limited ways people are encouraged to think about politics which often discounts their own political activity, may indicate reasons for their apparent disinterest in conventional politics.

There is plenty of evidence that many young people now operate with different and broader understandings of politics as 'participatory politics'. Yet unlike traditional political activity, it's highly interactive, peer-based, and not guided by traditional institutions like political parties or newspaper editors (*eg*, COHEN and KAHNE, 2012; KAHNE et al, 2014).

The absence of clarity about the political is often apparent in research reliant on quantitative techniques that aim to 'measure' young people's political disengagement or engagement. It is an approach that tends to see researchers assume they 'share a common understanding about the definition and meaning of politics' (HENN et al 2002, p. 168-169). Yet as McCaffrie and Marsh argue, these studies don't address what young people understand the 'political' to be (2013, p. 113). They continue: 'a pervasive problem with the mainstream participation literature [is that] a restrictive conception of politics forces a restrictive understanding of participation' (2013, p. 116).

With this in mind it becomes clearer how an overly restrictive concept of the political produces restrictive understandings of politics and political participation.

8. The Political

While a comprehensive discussion of 'the political' is beyond the scope of this article some consideration of what is meant by 'the political' is needed.

There are two related points made by a body of distinguished critics of contemporary liberal politics. One is that certain defining features of liberalism, like its privileging of rationality and consensus have helped erode a normative conception of the political as an inherently 'agonistic' enterprise (*eg* MOUFFE, 2005; UNGER, 2014). The other points to the ways liberal states often create 'states of exception' (AGAMBEN, 2005) as they breach constitutive principles of liberalism, like the rule of law and rights to freedom of speech and assembly in pursuit of order and 'security'. As my case study indicates, ostensibly liberal states are also repressing valuable kinds of political practice involving young people.

Some contemporary theorists refer to a crisis of liberal democracy (MOUFFE, 2005; FUREDI, 2005). For Mouffe, too many proponents of liberalism are 'blind to... the political in its dimension of conflict-decision' and cannot perceive the value of opposition in political life (2005 p. 3). As Unger argues, the liberalism assembled over many centuries (by *eg* Locke, Kant, Bentham, Mill and Rawls) privileges an excessively rationalist, universalist and individualist conception of human being and society (1977). It's a liberalism that assumes that rational consensus is possible, that it can eliminate conflict, that it's preferable to dissent and protest, and that electoral politics is the essential institutional device for a democratic polity. Habermas added the idea that a 'public sphere' connects rational deliberation to the democratic political process (1989).

Mouffe's point becomes clearer when she distinguishes between *antagonism* and *agonism*. *Antagonism* is a 'we-they' relationship where those involved are 'enemies' and do not share common ground. *Agonism* refers to a 'we' relationship in which conflicting parties declare commitments to shared ethical-political principles (*eg* liberal democracy). While agonists acknowledge there may be no immediate, or even long-term solution to their differences, they nonetheless recognize the legitimacy of their opponents' opposition and its value for democratic processes. Significantly that shared commitment makes them 'adversaries' not 'enemies'.

The preference for consensus over conflict and 'blindness' to the value of opposition

encourages a taming of conflict and dissent. It encourages a movement to the centre so options 'too far' from that midpoint come to be seen as 'extremist'. It is a tendency exacerbated by the rise of a neo-liberal political imaginary that promote the 'economisation' and 'technicisation' of politics which represent conflict as a source of economic inefficiency or political dysfunction (TULLOCK and BUCHANAN, 1962). All this depletes the public sphere.

At the same time a different but parallel criticism draws on the early twentieth century political theorists Carl Schmitt's critiques of liberalism in which he pointed out how liberal democracies are not consistently liberal especially when facing real or imagined threats to social order posed by internal enemies or external threats. Schmitt argued that while many may assume liberal cultures uphold democratic values (the rule of law, freedom, justice, and equity before law), they regularly suspend legal principles, constitutional practices and values when faced with national emergencies like war, civil riot or attempted coups (SCHMITT, 1988; also AGAMBEN, 2005). For this reason we act 'as if' these values and practices are central to democratic politics when they are not.

Contemporary theorists have applied Schmitt's critique of modern liberalism (AGAMBEN, 2005). Schmitt's conception of the political emphasized an existential will to power presupposing that anything a state needed to do to secure itself was right. Schmitt pointed to the ways Anglo-American liberal democracies were nihilist given the hegemony exercised by legal positivism and utilitarianism.

