An Ethical Framework for Hacking Operations

Ross W. Bellaby [1]

Abstract

In recent years the power and reach of prominent hacker groups such as Anonymous and LulzSec has been clearly demonstrated. However, in a world where hackers are able to wield significant online power, can they do so ethically as legitimate agents? To answer this question this paper will develop an ethical framework based on the premise that hackers have exhibited instances where they have acted to protect people from harm at a time when there was no one else to do so. At its core this paper will argue that political hacking can be justified when it is done to protect the vital interests of oneself or others. Moreover, it will also argue that just because hackers are outside the state does not automatically discount them as ethical actors and that when the state fails to protect people – whether it is due to a lack of ability, political will or because the state is the source of the threat – hackers can fill the void. In order to achieve this, first it is necessary to highlight the space for hackers to operate; second, guide hacker activity by creating an ethical framework detailing what actions are justified towards what end; third, to offer mechanisms that can aid in reaching these ethically justified decisions; and as a result, inform further ethical debates on how to react to these political hackers. This means that the framework can be used to both justify and condemn hacking depending on the circumstances, allowing those on the outside to distil and evaluate a political hack, both past and present, while guiding hacker collectives by providing clearer ethical tools for determining the appropriate agendas and methods.

Keywords Hackers · Ethics · Anonymous · Self-defence

1 Introduction

In recent years the power and reach of prominent hacker collectives such as Anonymous has been clearly demonstrated. These large, politically orientated hacker

---

✉ Ross W. Bellaby
   r.bellaby@sheffield.ac.uk

[1] Department of Politics, University of Sheffield, Elmfield Building, Northumberland Road, Sheffield S10 2TU, UK

collectives have targeted a range of actors over a number of issues, all without a consistent set of ethical statements to guide or evaluate their activity. On the one hand, these hacks necessarily use political violence outside the usual state-sanctioned systems without any clear moral authority and often for their own political goals. While on the other hand, many of their causes – targeting terrorist groups, fighting for LGBTQ+ rights, and protecting people's freedom of expression, autonomy and privacy – are intuitively good things to fight to protect. As a result, it can be incredibly difficult to apply clear-cut statements of praise or criticism. In a world increasingly obsessed with superheroes and villains, what do hackers represent? Are they a new force for good fighting against terrorists and hate groups, work the state is either unable or unwilling to do? Or do they hide in cyberspace carrying out their private wars fuelled by personal beliefs and vendettas with no oversight or control? Or both?

To navigate this tension this paper will develop an ethical framework based on the premise that hackers have exhibited instances where they have acted to protect people from harm at a time when there was no one else to do so. At its core this paper will argue that political hacking can be justified when it is done to protect the vital interests of oneself or others. Moreover, it will also argue that just because hackers are outside the state does not automatically discount them as ethical actors and that when the state fails to protect people – whether it is due to a lack of ability, political will or because the state is the source of the threat – hackers can fill the void. The aim is not to open the door to all private forms of political violence, nor is it to justify the abstract act of hacking. Rather, the purpose of the framework is to understand the ethical role a hacking operation can play in relation to the circumstances. In order to achieve this, first it is necessary to highlight the space for hackers to operate; second, guide hacker activity by creating an ethical framework detailing what actions are justified towards what end; third, to offer mechanisms that can aid in reaching these ethically justified decisions; and as a result, inform further ethical debates on how to react to these political hackers. This means that the framework can be used to both justify and condemn hacking depending on the circumstances, allowing those on the outside to distil and evaluate a political hack, both past and present, while guiding hacker collectives by providing clearer ethical tools for determining the appropriate agendas and methods.

2 Hacks, Hackers, Hacking and the Operation

Hacking is often used as a catchall to cover all forms of 'unauthorised access to or use of a computer system', but can encompass a very large range of different actors, intensions and activities (Conway 2003: 10; Barber 2001). From criminal hackers, or 'crackers', who maliciously attack or defraud systems for personal gain (Sheoran and Singh 2014: 112); to 'Skript Kiddies', often young males who use hacking tools created by others to vandalise or disrupt the Internet (Farsole et al. 2010: 15); to hacktivists, a portmanteau of 'hacker' and 'activist' who use 'acts of civil disobedience … carried out in the virtual realm of the Internet' (Lowes 2006: 115), to 'highlight political or social causes' (Jordon and Taylor 2004: 2; O'Malley 2013).

While the popularist terms oscillate between 'Heroes and hustlers, freedom fighters and cyber lynch mobs, political activists and anarchists' (Klein 2015: 379), and are often portrayed in media as 'lonely malicious criminals' (Thomas 2002: 6).

Of these various sub-classifications of hacking, this paper is focusing on what will be referred to as 'political hacking', where the hack is used in relation to some political or social agenda carried out by private individuals for their own political ends, often with this political element acting as a central justification for the hack. This marks political hacking as distinguishable from hacks for personal profit[1] (through theft, fraud or blackmail); hacks to test systems (white and grey hats for example)[2]; hacks to expand or demonstrate one's ability; attacks to create chaos for its own sake; and that these are different to those hacks carried out by the state or are state-sponsored.[3] This political element is widely conceived, and over their relatively short history the political agendas of hackers – whether individuals, groups with fixed-definable-members, or collectives with open and fluid membership – have varied from nuclear disarmament,[4] government

---

[1] The Sony PlayStation hack in 2011, stole customer personal details and credit card information for the purpose of fraud. See Quinn 2011. In 2016 Indian Banks – including SBI, HDFC Bank, ICICI, YES Bank and Axis had 3.2 millions debit cards compromised in a hack. See Shukla et al. 2016. This is similar to the 2014 JPMorgan Chase data breach which was believed to have compromised data associated with 83 million accounts. See Reuters 2014. While the WannaCry ransomware targeted computers running the Microsoft operation system and infected more then 230,000 computers over 150 countries, locking people out of access to their computer until they paid the ransom. See McGoogan 2017.

[2] Indeed, a key portion of work on hacker ethics examines the role that testing systems from the perspective of a hacker – sometimes invited and other times not. This includes 'white' or 'grey hat' hackers: people who test computer networks for weaknesses, the former with the owner's permission while the latter informs the owner after the weakness has been found. For example, using hackers to test computer networks for weaknesses, often concerned with determining what system an intruder could access and what information they could collect, what can be done with that information, and if anyone at the target system has noticed. 'World of Hell' was a grey hat computer hacker attack, specialised in targeting in websites with poor security and defacing them with an advice message (Sheoran and Singh 2014, 113; Ajinkya 2010; Bansal and Arora 2012; Cardwell 2011; Lu 2015).

[3] For (alleged) state or state-sponsored hacks include the Stuxnet computer worm found in computers at Iran's Natanz nuclear site, designed to control the centrifuges used to concentrate and refine Uranium, landed a significant blow on any Iranian nuclear ambitions without anyone lifting a sword. Sanger 2012; Farwell and Rohozinski 2011. Estonia in 2007, which brought down the websites of its banks, governmental agencies and media outlets, demonstrated the vulnerability of such structures as well as their increased importance in the modern world (BBC 2007; Traynor 2007; Landler and Markoff 2007; Blomfield 2007). Equally important is the threat of cyber-espionage. 'Titan Rain', for example, stole data from NASA's Mars Reconnaissance Orbiter and Air Force flight planning software as well as data from US government systems and defence contractors (Posner 2010); 'Operation Aurora' consisted of numerous attacks on high-tech, security and defence contractor companies (Cha and Nakashima 2010); and Operation 'Ghostnet' accessed the foreign affairs ministries of Iran, Indonesia, Philippines and the embassies of India, South Korea, Indonesia, Thailand, Taiwan as well as computers at NATO headquarters (Information Warfare Monitor 2009).