Other critics coming from different perspectives drew the same conclusions about the nihilism of liberalism arguing that liberal societies too easily accept the legal positivist proposition that for a law to be legitimate it only had to made by the state (FINNIS, 1980; SANDEL, 1997). Within the legal positivist and utilitarian traditions the 'why' question about the purpose or *telos* of political action went missing. So too did consideration of what constituted a good life and just society.

These insights into the paradoxes of liberal democracies are evident when observing moves to criminalize digital activism which itself is predicated on an appreciation of criticism, liberal values and alternate visions of the world and a preparedness to question common-sense understandings. If it is the case, as I argue here, that criminal and other laws are being used to repress dissent in contemporary liberal polities by targeting new forms of political activism, this ought to be a point of concern for critical scholars.

I now consider processes of criminalizing certain forms of political activism and its implications for democracy.

9. Criminalizing Youth Politics

The idea that states criminalize activities seen to threaten a given conception of the social or political order or the interest of elites is hardly new. Similarly the idea that justice and legal systems work primarily to promote and secure the interests of the powerful is not new (PLATO apud SACHS, 2007). Social elites rely on sections of the population whose labour and services secure their access to wealth, culture, status and power. Not surprisingly elite groups can feel threatened by the very existence of those on whom they rely for that privilege and exercise their influence to ensure the law protects their interests. As writers like Muncie argue, understanding crime entails understanding how power is exercised, how it is used to name certain conduct as illegal and how police regulate certain transgressions while ignoring others (2000). Criminalization is seen as one of several regulatory approaches and practices authorized by the state (ROBERTS, 1997), and an approach to crime control that leans heavily on threatening 'criminal penalties, criminal prosecution, and punishment' (SHOVER, 2003, p. 500). The focus is on criminal law-making in particular and the development of a body of law more generally. As JENNESS argued 'criminalization is a form of social control....' (2004, p. 149).

While the process of criminalization in general has received some attention in youth studies it has received more attention in other social science disciplines. The work that has been done clearly challenges conventional representations of crime and the law as 'neutral' practices or the result of the application of 'objective' normative standards (WHITE, 1992; YOUNG, 2008). Scholars like Husack (2007) and Lacey (2004; 2009) have tracked the accentuation in the scope and intensity of criminalization in advanced democracies over the past few decades. Lacey argues that laws are products of political processes (2009). Others documented the increased prominence of criminalization of street crime in the UK and the USA (HUSACK, 2007; LACEY, 2004; 2009).

Some scholars have more specifically been interested in processes that lead to young people being criminalized. It is a field of inquiry that engaged generations of critical researchers from symbolic interactionists to the Birmingham School to post-structuralists. Jenness surveyed a body of work addressing processes of criminalization but neglected the criminalization of political dissent (2004). Similarly a survey of criminalization processes in youth studies by Scraton frames criminalization in traditional ways referring to efforts by states to manage 'disruptive behaviours', and political-economic marginalization involving 'combinations of material deprivation, restricted opportunity, access to drugs and alcohol,

conflict and violence directed against the self and others ...(2008 p.9). Again the criminalization of political dissent is missing.

The literature addressing the criminalization of political dissent is not large.

According to Matza criminological positivists succeeded in separating the study of crime from the workings and theory of the state (1969, p.143). Hogg notes that criminologists and sociologists tend to be guided by the criminal law in adopting an apolitical concept of crime. Thus limited attention has been given to the political power to criminalize (2007 p.83). Yet Hogg's own inquiry into 'political crime' focuses on security, war and terrorism and overlooks the criminalization of political dissent. Here lies a link, as scholars like Hocking observe, developments since 2001 of counter-terrorist law and policy in western democratic states has allowed 'for the pre-emptive control of political conflict and dissent, which may or may not protect individual citizens but which certainly protects the state itself' (2003, p. 371).

The point I make is that the same scholarly attention is not given to the more mundane forms of political dissent. It is that absence which I attempt to address in this article.

In what follows I identify one kind of activism, namely, Distributed Denial of Service (DDoS) and the responses to it by governments to illustrate a broader anti-democratic trend on the part of liberal states in criminalizing new forms of political activity. Of interest is the discrepancy between the clear commitments expressed by those engaging in such political activity to democratic values, *and* the willingness of ostensibly liberal-democratic governments to represent this activism as criminal or terrorist and to use criminal law to repress dissent.

Scholars like Reyes who have addressed this process, argue that criminalizing political dissidence unfolds in stages. I use Reyes along with similar work by others (REYES, 2002; COHEN, 1972; MIRANEAU, 2014) to develop a heuristic frame to interpret and analyze the case study that follows.

Criminalization processes begins with state agents, spokes-people for the legal communities and media representatives characterizing political dissent as 'criminal' and 'terrorism' (REYES, 2002). Miraneu *eg* documented how environmental activists were described as terrorist and criminalized:

'in this process the 'terrorist' label functions as the important alarm that justifies a range of heavy repressive measures against environmental activists' (2014 p.88). The same processes are evident in the demonization and criminalization of prodemocracy and free-speech advocates.

A second step in criminalization processes is to ignore the important role of dissent in

democratic culture. Thirdly, certain official representatives attempt to de-politicize the activities of dissident groups by negating the importance of the issues in question. It can include ignoring the immediate and long term benefits of the action to the community (eg, whistle-blowing can reveal wrong-doing and harm caused by the state or others about which the citizenry would otherwise be ignorant). This 'stage' can also involve criticizing the political motivations or goals of the critics.

The fourth stage involves invoking fear to justify legal interventions. This can involve highlighting the dangers said to threaten the public interest if mechanisms of repression are not used, or if criminal sanctions are not enacted. Finally, we see the implementation of legal sanctions.

I use this 'heuristic' in the following case study to analyze processes of criminalization. I begin by outlining activities that fall under the rubric of the Distributed Denial of Service action.

10. Criminalizing New Politics: Applying The Heuristic

Criminalization processes begins with state agents, spokes-people for legal communities and media representing the activism as 'criminal' or 'terrorism'. Such characterizations have become prevalent since the 9/11 as many Western governments worked to manufacture a climate of fear and enhance popular anxiety by representing the world as a profoundly unsafe place. This has seen western governments introduce tranches of 'antiterror' legislation. National and cyber-security have become central to international defence strategies, while 'cyber-war' has come to characterize relations between countries like China, North Korea, Russia, the UK, Australia and the US.

Unprecedented numbers of new 'anti-terror' offences created in this context is telling. Steps taken in Britain under the Labor government (1997-2008) *eg* are illustrative of a general trend. According to Skrimshire, labor created over 3,000 new offences, an unprecedented number compared with earlier Conservative governments -1979-1997 (2009). In the UK the *Anti Terrorism Act* 2000 was used to detain legitimate protestors since the G8 Summit in Scotland. The *Anti Terrorism Act* 2000 was invoked against anti-war protestors at the Fairford RAF base. Protestors were repeatedly stopped and searched in police action later deemed

unlawful by the High Court (SKRIMSHIRE, 2009, p. 53). It was a practice repeated in the USA, Australia and many European countries.

We have a political environment that encourages rhetorical techniques designed to justify the abrogation of civil liberties and targeting of particular groups.

When citizens rely on DDoS for political reasons it is represented as criminal and-or terrorist activity that threatens social order. The seriousness with which DDoS action is regared by governments is evident in the US government's reaction to the Anonymous 'Operation payback' campaign involving DDoS attacks on Mastercard, Visa and Paypal after those companies blocked donations to Wikileaks. In response to the DDoS action the US government served 42 warrants and charged 14 protesters. As Leiderman observed:

While protest charges have typically been seen as tantamount to nuisance crimes, like trespassing or loitering, these were different. The fourteen PayPal defendants, some of whom were teenagers when the protest occurred, find themselves looking at 15 years in federal prison - for exercising their free speech rights; for redressing their grievances to PayPal, a major corporation; for standing up for what they believed was right (2013).

Those participating in DDoS were represented as criminals, 'enemies' or 'militant Islamic jihadist' (Coleman 2014). Conflating DDoS with war and 'cyber-terrorism' frames the problem as one of national security and a direct threat to national security. Conflating DDoS protests with hacking for the purpose of theft for personal gain similarly works to frighten people fearful of having their bank accounts raided.

'Confusing' or conflating DDoS with 'hacktivism' functions to obfuscate public discussion by representing the two activities as the same thing. They are quite different: hacking involves computer break-ins or 'trespassing', while DDoS slows down or blocks servers by sending too many requests. Conflating the two activities works to confuse and reinforce the message that DDoS is like hacking and analogous to a 'dangerous' 'weapon' that can wreak havoc and take-down domestic infrastructure like national power grids, water, banking systems, nuclear, chemical and security systems (Amoroso 2013).

Confusing DDoS with hacking also underscores the criminal label. As the FBI's Deputy Assistant Director, Chabinsky argued even if 'hackers can be believed to have social causes', their actions are unlawful and unacceptable (cited in Gjelten 2011). It is worth noting the reference to political motivation by the FBI which distinguishes DDoS users from criminals and terrorist, but nonetheless does not exempt them from prosecution. This is an important distinction because as criminals or enemies-terrorists the state is justified in prosecuting because they are said to have broken the law or breached the social contract.