[4] In 1989 computers at NASA and the US Energy Department were hacked with the anti-nuclear 'WANK' worm, which altered login screens with the 'Worms Against Nuclear Killers' message, the second worm of its type used but the first with a distinctly political message. (McCormick 2000: 24).

responses to local public disorders and protests,[5] government restrictions to online freedoms,[6] court decisions,[7] corruption, private actors restricting the sharing of information online,[8] organising and facilitating public protests,[9] locating and revealing the identities of online-paedophiles and hate groups,[10] demonstrating the weakness and subsequent dangers of inadequate network security, and directly protesting and disrupting the growing power and prevalence of the security powers of the state. Indeed, as Gabriella Coleman states, 'Beyond a foundational commitment to the maintenance of anonymity and a broad dedication to the free flow of information, Anonymous has no consistent philosophy or political program' (Coleman 2014:3). This does, on the one hand, make it difficult to pin the political hacking phenomenon to a particular ideology or ethical objective, especially given Anonymous' 'rhizomatic' nature, where their self-defined 'antileader, anticelebrity ethic', with a membership that is open 'to all who care to contribute' and where the cause is king (Coleman 2011: 511; Liu 2004), prompts them to move from issue to issue without a seemingly clear set of long-term plans or underlying political objectives.

The challenge, therefore, is how to create an ethical framework that can evaluate a highly varied set of political agendas, especially when it is difficult to both access and categorise the phenomenological experiences and justifications of such a diverse set of agents. To overcome this, the ethical framework focuses on the hacking activity as part of a wider (political) situation, often best evaluated through the hacking 'operation' as the manifestation and articulation of the hacker's political role. That is, the ethical framework will enable the evaluation of the hacking operation through both its separate parts as well as the culmination of the hacking agent and their political role at that point in time. What an operation can look like can vary, from the very specific efforts of an individual such as Aaron Swartz who accessed and released academic papers from the JSTOR archives (Utterback 2013; Ludlow 2013), right through to large, open ended and inclusive movements that span a longer timeframe with multiple strands, methods and targets involved and can evolve and change over time – for example Anonymous' attacks on ISIS, which include Operation: Troll ISIS, Operation Paris and Operation CharlieHebdo (Anonymous France

---

[5] Both Operation BART and Operation by Ferguson were Anonymous responding to the US officials restricting protests and review of police activity after the shooting of Charles Hill by the police in July 2011 and when police shot teenager Michael Brown. (Stone 2011; Rogers 2014)

[6] In 1990 the 'Cult of the Dead Cow' (cDc) worked (with the help of the Hong Kong Blondes, a groups cDc later stated they fabricated) to help Chinese citizens gain access to blocked websites. (Menn 2019; McCormick 2000).

[7] In April 2013, the suicide of Rehtaeh Parsons prompted Anonymous to action after they became aware of the failure of the Royal Canadian Mounted Police and Canadian officials to investigate a sexual assault. (Coleman 2014:370).

[8] Anonymous targeted the Church of Scientology in one of its earliest political hacks, Operation Chanology, in response to the Church's secretive and controlling nature and their insistence over the removal of a video that was released online (Coleman 2014:58). Also, the support Anonymous gave to Wikileaks after the organisation's money flow was halted in Operation Avenge Assange was premised on the role of Wikileaks sharing information that people had a right to as well as that by cutting off funding to Wikileaks the government and corporations were acting as a censoring force (Coleman 2014:2, 121).

[9] For example, during the Arab Spring Operation Tunisia and Operation Egypt played an important role in the emerging protest movements by DDoS-ing government websites and helping dissidents circumvent online censorship. (Wagenseil 2011; mmxanonymous 2011; Emspak 2011).

[10] Through Operation Death Eaters and Operation Dark Net sought to collect evidence against international pedophile rings (Eleftheriou-Smith 2015). Also from 2014 onwards Anonymous targeted the US hate group Klu Klux Klan threatening to reveal the names of its members (O'Neil 2015).

2015), or Operation Payback which involved targeting a range of anti-piracy organisations but changed in terms of emphasis and tactics over its time (Coleman 2014:96–105). Despite this variance, however, the hacker activity or operation can be coherently discussed and examined. It is possible to talk about who is being targeted and impacted, to detail the type of methods are used and what harm is caused, the different roles those involved are playing, and the political agenda sought. Similar to other ethical discussions of agents who are made up of fluid collectives pursuing long term political agendas through multi-streamed approaches, it is even possible to make distinctions within an operation, ethically condoning or condemning specific parts over others. Once the ethical evaluation of the hacker's activity has been made we can then use this as the foundation for further ethical discussions, such as who is responsible and to what degree, what type of praise or punishment is therefore required, and how the political community should respond to or conceptualise the hackers.[11]

To achieve this mapping across a variety of political agendas the methods, targets, narratives, and ends of the operation are examined, both as individual parts as well as how they (in)congruently map to each other to create the operation as a whole. That is, in common moral discourse it is argued that the central intention or justification of an action should be reflected in the means used, targets chosen, and outcomes pursued (Thomson 1986:101–102; Scanlon and Daney 2000; Lackey 1989:32). All have a part to play in how we judge an action, and all are interrelated to each other. For example, if the justification is one of self-defence then the actions must flow directly from this and not involve tactics of domination or subjugation of the aggressor; and that we can tack back from the methods and circumstances of a situation to understand the intention. This means that by examining the key features of a hack – the techniques used, the position/role/function of those targeted, the normative narrative delivered, and what types of harms are allowed – it is possible to map out and evaluate the operation. This approach allows for an evaluation of the hack as the outward expression and actions of the collective whole, rather than necessarily having to examine the singular, and potentially highly varied, motivations of all those individuals involved. This is particularly important and helpful in evaluating the actions of those operations that necessarily rely on wide and open involvement from the hacker community. For example, *en masse* methods such as Denial of Service attacks, virtual sit-ins, and email bombs, can utilise thousands of individuals contributing to the effort. In this instance the political agenda and actions of the collective are examined through the operation rather than any given individual. It could be that some members are involved because of their genuine belief in the stated political agenda of the collective, while others might contribute because of some other general belief (anti-establishmentism for example), whereas some might wish to feel a sense of inclusion and camaraderie and so contribute, and some might act to demonstrate their own power and

---

[11] Indeed, this does not preclude punishing particular individuals in a collective in regard to an unjustified hack. Like many other collectives where individuals might work towards a common goal while following the same methods yet for very different personal reasons (most notably evaluating a state's decision to go to and subsequent performance in a war, the intentions of rule abiding soldiers are not necessarily included in evaluating the ethical performance of the state) it is still possible to isolate ring-leaders (politicians and commanders in the war-time example) who must represent and take responsibility of the super-organisms operational behaviour. How blame is proportionally distributed in a collective or multiple-agent operation is in turn a separate question. For useful conversations on this see Lepora and Goodin 2013, Bellaby 2018, Braham and van Hees 2012; Sankowski 1992; Williams 2003; Squires 1968.

influence. However, in such an open situation it is both unhelpful and unnecessary to examine the intentions and motivations of all those involved if they all contribute towards the same ends, through the same means, with the same limitations. This allows for the hack to be evaluated as the manifestation of the collective effort, and then if needed track any necessary praise or condemnation onto those most responsible for the operation.[12] As a process, this type of ethical evaluation is particularly common in international ethics when evaluating the actions of collectives where a varied membership contributes through similar actions towards a common goal but for indistinguishable and potentially highly varied individual reasons. Evaluating collectives in this way has thus become an important part of our common moral discourse, altering how we talk about, speculate on, and judge the actions of states, political collectives and their representatives (Lackey 1989:32).