Participants in DDoS however are exercising their citizen rights to protest for a cause (Coleman 2011). In spite of the distinction, those arrested were charged and punished.

The word 'chaos' is often used to characterize DDoS action thereby denoting the prospect of disorder and lawlessness. FBI's Deputy Assistant Director extended the disorder theme evoking images of outlaws and the wild west, metaphors that have powerful resonances in the USA:

The Internet has become so important to so many people that we have to ensure that the World Wide Web does not become the Wild Wild West." (cited in Gjelten 2011).

Similar characterizations can be found in official statements like those made by UK government's legal representative who argued for the prosecution of those who participated in the Anonymous 'Operation Payback' when Paypal refused to process payments to Wikileaks. According to the prosecution, those involved were cyber-criminals waging a sophisticated and orchestrated campaign 'attacks' on the computer systems of several major companies' (cited in Fortado, 2012).

In the same way the DDoS actions of 20 year old American Timothy French reportedly connected with a hackivist group 'NullCrew' was represented by US Attorney for the Northern District of Illinois as 'criminal activity': "Cyber crime sometimes involves newage technology but age-old criminal activity ..." (Fardon, cited US Attorney's Office 2014).

NullCrew is a hacktivist collective operating since 2012 that targets organisations they consider corrupt and engaged in harmful and anti-social activities. In 2012 they accessed the World health Organisation (WHO) in protest against poor health care systems releasing sensitive material. According to NullCrew, the reasons:

...for this hack are because of the pathetic health-care. It's been decades and our Heath Care system has never been what it should be. Thousands of people are dying just because of this. Either waiting in waiting rooms for too long, or not being able to pay the extreme amounts to be cared for. We deserve better. Now NullCrew has taken one step forward to fight for our proper rights (Bat-Blue Networks 2012).

Other organizations NullCrew have protested against include a South African ISP online directory. The reasons for this action was to protest against corruption, the molesting of children, use of their labour in the sweatshops and government corruption (Softpedia nd). NullCrew also protested against the Cambodian government after it arrested a founder of Pirate Bay. For similar reasons they targeted educational institutions like Yale and Cambridge Universities, Netcom, and Memotext electronics. They joined 'stop on line piracy' debates, and have demonstrated against the use of new technologies designed to detect copyright infringements as part of an 'anti-pirate crackdown' that involves corporations sending warnings to people downloading copyright material before prosecuting them (Fuchs 2013). As part of this campaign NullCrew accessed Time Warner Company that was using the 'alter system', they defaced its website for a few hours and added the image of a gorilla. According to NullCrew their action was in support of open and free access and in protest against the detection and punishment subscribers who use copyright content. NullCrew explained on twitter: "We hacked Time Warner Cable, due to them attempting to participate in the six strikes' (NullCrew 2013)".

In parallel with representating digital activists as 'criminals' or 'terrorists', governments routinely attempt to 'de-politicize' dissident activities by negating the importance of the issues in question or by criticizing their political motivations or by ignoring the ethical motivations that prompt DDoS action.

Governments de-politicise DDoS and similar actions by ignoring the value of dissent or the political the actual issue being objected to. Reliance on an overly Hobbesian conception of the state that insists it must do whatever is needed to secure social and political order means the values of dissent routinely ignored.

In the post 9/11 context conflating DDoS activism with the broader category of hacking and the 'enemy' and 'war' has been an effective tactic. In America, the FBI exemplified the way such language could be used to invoke fear and so justify legal action. The FBI invoked the falling dominoes metaphor arguing that DDoS can evolve into dangerous cyber activity if organized crime and terrorists were ever to emulate groups like Anonymous and Lulzec:

There has not been a large-scale trend toward using hacking to actually destroy websites, [but] that could be appealing to both criminals or terrorists ... That's where the 'hacktivism,' even if currently viewed by some as a nuisance, shows the potential to be destabilizing (Chabinsky cited in Gjelten 2011).

These discursive techniques are routinely used to 'reform' existing legislation or to introduce new legislation that criminalizes protests like DDoS.

A DDoS action is a criminal offence in most countries. However specifying how the criminalization process is used is not an easy task. While a jurisdiction may have list of laws that may be applied, determining what a person is to be charged with depends on the particular the case, the nature of the actions, whether intent can be demonstrated, the nature of the evidence, who is involved and to degree to which they participated. As Slobbe and

Verberkt explain:

As the digital world is much larger than country borders prescribe, it is difficult to cope with cases where the national legislation of two countries differ. At the same time, world wide legislation is not easily made not even to mention enforcement (2012 p.5)

The fact that DDoS are used for a variety political and non-political reasons adds to the complexity and to the ways different legal sanctions are applied. Having said that, the fact remains, DDos are regarded as 'high tech offences in most jurisdictions.