By focusing on the operations in this way it is possible to distil and map the political nature of a large range of activities by relating them to our core human rights, focusing on the relationship to our fundamental interest in maintaining our physical and mental integrity, autonomy, liberty and privacy. Indeed, political hacking has gravitated towards our key human rights, predominantly those ideals found within Steven Levy's early 'hacker ethic' work on the freedom of information and a mistrust in authority, reflecting the importance of autonomy and privacy in people's lives (metac0m 2003). For Christian Greenberg this has manifested as Anonymous having some overarching political orientation where it 'attacks whatever target offended its values, like freedom of speech and anti-corporatism' (2012a: 183). While Andy Fuchs, David Golumbia and Steven Levy see Anonymous as reflecting a socialist worldview, or cyber-libertarianism with a primary focus on free-speech and deregulation (Fuchs 2013: 7, 15; Borsook 2000; Levy 2000; Krauth 2012). In practice therefore, even within the most fluid of collectives where there are multiple voices calling for a variety of different political agendas it is still possible to see a 'shared awareness', where 'otherwise uncoordinated groups begin to work together' and to act towards a common goal (Shirky 2008: 163). The so-called 'hive-mind' of Anonymous, for example, operates as a super-organism, with many individuals working individually but possessing the nature of a single entity, and outwardly expressing a significantly coherent political rationale and narrative as a result. As Anonymous stated in an early video, 'Hello Internet. I am one Anonymous. Anonymous is a collective of individuals united by an awareness. We promote the truth, promote free speech, stand up against human injustice, we fight corrupt corporations and protest governments who bastardise freedom' (FLSnag 2011). Such ideals were then further detailed in their 2011 Anonymous manifesto which argued for the upholding of the rights and liberties of its citizens, free from undue influence from those privileged by greater resources, influence and power; to circulate uncensored information in order to guarantee these rights; that citizens should not be the target of any undue surveillance; that privacy is a common interests of humanity; and that it is the responsibility of all citizens to take actions and maintain an open and transparent society (Anonymous,

---

[12] For a flexible methodology on tracking and distributing responsibility across complex relationships and within fluid collectives see Bellaby 2018 who argues for a fluid and flexible understanding on the different normative roles various actors play which in turn can shape the type and level of responsibility allocated, and subsequently the specific type of punishment required.

2011). Other self-theorising communicated often makes reference to fighting 'the loss of more liberties such as censorship, phone and Internet surveillance and eminent domain laws' (Kumar 2011), stopping 'campaigns of misinformation' and the 'suppression of dissent' (Vamosi 2008), while Anonymous' 'anti-hate' stance has resulted in them targeting governments for passing homophobic legislation (Boone 2013; Littauer 2013). It can be argued, therefore, that many of the political operations can be mapped onto our core rights, with a significant proportion relating to our autonomy, including the right to protest, to be an informed, fair and equal political agency, and to carry out one's political will. Or the right to privacy and the subsequent restrictions on surveillance this creates (both government and corporate). Or targeting hate groups and paedophiles as a way of preventing physical and mental harm that such groups are causing or fostering.

As will be shown, sometimes the hacker's actions are justified given the core right being threatened, but at other times they are unjustified when those methods do not match the threat or where the hack causes a greater harm to our core rights. What is important, is that it is only by distilling the different political agendas and hacker activities it in this way that we can make such comparisons across a diverse phenomenon.

3 Filling the Void: Hackers Using Political Violence

One of the key criticisms levied at hacker activity is that they are private actors carrying out their own political ends through the use of political violence. So, while collectives such as Anonymous have engaged in what can broadly be referred to as digital resistance (Delmas 2018), digital disobedience (Scheuerman 2016) or digital activism (Sauter 2014) and use methods which range across the activist spectrum, a distinguishing feature of the type of political hacking examined here is the use of political violence, which arguably distinguishes it from some of the conceptualisations and discussions on 'hacktivism' and those related justifications based on non-violence and often through a civil disobedience framework. For example, Kenneth Himma argues hacktivism is 'the commission of an unauthorized digital intrusion for the purpose of expressing a political or moral position' and is 'nonviolent in nature' (2008: 200). Indeed, Candice Delmas describes the standard approach to the definition and justification of hacktivism as involving acts that are a 'public, non-violent, politically motivated, and conscientious breach of law undertaken with the aim of bringing about a change in laws or government policies' (2018: 65), while other emphasise the 'peaceful breaking of unjust laws' with 'non-violent means to expose wrongs, raise awareness, and prohibit the information on perceived unethical laws by individual, organisations, companies or governments' (Manion and Goodrum 2000: 14. Also see Hampson 2012a, b, c; Dittrich and Himma 2006; Crosston 2017; Goode 2015; Pavli 2019; Taylor and Harris 2006). Indeed, Cult of the Dead Cow, Oxblood Ruffin, defined hacktivism as something that uses 'technology to improve human rights. It also employs non-violent tactics and is aligned with the original intent of the Internet, which is to keep things up and running' (Smallridge et al. 2016: 61). Furthermore, Delmas notes that 'painting hacktivism as civil disobedience highlights their principles and communicative intentions' where their actions are 'speech acts, grounded in sincere political commitments', situating it to the 'broader public as a protest' and therefore well within the 'respectable tradition of civil disobedience' (2018: 64. Also see Auty 2004; Hampson 2012a, b, c; Jordan 2014).

In comparison, the type of political hacking discussed here often relies on methods that use some level of destruction, harm or damage and are powerful because of the (threat of) coercive power or damage they cause.[13] This can include: Distributed Denial of Service (DDoS) attacks where the normal traffic of a targeted server, service or network is disrupted by overwhelming it or the surrounding infrastructure with a flood of Internet traffic with the aim of either temporarily or permanently shutting it down, causing damage to both the target's infrastructure as well as their ability to interact with their client and those client's ability to pursue their own ends; doxxing, whereby private information about an individual or organisation is collected and widely released online, causing harm through the violation of people's privacy, and potential loss of reputation and income; leaks and the unsanctioned release of confidential information (whether state or corporate) to news media outlets, which can cause both direct damage through the leak, or subsequent harm through how others use the information; and viruses and malware with the aim of causing damage to a network system.[14]

The question, therefore, is what moral authority hackers have to use violence for a political objective when they act outside of the system. This is often contrasted against the normative authority states claim – a claim often made through its representation of the political body or protector of the polis. Indeed, there are strong arguments that the state is the only actor who can legitimately use political violence (Duff 2011: 6). This includes the argument that, firstly, there is a broad social contract where individuals give up their absolute rights to carry out their own private wars or pursuit of personal justice in return for the comfort and protection provided by the state.[15] The state therefore has the duty to ensure that individuals are protected, that rules are maintained, and differences are arbitrated. In return there is a prima facie obligation to obey the rules and mechanisms established (Markel 2011: 54). Hackers do not have any of this and, moreover, when they carry out harmful activities, they in turn break the agreement to not carry out private acts of violence, marking themselves as the threat to the social whole and the good found in the stability of the rule of law.

---

[13] This is a distinction drawn in this paper and is not one necessarily maintained across the literature, especially as terms like hacktivism, hacking, and digital disobedience are used interchangeably. For example, Sauter (2015) and Deseriis (2016) include DDoS in hacktivism (2016). The point here is more to draw the distinction between non-violent and violent forms of hacking and to focus on the latter. In addition, there is some excellent work that seeks to expand the definition of civil disobedience in order to include different forms of hacking and explore whether the justifications of civil disobedience can be applied to them. See Scheuerman (2016), Brownlee (2016) Celikates (2016) (Sauter 2015) Ludlow (2013). Candice Delmas (2018) is at the forefront of this debate, giving a detailed view of the different avenues taken and puts develops their own framework for hacking and civil disobedience. However, this is a separate debate to the one being had here. This paper does not discount these other debates. But they are different conversation to be had. Their main effort is to locate (or not) different forms of hacking within civil disobedience – and so focus on civil disobedience, its (over)stretching and usefulness. While the focus here is on examining the ability to use political violence and the more destructive forms of hacking more through developing a fundamental set of ethical questions for hacking activity. Indeed, some authors focus on the (il)legality of hacking, which is a separate discussion to the ethical debates being had here.
[14] This is also distinct from cyber-terrorism which relies on 'the hack to cause grave harm... such as loss of life, or severe economic damage', where the intent is cause fear to send a message to a third-party audience. Whereas the political violence used in the hacks discussed here does not only utilises a much lower level of harm or destruction – being without the intent to cause loss of life and the direct aim of causing fear – but also the hack itself is used a form of direct action, to directly achieve the end the hacker is aiming for. (Denning 2000. Also see Holt et al. 2017; Jordan and Taylor 2004; Karagiannopoulos 2018; Tanczer 2017; Jackson and Pisoiu 2018)
[15] For classical social contract theory, including Hobbes (1985) and Locke (1988) and modern political theories of the evolution of governance like that of Robert Nozick (1974), civil government springs forth from the *state of nature*, a pre-social anarchic state in which individual action is at its peak.

However, this does not necessarily reject hacking completely. The state's legitimate authority is not derived from its de facto position or its coercive sovereignty, but from its role as representative and protector of the political community (Norman 1995: 118). States have value because of the role they play in an individual's life as the moral unit of concern: their moral authority or legitimacy of the state is based on its role in protecting vital interests and fundamental human rights (Fabre 2008: 964). So, while there can be arguments in favour of the general obligation to obey authority when the state is furthering the protection of this moral unit, if the state is absent in its application of this role then others can, and should, act. If the state fails to uphold its end of the bargain, due to lack of will, capability, negligence, or because itself represents an unjustified source of harm, then it loses its legitimate authority in this specific instance.

Indeed, arguments can be made that rather than fighting against the political community and even the state, private actions such as those carried out by political hackers can reinforce the importance of social norms and are replicating the important protective role the state should play: that they can 'claim to respect the law even more than the sitting government officials, since he takes it seriously enough to want to see it enforced' (Dumsday 2009: 59). Johnson argues that through organised and coordinated forms of political violence, non-state actors can be justified when they act as the state should be acting. For example, when the state has good laws that are misapplied or not being enforced; when the state has failed to enact good laws; or where unjust laws are being enforced (Johnston 1996, 220; Dumsday 2009; Reynolds 2015). Such activities, while outside the normal state-sanctioned infrastructure, are instances where private actors represent what the state should be doing or where they seek to circumvent the harm the state is causing. When the hacker, for example, provides people with technology that allows access to the Internet when it is blocked by their government, or raises awareness about or seeks to directly stop a particular political agenda that actively harms or discriminates part of society, they are not denouncing key ethical and social norms but are emphasising them, while highlighting the failure of the state or marking it as the source of the wrong. These hackers are seeking to maintain those ethical and social norms that are already in existence, that are widely already agreed upon and have already moral authority. Developing an ethical framework for hacking therefore rests on the core argument that this activity is about replicating that good the state represents in people's lives by acting to protect people as the state should, albeit outside the usual mechanisms.

Therefore, in instances where good laws are not being enforced then the laws themselves can act to provide both legitimacy and guidance to the hacker. Such laws already represent a source of good in society, are agreed upon by the political community and are recognised as being worthwhile. In this instance the hacker can appeal to the law as it stands, and in doing so acts as the state should. This allows a more nuanced and detailed set of instances for when the hacker can act given the established body of law that exists. Whereas in cases where the state is enforcing 'laws that are actually evil or unjust and, as such, do not afford protection to members of society that they should' (McReynolds 2015: 441), to make this determination reference should be made to the fundamental vital interests to determine the threat posed to an individual's physical or mental integrity, autonomy, liberty, or privacy. For example, Carl Cohen argues that certain laws can be deemed as invalid if they deprive someone from constitutionally guaranteed rights (1970: 7); while David Lefkowitz refers to the need for a clear 'undefeated moral reason' (2007: 206); and Rawls that the laws must be clear 'principles for assigning and servicing fundamental rights and liberties' (2009: 245). Recognising such transgressions as well as what counts as a good law can be aided by appealing to universal

statutes, the Universal Declaration of Human Rights for example, as they offer a codified version of our vital human interests and can act as a source of international authority from which the hackers can draw. However, due to the various localised interpretations of such norms they can only act to provide a thin layer of protection, a minimum level to which all people's vital interests should be ensured. For example, that people should, other things being equal, be free from pain and mental anguish, should have spaces where they know and can reasonably expect to be in private and have control over their information, have freedom of movement, value their self-worth, and have the capacity to decide for themselves how to make decisions, an important aspect of which is being aware of relevant information and being able to access information to aid in their decision-making processes.

Significantly, in making this calculation the initial position is such that legitimate authority rests with the state, and only when it fails to fulfil its ethical obligation can other actors intervene. This means recognising that, on the one hand, that no state is perfect and such imperfections do not make the whole state a failure and undermine all its legitimate laws and activities, but on the other hand even near-just states can fail in specific areas and thus create a space for intervention. This means distinctions are needed between instances where the state fails because it is not infallible in an uncertain world, and those where the state has acted negligently. In the case of the former if the processes are generally sound and are not in themselves problematic, then the failure or the occasional miscarriage of justice is not sufficient to argue that the state has failed in its attempt to offer protections. Failure is different to negligence whereby the latter denotes deficiency in exercising appropriate care and judgement – whether wilful or not – that results in the harm of another. This can include intended and unintended negligence where the actor fails to maintain the general ethical expectations of society as well as the specific additional standards of their profession.[16] For example, systematic discrimination such as racism or homophobia, corruption, failure of the duty of care, are instances of negligence, while plea-bargaining, unforeseen accidents, or rules that in the majority of cases provide just results but do fail and whose failure could not have been anticipated, represent mistakes in an otherwise just system. Therefore, the hack should be targeted only on those instances where the state has neglectfully failed, recognising that near-liberal states can have such instances due to negligence, incompetence, inability or lack of will. It is just that in authoritarian states such failures are more likely to be widespread, systematic and of a greater magnitude.