11. The Legislation

If a person is found guilty of DDoS action in the UK they can be charged in accordance with the Computer Misuse Act. In the USA a variety of 'cybercrimes' can be prosecuted under the Computer Fraud and Abuse Act 18 U.S.C. §1030 (Doyle 2014). The Act was passed in 1986 but substantially amended after passage of the USA Patriot Act 2002. 18 U.S.C. §1030 draws a long bow in defending 'protected computers' from 'attack'. Among the key provisions outlawing 'cyber crime' is action that damages a government or bank computer, or a computer used to affect interstate or foreign commerce (e.g., a worm, computer virus, Trojan horse, time bomb, a denial of service attack) 18 U.S.C. 1030(a)(5).

As Dittrich et.al (2005) argued, breaking into a computer or network to install DDoS handlers and agents may violate 18 U.S.C. §1030(a)(3). Penalties range from imprisonment for not more than a year for cyberspace trespassing, to a maximum of life imprisonment when death results from intentional computer damage. There can also be civil cause for action if it's demonstrated that the action caused financial loss of at least \$5,000 of impairment or injury.

The US has seen a number of high profile cases involving 18 U.S.C. §1030 and digital activists. One involved PayPal in 2011 when a group of young people staged DDoS action against PayPal as part of an Anonymous campaign, (Operation Payback) after PayPal blocked payments in the wake of Wikileak's released leaked information about US government's foreign activities.

My own review of developments reveals that many young people have been arrested, charged and imprisoned in a number of countries for their involvement in DDoS activities. As mentioned, Christopher Weatherhead was 20 years old when he participated in DDoS action. He was convicted of conspiracy to impair the operations of a computer, a charge with a maximum penalty of 10 years jail: he was sentenced to 18 months imprisonment. Ashley

Rhodes was 27 at the time of his DDoS 'offence' and was charged with conspiring to impair the operations of computers, and imprisoned for seven months. Peter Gibson was 22 at the time of the action was given a 6 month suspended sentence. Jake Birchall 16 at the time of the DDoS action was informed he would have been imprisoned had he not been so young at the time of the offence.

This is a context in which 'dissident' organisations themselves have all became the target of reprisal Distributed- Denial-of Service Attacks perpetrated by state security agencies. It is ironic that leading liberal intellectuals like Sunstein recommended that the US engage the services of undercover agents to infiltrate activist groups and selected online groups and websites in 2008 (SUNSTEIN and VERMEULE, 2008).

According to the National Broadcasting News (NBC), British secret intelligence service presented a conference paper in 2012 revealing how it engaged in DDoS action as part of its Rolling Thunder operation against Anonymous hacktivists.⁴ It was an initiative said to have been carried out in 'the guise of the Joint Threat Research Intelligence Group (JTRIG)', an intelligence unit unconstrained by domestic or international laws (NBC News nd).

According to the documents, a division of Government Communications Headquarters (GCHQ), the British counterpart of the NSA, shut down communications among Anonymous hacktivists by launching a "denial of service" (DDOS) attack - the same technique hackers use to take down bank, retail and government websites - making the British government the first Western government known to have conducted such an attack (Schone et.al nd).

'Distributed Denial of Service 'attacks' have also been used by governments against 'terrorist' or dissident websites (ARTHUR, 2011). Wikileaks has been subject to DDoS attacks, action sometimes attributed to extra-legal 'public-private partnerships' (BLENKER, 2010, p. 311-397).⁵ Presumably these reprisals are not subject to criminal sanction.

DDoS is but one example of political action that is being suppressed through the process of criminalization. It is a response on the part of the state that illustrates a broader anti-democratic trend, and one relevant to scholars interested in young peoples political participation and the state of liberal democratic societies.

12. Conclusion

⁴

⁵ Some hackers are said to be co-opted state security agencies to coordinate DDoS attacks against foreign governments (Fisher and Keller 2011). Many governments use DDoS as part of their 'front-line cyber weaponry'. They are also used by some corporations to gain advantage over competitors (ibid, Coleman 2014, pp.96-99).

This article addressed an issue central to contemporary political studies and youth studies, namely, how best to understand new on-line political activity like Distributed Denial of Service activism.

As political action, DDoS can disrupt websites and the operation of organization, and when targeted at state and corporate sites it creates a 'counter-artifact' that highlights and contests what is typically a one-way flow of communication. As Sauter argues:

Direct action is an ideological mode of activism that encourages activists to disrupt harmful processes and systems at the same time as they attempt to provoke a dramatic, illustrative reaction from their target (2014, p. 34).