This can include for example, first, when the state is the source of the threat. For example, *en masse* violations of vital interests such as freedoms of speech, privacy or association means the state loses its legitimate authority and the hackers can intervene. Or second, when the state is unwilling or unable to prevent harm because it does not have the technical ability or manpower- although hackers should relinquish authority once the ordinary mechanisms are sufficiently available. For example, dark web activity entails a large degree of technical skills and manpower, but once information of harmful activity has been collected it should be forwarded for state authorities to act. Third, this also includes cases in which the state is unwilling to act to protect people – through a lack of political will for example – despite clear and compelling evidence of a threat. Appealing to legal cannon on evidence and balance of

---

[16] For example, 'professional negligence' demands that individuals within a profession or position of authority are held to a higher standard where they are charged with additional duties to protect those within their care and are expected to have higher than average abilities, knowledge or training and should act diligently and knowingly. (Horsey 1994:974; Lepora and Goodin 2013)

probabilities can aid the hackers in knowing how and when to act. However, simply disagreeing with the state's legitimately arrived decision is not sufficient. If, for example, the court has reviewed a case, the correct processes were followed and the judgement was one of not guilty then, short of new evidence, the hackers should not act. Therefore, the aim is not to justify all forms of private political violence, but only in very specific instances where the state has negligently failed, and then only when there is a just end as detailed in the next section.

4 Ethical Framework: Justifying the Act

As it has been previously detailed, the political justifications often directly stated by hackers can be quite varied, ranging from delivering punishment against wrongdoers including paedophiles, hate groups, and corrupt businesses, to protecting key civil and human rights, such as the right to information, expression and speech.[17] Or they can reflect a broad political orientation or ideology, ranging from generic left-leaning and socialist ideals, to anti-right-wing sentiments, to specific statements on anti-establishment or anti-corporativism, to radical freedom of online information where information should be free for sharing regardless of the original owner of the information.[18] To this end, despite the different objectives put forward by hackers it will be argued that acting in self-defence/defence of others can offer a way of understanding if and when the hack is justified. Moreover, by examining the hack in terms of self-defence, it is possible to further see how private individuals can act to use political violence as legitimate agents.

In terms of self-defence, while there is significant debate regarding its underlying justifications, and Fiona Leverick offers a very strong review of consequentialist and person partiality approaches, it will be argued here that at its core the individual first and foremost has the right to protect their own life, even at the expense of another's; and that when an attacker represents a threat they forfeit their usual protections that prevent the victim from killing them (Alexander 1976; Kasachkoff 1998; Montague 1989; Otsuka 1994; Thomson 1991; Leverick, 2006). The starting position here is that the right to life is considered a fundamental, if not the fundamental, human right. Moreover, this is a Hohfeldian claim-right where the importance of the right to life is such that it places duties on other individuals to act so as not to violate that right (Hohfeld 1913). There is a duty to respect the right to life. This duty means that it is not just the victim who has a right to act, but others can intervene to prevent the attack. (Thomson 1991: 306; Christopher 1998; Wasserman 1987). Fabre extensively discusses this point arguing that the victim's 'fundamental interest in surviving A's attack is not merely protected by a right to kill A: it is also protected by a *prima facie* power to transfer that right' to a third party and to 'claim otherwise is to impose an arbitrary restriction on V's ability to promote this fundamental interest of hers' (Fabre 2012: 62–63). This duty created not only prevents violating an individual's right to life, but actively promotes others to avoid violating it and also allows defenders to intervene when appropriate. Importantly, this means the individual's right to self-defence has primacy over other considerations, such as

---

[17] For example, Operation Tunisia and Operation Egypt sought to provide tools to circumvent state online censorship.

[18] For example, Operation Megaupload hacked United States Department of Justice, the United States Copyright Office, the Federal Bureau of Investigation, the MPAA, Warner Brothers Music, the RIAA, and the HADOPI in retaliation for the shutting down of the file-sharing platform Megaupload.

limiting the legitimate use of violence to only state representatives. That is, the victim or defender need not wait for a state representative – such as the police – to intervene before they can carry out their necessary protections. While there are practical considerations that often promote turning to state representatives, the individual's fundamental right to defend themselves comes first.

While much of the self-defence literature, especially that which focuses on wartime killing, is often interested in protecting life and limb and the right to use deadly force to protect oneself as a result, this can be expanded to recognise the other key aspects of the human condition that need protection. That is, protecting oneself should include protecting all our vital interests: those preconditions that all individuals have, by virtue of the human condition, that need to be fulfilled if they are to continue living their own version of the good life. Feinberg calls these requirements 'welfare interests' (1984: 37) and John Rawls calls them 'primary goods' (1971: 62), whereby regardless of an individual's conception of the good life these preconditions must be satisfied first in order to achieve them. In this way, these interests are the most important a person has, and thus cry out for protection (Feinberg 1984: 35; Nussbaum 2000: 76). These vital interests include, probably most obviously, the interest in maintaining one's physical integrity and the need to be free from pain, but also includes psychological and emotional integrity, autonomy, liberty and privacy. Moreover, these vital interest work as a matrix, each contributing to the human experience and all needing to be maintained to a minimal level and where an excess of one cannot make up the absence of the other.

These rights are so important that they cry out for protection, and indeed create obligations on others not to infringe upon them. So, while self-defence is often examined in terms of maintaining one's physical integrity it can also be understood as the right of the individual to protect their privacy, autonomy and liberty. Using the 'self-defence' terminology to refer to protecting one's non-physical vital interests might cause some to pause, but this is more because of the focus in the literature on discussions over when it is right to kill another to stop an impending aggressor, rather than there being any lack of there being a right to act to protect one's other vital interests from the unjustified infringement by others. For example, the privacy literature extensively discusses the different instances and types of defensive barriers one can erect and the actions one can take to stop others from accessing personal information – whether legal, physical or metaphorical.[19] Equally, the literature on autonomy argues for even forcible responses on those who wish to control one's ability to make and perform one's own informed decisions.[20] This conceptualisation helps give greater credence to arguments where a victim could be justified in harming an attacker who threatens their non-physical vital interests, such as those who suffer psychological and emotional harm. For example, this stresses the uniquely horrific harms of rape as it adds the severe psychological, emotional and autonomy harms to the physical (Laugerud 2019); or it could also give greater weight to victims of spousal abuse who suffer psychological torment, or are abused through controlling and manipulative behaviour; or even torture which relies on psychological and emotional attacks such as degradation, humiliation, and fear. What is key is that an individual's vital interests are fundamental to the human condition, require protection, place duties on others not to unjustly infringe on them, and in turn give the individual the right to defend through some appropriate and proportional action from others infringing on them. Importantly for this paper, understanding self-defence

---

[19] For the right of privacy and the limits – whether as control or boundaries – see: Paine 2000; Fairfield 2005; Marx 1998; Thomson 1975; Shils 1966; Westin 1967; Fried 1969.
[20] Nussbaum 2000:79; Feinberg 1973; Lindley 1986a, b; Frankfurt 1971; Herman 1996.

as being more than just physical protections is important because it highlights other key, cyber-related interests that need protection – such as the interest in autonomy and the implications this has for the right to information.

This expansion also nuances the connected defensive action, highlighting the relationship between the vital interest threated, the type of threat posed and thus the justified appropriate means for achieving the necessary protection. A key part of this is understanding that these interests are not binary, whole one minute and destroyed the next, but occur and are impacted in different ways and to different extents, and in turn shape different types of justified defensive activities. The type of self-defence justified, therefore, is determined by the particular vital interest threatened, the severity and duration of the threat, and its temporal proximity. (Feinberg 1984: 37; Rescher 1972: 5). For example, each of our vital interests can be impacted to different degrees: people can suffer various levels of physical and mental pain; their autonomy can be circumvented to different degrees; their physical liberty restrained for different periods of time; and their privacy can be perceived as consisting of different levels where the more personal or intimate the information the greater the expectation of privacy and the greater the harm caused when violated (Marx 2004: 234; Hirsch 2000; Feinberg 1984: 46). Thus, for threats that are of lesser magnitude than killing or severe pain, while there might not be a justification to kill in self-defence there could be justification for a low-level physical response, loss of property and resources, or sanctions (Pattison 2018).

Furthermore, this more flexible conceptualisation of self-defence has a key temporal aspect. Many self-defence justifications include a feeling of imminence, such as Thomson's innocent who is about to be run down by a truck, where the threat posed to the victim is very nearly upon them, which means the probability of the threat materialising is high and there are no opportunities for less harmful counterattacks (1991: 283). However, imminence is not always helpful when considering threats which are highly likely to occur but are far away; or where the threat is the systematic and widespread erosion of core vital interests; or where the only viable form of defence is when the threatening actor themselves no longer represents an immediate threat – most notably in the case of women who kill their abusive husbands while they sleep. As a result, the self-defence literature makes the distinction between 'self-defence against present definite threats… definite future threats… as well as indefinite potential threats' (Lee 2018: 346; Walzer 2000). These temporal and probability distinctions in turn shape the type of defensive action the potential victim can take. That, while imminent threat to life is often used in justification of killing in self-defence, threats which are more temporarily distant can still be defended against through non-lethal, though still harmful, defensive actions such as restricting the liberty of the threat, reputational and financial harms, and temporary physical harm such as unconsciousness (Pattison 2018).

In terms of hacking, therefore, what this means is that the hack used should reflect the threat posed. That is, in those instances where the individual's rights to information are being circumvented then the defence act justified is to provide individuals greater online protections or the ability to circumvent state online censorship tools to protect people's vital interest in privacy and autonomy.[21] In comparison, if the threat posed is to the individual's physical and mental integrity then following the more traditional arguments of self-defence the hackers are justified in using more destructive means, though given the likelihood that an individual's life

---

[21] The most famous of these is China's 'Golden Shield Project' – also known as the Great Firewall of China – that not only censor online content but also systematically probes for and shuts down any programs that might try to aid access to outside information. See TOR (2015).

is not going to be in imminent danger then deadly force would not be justified. While instances where the threat has more direct implications for an individual's ability to act as a free political agent then the hack should be used to provide that agency, using proportional force to the degree to which the individual's autonomy is being controlled or subverted.

4.1 Wider Consequences and Protecting Innocents

Additional limits are necessary in order to aid guide the hacker while also preventing unjustified harm in terms of level of attack and the targets impacted. One limit is that of proportionality, which itself raises two different requirements: first, there needs to be a threshold that must be reached before the hacker can act because not every small insult or injury warrants the type of damage caused. Second, that the response itself must be proportional to the problem faced. For the first point, hacking is essentially an extraordinary response, a situation where the normal mechanisms of the state and its institutions are deemed to have failed. The private action is supporting the ethical role of the state in its idealised form; it is not intended to replace the state per se. It should therefore seek to not be the norm. In an idealised situation it would not be needed. Therefore, it should limit itself only to those failings that are clear and significant. For example, 'rude behaviour in traffic even where there isn't an adequate police presence would not suffice to justify a vigilante response. Nor would rude behaviour on an Internet message board' (McReynolds 2015: 427).

To make the second calculation on the overall benefit of the hack, key critical questions can be asked to help guide decision-making, including first, what level of harm is caused by the hack? Most hacks will necessarily entail some form of damage. For example, this could range from financial costs as a website or network is rendered inoperable, or reputational costs as systems are undermined and / or embarrassing information is revealed; to costs to one's privacy or autonomy as private information is stolen and released; to even costs to people's lives if critical infrastructures are shutdown or hindered. These damages must not exceed the perceived benefit of the hack, and in doing so this limits the hack from escalating. This means detailing what benefits the hack will provide as a positive in the calculation, such as providing increased access to online information and enabling freedom of expression, or actually preventing the violation of an individual's privacy or autonomy. Finally, what harms are allowed to continue if the hack is not carried out? For example, who is being harmed or is likely to be harmed and what is the extent of the harm if the *status quo* is allowed to continue. So, if an individual's right to information is being limited then the hack must correspond and correct this harm by giving them greater access; whereas if their physical security is threatened then this would represent a justification for a greater hacker attack that sought to prevent this harm from happening, such as coercing or even harming the threatening agent. There are, however, limits to the necessary calculation hackers have to make. For example, unforeseen and/or unintended consequences cannot be expected to be included in the moral calculation made by hackers. Similar to the doctrine of double effect, whereby actions with foreseen damage can be permitted when the harm is not directly intended, nor is a means to achieving the good and proportionate end (Mangan 1949: 43).

Finally, the attack must discriminate between legitimate and illegitimate targets. The underlying argument is that those individuals who make themselves a threat or do wrong essentially waive or forfeit the normal protections they have from being interfered with (Nagel 1986: 162; Moore 2010: 1). It can be argued, therefore, that the harm directly inflicted through the hack should only negatively affect those who have either done wrong or who pose a threat.

This can include not only individuals who have caused or will cause others harm, but organisations and states as well. In these latter cases the attacks can either be targeted against the offending systems or structures, or those individuals directly responsible for them and for the continuation of the harm. Broadly speaking this would mean that the hack should only directly affect those who are the source of the problem and not impact 'innocent' bystanders. This can be quite flexible however, with different hacks being justified against different actors depending on their role. In this way, involvement can be seen as a spectrum, where depending on one's role in the threat the level of harm caused by the hack should vary. At one end are those who (whether people or institutions) have actively fostered an highly unethical state of affairs – including perpetuating or carrying out systematic physical attacks against others for example – making them legitimate targets for harmful hacks, while at the other end those who are minimally complicit – by failing to act when they reasonably could have but who have not directly contributed for example are only just targets for hacks that minimally impact them, a mild irritation or inconvenience for example.

4.2 Decision-Making and Limiting Bias

At the core of this paper is the argument that hackers can legitimate when their activities are used to protect others from unjustified harm and when there are no other actors, traditionally the state, who are able or willing to intervene. This places the right to defend others as primacy over making sure that more established actors are the ones to act. That is, one does not need to wait for the police before defending someone else's life. However, there are still some ethically important practical mechanisms used to help guide decision-making that, as much as possible, aim to achieve the best ethical end; so that the correct individual is subjected to the appropriate type and level of response. Indeed, traditional mechanisms such as due process, right to appeal, transparency, right to representation, and complaint mechanisms are valuable because they represent key mechanisms for ensuring the best form of action; for trying to ensure the right action is carried out to the right individual, or that all individuals' rights are treated equally. The concern is that hackers could be prone to making biased, politically partisan, or incorrect decisions.