The focus in this article was less on the political motivations of those engaged in this direct action and more on the ways states have criminalized Distributed Denial of Service activity and what this suggests about those states and the nature of 'the political'.

The article explored the significance of moves by ostensibly liberal states to use their legal and extra-legal powers to clamp-down on new forms of political dissent. What was questioned is how contemporary political communities understand the political. How have those working in the social sciences and youth studies conceptualize the political, the politics of young people and the reactions of political elites to their participation?

The reactions of liberal states to digital political action of the kind discussed above may be understood in a few ways. One is to recall how historically young people, as a political constituency, have largely been excluded and marginalized from the 'public sphere' and from electoral processes, yet now many have the capacity not only to enter the political domain, but also to be very effective as political agents courtesy new digital technologies. This clearly has the potential to be quite disruptive of the age-related status-quo of power relations. Another way of understanding the reactions of liberal states to digital political activism of the kind discussed here is to recognize how those states, whatever they may say publicly about their commitment to promoting debate or the value of dissent and free expression, frequently find reasons justified by appeals to the old Roman adage that 'the security and safety of the people is the first law'. Thus, when political action is described as 'threatening security', the 'obvious' response is to constrain politics in ways that entail suspending the officially declared regard for such political rights. Moreover, it's reasoning typically enacted by military and state security. Such recourse to the practices of sovereign exceptionality raises questions about the legitimacy of our claims to be democratic as well as the genuineness of recent political and policy claims to 'give voice' to young people

13. References

AMOROSO, Edward. Cyber Attacks: protecting National Infrastructure. Boston: Elsevier, 2013.

AOUDE, Ibrahim. Arab Americans and the Criminalization of Dissent. **Social Analysis: The International Journal of Social and Cultural Practice**, 46, (1), p. 125-128, 2002.

ARVANITAKIS, James; MARREN, Siobhan. Putting the Politics back into Politics: Young people and Democracy in Australia: Discussion paper. Sydney: University of Western Sydney, 2009.

AUSTRALIAN FEDERAL POLICE, ND. **High Tech Crime**. Available in http://www.afp.gov.au/en/policing/cybercrime/hightech-crime.aspx#distributed-denial-of-service-attacks.

BAT-BLUE NETWORKS. NullCrew Hacks World Health Organization and Leaks 568 User Credentials, 2012. Acessible in: https://www.facebook.com/BatBlueNetworks/posts/446104122090539.

BAUERLEIN, Mark. The Dumbest Generation: How the Digital Age Stupefies Young Americans and Jeopardizes Our Future. New York: Penguin: 2009.

BAUMAN, Zygmunt., Liquid Modernity. Cambridge: Polity Press, 2000.

BECK, Ulrich. Risk Society: Towards a New Modernity. London: Sage, 1992.

BENNETT, W. L., WELLS, Chris., and RANK, Allison. Young citizens and civic learning: two paradigms of citizenship in the digital age. **Citizenship Studies**, 13(2) p. 105-120, 2009.

BERRERDA, L., 2015 cited in 'The PP Criticized the Support of the Comedian Facu Pable Iglesiuas Diaz". Not anything goes, ABC. Available in:

https://translate.google.com.au/translate? hl=en&sl=es&u=http://www.abc.es/espana/20150110/abci-iglesias-facu-diaz-201501091656.html&prev=search-10-January>.

BESSANT, Judith. Democracy Bytes: New Media, New Politics and Generational Change. London: Palgrave-Macmillan, 2014.

. Mixed Messages: Youth Participation and Democratic Practice, Australian Journal of Political Science, 39 (2), p. 387-404, 2004.

BENKLER, Yochai. A Free Irresponsible Press: Wikileaks and the Battle Over the Soul of the Networked Fourth Estate. Harvard. C.R.-C.L. L. Rev. 46, p. 311-397, 2011.

BRABAZON, Honor. Protecting Whose Security? Anti-terrorism Legislation and the criminalization of Dissent, YCIS Working Paper 43, York University, Toronto, 2006.

COHEN, Cathy, and KAHNE, Joseph. Participatory Politics: New media and Youth political Action, 2012. Available in: http://ypp.dmlcentral.net/sites/all/files/publications/YPP Survey Report FULL.pdf>. Access in: 16 dez. 2013.

COHEN, Stanley. Folk Devils and Moral Panics. London: MacGibbon and Kee, 1972.