So, while the ethical framework can be used to inform hackers and society on what an ethically justified hack might look like, there are additional mechanisms that can also help the decision-making process itself while also reassuring the rest of the political community. To aid hackers we can draw out some of the key lessons from deliberative democracy concepts and institutions. For example, Chambers argues that even in secretive environments, a deliberative ethos can still be replicated 'applying the publicity test by welcoming diversity of opinion' (2004: 408). For hackers this highlights the need for mechanisms that instil a process of engagement and dialogue; that they have mechanisms for discussion, interrogation and review. The devil, however, is often in the detail and, while it is not the aim of this paper to give organisational specifics but to highlight underlying principles, it is possible to foresee what useful tools might look like. This would include, firstly a deliberation process to allow critique, debate and reflection to minimise the likelihood of personal bias. Hacker intentions, objectives and demands should be made public to allow for others to reflect on their reasoning. Second, a means for publicly debating these objectives and intensions can help ensure the logic is sufficiently interrogated. This could be supported by a means of collecting and sharing different opinions and giving individuals opportunity to voice objections or provide new information. Finally, a means of collating and distilling an overall decision can shape a

coherent justification and matching methods. While these mechanisms do not guarantee an ethical decision will be made, their aim is to increase its likelihood, and by presenting the process publicly reassure the political community as to the deliberative process.

While there might be concerns that such mechanisms are not feasible due to hacker anonymity and given their decentralised and anti-hierarchical structure, this is not necessarily the case. In practice being decentralised, anti-hierarchical and anti-leader does not necessarily mean that there are no decision-making processes or discussions in place, nor that they cannot be made more systematic and engaging – and can in fact prove to be a benefit to the collective itself. Philip Gray (2013) argues in regard to other protest organisations, having an anti-leader, non-hierarchical structure can act to facilitate discussion and action, allowing for greater flexibility, adaptability, wider appeal and inclusivity, while still being able to make decisions in a timely and directive manner. While these principles might initially seem counter to the idea of the lone hacker wreaking havoc from their private rooms, many hacker collectives exhibit such behaviours. Indeed, the Anonymous super-organism, whereby individuals coalesce around a particular cause and cooperate to produce the necessary results, operates in a similar methodology to the 'occupy movement' whereby individuals came together to fulfil a particular goal but move away again once the movement is over (Serracino-Inglott 2013). This fluid and open structure necessarily invites dialogue and debate, albeit through non-traditional avenues. The internal decisions are already typified by horizontality and consensus, where plurality of opinion and a reliance on mass contribution limits bias, and as Coleman details through the 'public channels' Anonymous does debate and vote on operations (2014: 101–105). Indeed, the anti-leader ethos actively promotes discussion and voting procedures in order to enable a decision-making process. Though these processes should be encouraged through more explicit, public and open dialogue on online public forums with an established decision-making process. For example, there are already established platforms for sharing of ideas that rate ideas and have proven useful in generating a collective understanding on a topic from a diverse global membership. Most notable among these is reddit.com, a social news aggregation and content rating website that allows members submit content - such as links, text posts, and images – that is then voted up or down by other members.[22] Anonymity can still be maintained and it can reflect an anti-hierarchical ethos, though making it more officially open to outside involvement and formalised to ensure alternative points of view.

The overall framework therefore does not discount individuals or smaller groups from acting, just that these inclusive mechanisms increase the likelihood of a more reflective decision being made and that agents should be aware of their own shortcoming in making decisions and their implications.

5 Applying the Framework: Hackers, Online Rights and Real-World Fights

In one set of attacks hackers have focused on government institutions and representatives in order to protect freedom of information, expression, association and autonomous political engagement – all key manifestations of the vital interests' people have in maintaining their autonomy and privacy. During the Arab Spring, for example, Operation Tunisia and Operation Egypt, Anonymous aided the emerging protest movements by shutting-down government

---

[22] See https://www.redditinc.com

websites and helping dissidents circumvent online censorship. On 2nd January 2010, Anonymous began Operation Tunisia by landing a successful DDoS attack against several Tunisian government websites include the President, Prime Minister, and Ministry of Industry, Minister of Foreign Affairs, Stock Exchange, and the government Internet agency that had been censoring online dissidence. Operation Egypt started on 26th January 2011 with DDoS attacks on Egyptian Cabinet Ministers and provided online 'core packages' to aid communications during the protests; while in 2012 Anonymous attacked Syrian government websites in an attempt to fight government censorship (Greenberg 2012b). Anonymous announced in relation to Operation Tunisia: 'A time for truth has come. A time for people to express themselves freely and to be heard from anywhere in the world. The Tunisian government wants to control the present with falsehoods and misinformation in order to impose the future by keeping the truth hidden from its citizens. We will not remain silent while this happens' (Coleman 2014: 148). In other non-Arab Spring examples Anonymous attacked the Thai government through Operation Single Gateway after it was reported that all Internet activity would be routed through a single node that would allow for government monitoring. Anonymous stated, 'We saw the situation in Thailand for the past months going too far, restricting basic access to freedom of speech, protests and basic human rights against anyone who criticised the Thai Junta' (Bangkok Post 2015).

Each of these attacks focuses on the importance of online freedoms, seeking to preserve or reinstall civil and human rights, and aims at damaging state infrastructure through DDoS attacks or undermining the legal restrictions on digital access. In all of these cases the state directly limited the people's access to information, an extension of the right to the freedom of speech recognised in international law as a fundamental human right, causing them harm. Freedom of expression and information goes to the heart of the vital interest individuals have in protecting and carrying out their own fully autonomous life and preserving their privacy – both vital to the human condition. It can be argued, therefore, that tools that damaged or destroyed excessive government control of cyberspace offers a means to remedying that harm. In Tunisia 'Ben Ali's government tightly restricted free-expression and political parties' (Anderson 2011: 2), while in Egypt as the protests started social media websites were increasingly blocked (Woodcock 2011), and in Libya Gaddafi's government severed Internet access and international phone calls (Hill 2011). The DDoS attacks represent a direct attack on the government as the source of the harm, and while the attack was damaging and a form of low-level violence, the impact is still lesser compared to the larger harm caused by limiting people's freedom of expression. Also, as the source of the threat there is no authority to appeal to or legal route to work through, offering no other resorts. Therefore, these attacks can be justified. While freedom of expression is a contested concept and determining its exact nature difficult – with courts debating where to draw lines between free speech and saying offensive, aggressive or hateful things – the right to expression or information access can be strongly established both in international law and in reference to the important role it plays in people's autonomy (Nussbaum 2000: 79; Frankfurt 1971: 7). Indeed, if individuals do not have the full facts before them or could not reasonably be able to comprehend its meaning then they are unable to make an informed decision; their capacity to reflect on options and determine for themselves their most appropriate action is prevented and they are therefore unable to act autonomously. Therefore, providing people with technology that stops state control and unjustified state monitoring plays an important role in re-establishing people's vital interest in autonomy. Also, anonymising technology can promote a realm of greater autonomy exploration as people's actions would be unmonitored and preventing the stifling effect that

outside monitoring can have as particular standards of 'correct', 'right' or 'true' are imagined or imposed. What anonymising technology creates is a more open space for individuals to explore these issues themselves.