COLEMAN, Gabriella. The ethics of digital direct action Denial-of-service attacks and similar tactics are becoming more widely used as protest tools. Aljazeera, 2011. Available in: http://www.aljazeera.com/indepth/opinion/2011/08/20118308455825769.html.

COLEMAN, Gabriella. Hacker, Hoaxer, Whitstleblower, Spy: The many faces of **Anonymous.** London: Verson, 2014.

DITTRICH, D., MIRKOVIC, J., REICHER, S., et.al, Internet Denial of service attack and **Defense Mechanism.** Pearson, 2005.

DOYLE, Charles. 'Cybercrime: A Sketch of 18 U.S.C. 1030 and Related Federal Criminal Laws, Congressional Research Service, Washington, 7-5700, 2014, www.crs.gov RS 20830.

FARDON, Zachary, 2014 cited in US Attorney's Office, 16 June 2014. Available in: .

FARTHING, Rys. The politics of youthful anti-politics: Representing the 'issue' of youth participation in politics, **Journal of Youth Studies**, 13 (2) p. 181-195, 2010.

FORTADO, L. Anonymous' Hackers Convicted of Targeting PayPal, MasterCard, 2012, Bloomberg Business. Available in: http://www.bloomberg.com/news/articles/2012-12-06/- anonymous-hackers-convicted-of-targeting-paypal-mastercard>.

FUCHS, E. Time Warner Cable Site Defaced with Gorilla Over its New Anti-Piracy Policy, Business Insider, 2013, Available in: http://www.businessinsider.com.au/time-warner- hacked-by-nullcrew-2013-3>.

FUREDI, Frank. The Politics of Fear. Beyond Left and Right. London: Continuum, 2005.

GARLAND, David. Culture of Control: Crime and Social Order in Contemporary **Society.** Chicago: The Chicago University Press, 2001.

GIDDENS, Anthony. Modernity and Self Identity: Self and Society in the late modern Age. Stanford: Stanford University Press, 1991.

GJELTEN, T. FBI Tries To Send Message With Hacker Arrests, National Public Radio, 2011. Acessible http://www.npr.org/2011/07/20/138555799/fbi-arrests-alleged- in: anonymous-hackers>.

GLEICK, James. Today's Dead End Kids. The New York Review of Books, 2014, december 18: p. 36-38.

HENN, Matt; WEINSTEIN, Mark. Young people and political (in)activism: why don't young people vote? 2006, **Policy & politics**, 34 (3): 517-534.

HENN, Matt; WEINSTEIN, Mark; WRING, Dominic. A generation apart? Youth and political Participation in Britain. 2002, **British Journal of Politics and International Relations**, 4 (2), p.167-192.

HOCKING, Jenny. **Terror laws: ASIO, counter-terrorism and the threat to democracy**. Sydney: UNSW Press, 2004.

HOGG, Russel. Criminology, Crime and Politics Before and After 9/11. 2007, **The Australian and New Zealand Journal of Criminology**, 40 (1), p.83–105.

JENNESS, Valerie. Explaining Criminalization: From Demography and Status Politics to Globalization and Modernization. **Annual Review of Sociology**, 2004, 30, p. 147-171.

KAHNE, Joseph; MIDDAUGH, Ellen; ALLEN, Danielle. Youth, New Media and the Rise of Participatory Politics, **YPP Research Network Working Paper Series**, n. 1, 2014, Civic Engagement Group.

KAPLAN, D. WikiLeaks undergoing massive denial-of-service attack, Secure Computing monthly magazine, 2012. Available in: http://www.scmagazine.com/wikileaks-undergoing-massive-denial-of-service-attack/article/254267.

LEIDERMAN, J. Justice for the PayPal WikiLeaks protesters: why DDoS is free speech. **The Guardian**, 23, jan. 2013. Available in: http://www.theguardian.com/commentisfree/2013/jan/22/paypal-wikileaks-protesters-ddosfree-speech.

MANNING, Nathan. Young people and politics: apathetic and disengaged? A qualitative inquiry. Koln: Lambert Academic Publishing, 2009.

23

MARTIN, Aaron. Political Participation among the Young in Australia: Testing Dalton's Good Citizen Thesis. **Australian Journal of Political Science**, 42, p. 211-26, 2012.

MATZA, David. **Becoming Deviant**, Prentice Hall, Edgewood Cliff, 1969.

MAYER, Karl Ulrich. The sociology of the life course and life span psychology: Diverging or converging pathways? In U. Staudinger, M. and U. Lindenberger (Eds.). **Understanding human development: Dialogues with lifespan psychology**, p. 463-481. London: Kluwer Academic Publishers, 2003.

MCCAFFRIE, Brendan; MARSH, David. 'Beyond mainstream approaches to political participation: A response to Aaron Martin. **Australian Journal of Political Science**, v. 48, n.1, p. 112–117, 2013.

MIRANEAU, Manuel. The Criminalization of Environmental Activism', **Studia Universitatis Babes-Bolyai**, 2, p. 87-103, 2014.

MOSES, A., and GARDINER, S. LulzSec hack into Murdoch's British websites. **Sydney Morning Herald**, 19 jul. 2011. Available in: https://www.smh.com.au/technology/technology-news/lulzsec-hack-into-murdochs-british-websites-20110719-1hm6r.html.

MOUFFE, Chantal. **On the Political**. London: Routledge, 2005.

MUNCIE, John. Decriminalising Criminology, Proceedings. Volume 3. **Papers from the British Society of Criminology Conference**, Liverpool, 1999. Editors: George Mair and Roger Tarling. Acessible in: http://britsoccrim.org/volume3/010.pdf>.

NBC NEWS. The Snowden Files: British Intelligence Agency describes attack on Anonymous.

Available in:

http://msnbcmedia.msn.com/i/msnbc/sections/news/snowden_anonymous_nbc_document.pd

*NullCrew. 2013, @NullCrew_FTS twitter. Available in:

https://twitter.com/NullCrew_FTS/status/309172610204315648>.

O'TOOLE, Therese. Engaging Young Peoples Conceptions of the Political. **Children's Geographies**, v. 1, 1, p. 71-90, 2003.

POYNTING, Scott; WHITE, Robert. Youth Work: Challenging the Soft Cop syndrome. **Youth Studies Australia**, 2004, 23 (4): 39-46.

RANCIÈRE, Jacques. Dissensus: On Politics and Aesthetics. New York: Continuum, 2010.

REYES, Yanira. Law, media and political dissent: The case of the FALN, **E-Ph.D**, Purdue University, 2002. Available in: http://docs.lib.purdue.edu/dissertations/AAI3105012/.

SACHS, Joe. Plato: Republic. Newburyport: Focus Publishing, 2007.

SALTER, Colin. Activism as Terrorism: The Green Scare, Radical Environmentalism and Governmentality. **Anarchist Developments in Cultural Studies**, Ten Years After 9/11. An Anarchist Evaluation, p. 211-238, 2011.

SAUTER, Molly. **The Coming Swarm:** DDOS Actions, Hacktivism, and Civil Disobedience on the Internet. London: Bloomsbury, 2014.

SCHMITT, Carl. **The Crisis of Parliamentary Democracy**. Cambridge: MIT Press, 1988. Tradução: Kennedy, E.

SCHONE, M.; ESPOSITO, R.; COLE, M.; GREENWALD, G., nd.. Exclusive: Snowden Docs Show UK Spies Attacked Anonymous, Hackers. Available in: http://www.nbcnews.com/feature/edward-snowden-interview/exclusive-snowden-docs-show-uk-spies-attacked-anonymous-hackers-n21361.

SKRIMSHIRE, S. Demoralising Britain: ten years of Depoliticisation, in Scott, D., Graham, J., and Baker, S., (eds), Remoralising Britain? **Social ethical and Theological perspectives on New Labour**. Continuum, London. p. 38-57, 2009.

25

SLOBBE, J., and VERBERKT, S. Hacktivists: Cyberterrorists or Online Activists? An Exploration of the Digital Right to Assembly, 2012, v.org/pdf/1208.4568.pdf

Softpedia. 'Nullcrew Hacks South African ISP Directory, 450 Accounts Leaked'. Acessible in: http://news.softpedia.com/news/NullCrew-Hacks-South-African-ISP-Directory-450-Account-Details-Leaked-281630.shtml>.

SUNSTEIN, Cass; and VERMEULE, Adrian. Conspiracy Theories. Harvard University Law School, **Public Law & Legal Theory Research Paper Series**, 2008. Acessible in: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1084585.

TWENGE, Jean. The Narcissism Epidemic. Free Press: 2009.

VROMEN, Ariadne; COLLIN, Phillipa. Everyday youth participation? Contrasting views from Australian policymakers and young people. **Young**, 18 (1): p. 97-112, 2010.

WEINSTEIN, Emily. The Personal Is Political on Social Media: Online Civic Expression Patterns and Pathways Among Civically Engaged Youth. **International Journal of Communication**, p. 210–233, 2014.

XENOS, Michael; VROMEN, Ariadne; & LOADER Brian. The great equalizer? Patterns of social media use and youth political engagement in three advanced democracies. **Information, Communication & Society**, 17 (2) p. 151-67, 2014.