These cases do raise an important broader question of whether hacks that argue for the freedom of information should use tactics that ultimately restrict people's access to information. Indeed, this is a concern Coleman notes that hackers themselves have raised: 'whether DDoSing is an exercise of the right to free speech or an act aimed at precluding the same right for other' (2014: 132), and as one Anonymous contributor argued 'i dont think DDoS can be in the name of freedom of speech' (2014: 133). As previously argued, however, by distilling the different political acts to their relationship to our core vital interests such comparisons can be made. That is, in Operation Tunisia and Operation Egypt, there is a much greater and systematic limit to a general right to free speech that make the localised government shutdowns the lesser of the rights violations. In comparison, when the US government shutdown video and file sharing platform Megaupload for illegal distribution of copyrighted data and Anonymous responded with hacks that shut down US Department of Justice, Warner Music Group, Motion Picture Association of America and Universal Music Group's websites, it can be argued that this was essentially an unjustified hack. The justification given by Anonymous was based on a freedom of information mandate (Waqas 2012). While the right to share information does have virtue when it has been decided by the owner of that information, to go against the originator's wishes is essentially a violation of their right to privacy.[23] There is therefore no justification in that there is no threat to someone's vital interests – there still exists a general right to share information which is yours to share, something not seen in the case of Tunisia and Egypt.

In a slightly different set of attacks, hackers have sought to apply pressure and blackmail governments to prevent legislation that will discriminately harm a section of their society. For example, in both Nigeria and Uganda, Anonymous launched hacker attacks in response to their anti-gay legislation, taking down government websites in response to the 'intent to pass a law that would jail LGBT people for up to 14 years' along with other discriminatory policies (Littauer 2013; Ford 2012). Anonymous declared, 'Nobody should live in fear of being jailed, when their only action is loving another consenting adult, regardless of gender… Failure to follow our order will unleash a torrent of fury aimed directly at the direction of your administration, starting with some startling but unsurprising evidence of corruption in your ranks' (Littauer 2013; Boone 2013). In these cases it can be argued that given the political and social climate that homosexuals (or even those wishing to act on their behalf) have suffered in these political communities, there is a clear threat to their physical, emotional and psychological interests. Examples of violent, public abuse to homosexuals — by official authorities including the police – serves to highlight the social problems and the harm that homosexuals are likely to face as a result of a law that encourages discrimination and the normalization of existing abusive treatment (Walker 2016). Furthermore, social stigmatization and institutional abuse is likely to limit individuals coming forward, restricting ordinary legal avenues. In terms of authority, the state represents the source of the threat and so calls out for a new entity to act

---

[23] This is following Judith Thomson's argument that one way of conceptualising privacy is to see it as being akin to a collection of property rights. That is, individuals have the right to control that which is about them or that which they are author of as an important part of their right to privacy. They might wish no one being privy to it, or they might wish only certain people to be included. They can even pass this decision on to others, including corporations. In this way we can see copyright as part of a wider set of debates over privacy and the right control that which is ours. See Thomson 1975:303; Shils 1966:290; Parent 1983.

on behalf of those who would be harmed. For proportionality, given the threat to the lives of homosexuals in Uganda and Nigeria, using hacks that caused a minimal amount of physical damage in order to raise awareness of the problem to the wider public and to put pressure – even blackmail – on the government is justified as it seeks to prevent harms and defend homosexuals against clear physical and social harms. While shutting down government websites might negatively impact people, the damaged caused to inconveniencing people is less than legislation that encourages and fosters severe harm to a portion of society, especially when the websites concerned are predominately for information and the attack was more symbolic rather than limiting necessary information or services. These cases represent an instance of the state erecting bad laws that unjustly discriminate a portion of their community while also fostering and promoting a homophobic atmosphere that will cause harm to the LGBTQ+ community.

A third key set of hacker attacks has been made against what would be considered to be more 'liberal-democratic' states, mainly the USA. Operation BART, for example, was in response to the San Francisco's Bay Area Rapid Transit (BART) team turning off cellphone service in reaction to a planned peaceful protest that itself was being held to protest the fatal shooting of Charles Hill by the police in July 2011. In one video Anonymous argued that such tactics represented a direct threat to the rights and safety of US citizens, and announced that it would 'show those engaging in censorship what it feels like to be silenced' (anon2world 2011,) and bombarded BART officers with copies of its political message; attempted to bring down the BART website through DDoS; and finally released 2400 BART customer's information in an attempt to embarrass the organization. In a similar case, after police shot teenager Michael Brown, Operation Ferguson supported local protests by applying pressure to have the shooting police officer's name released by shutting down City Hall websites and phone services. When the name failed to be released @TheAnonMessage threatened to publish St Louis police chief's daughter's personal details, including social security number and phone number (Rogers 2014). Finally, in yet another similar case in Cleveland, Anonymous attacked the city's official website after 12-year-old Temir Rice was shot by local police, with the aim of raising awareness to the incompetence of police training and again calling for the names of the shooters (Stone 2014).

These hack attacks were aimed at raising awareness and forcing what they saw as suitable responses from the police as well as seeking to punish those who caused the harm by shaming the authorities and encouraging official steps to be made against those involved. In the case of BART the hackers were seeking to re-install the ability of protesters to carry out their protest successfully. There is a justification, therefore, for some action as the state threatens without reason the general right to protest. However, when the attacks turned to revealing personal information of BART customers the justification is lost as it affects those who were not involved. The personal information of these customers is their property to determine who has access to it; the hacker's information dump undermines their vital interest in privacy (Fried 1969: 475; Gross 1971: 169; Thomson 1975: 303; Breckenridge 1970: 1). Equally Operation Ferguson's aim to force the authorities to release the names of the shooters can be justified as encouraging already established oversight mechanisms. However, again when it comes to doxxing – releasing the police chief's daughter's private information – this crosses the discrimination line. While collateral damage could be justified in-line with the doctrine of double effect if the harm was foreseen but unintended, this was directly aimed at causing to daughter distress to alter the police chief's activity. While arguably the chief of police is a legitimate target – he is aware of his rank, position of authority and his part in the game being

played (Pfaff and Tiel 2004: 7) – and so has agreed to the responsibilities and dangers that come with his position, his family and friends are not legitimate targets: they hold no position of authority nor have they acted in such a way as to waive their protective rights. While doxxing would often therefore be discounted as an ethical tool given its reliance on sharing private information of those who are not involved in the threat, if the release was such that it included evidence of those involved causing harming then this harm would justify the violation of privacy. For example, the doxxing of Klu Klux Klan members in 2014 who were issuing threats to protestors who were responding to the police shooting of Michael Brown, and in the 2011 Operation Darknet, 2015 Operation DeathEaters and 2017 Operation Darknet Relaunch where Anonymous sought to collect evidence against international paedophiles rings so to 'bring them to justice' by revealing their identity (O'Neil 2015; Eleftheriou-Smith 2015). Though to whom the information is released and in what format will be determined by the type of threat and required remedy.

Finally, there have been some hacks that, while they have a clear political message, are more a representation of the personal politics and beliefs of the hackers. For example, in 2015 the World Trade Organisation was compromised when hackers leaked more then 53,000 email addresses, with 2100 names, phone numbers and job titles. In addition to the breach there were concerns this personal information could place the workers at risk of 'phishing attacks' whereby their emails are used to defraud them or to install malicious programs. The hack was accompanied by a vague anarchist statement against large corporations and governments: 'We are here to hack all your systems. We will not stop. We will not give up. We have enough rope to hang you and your puppets. Expec us [sic]' (Hackett 2015). The attack itself has been tied to the 'operation green rights' cause that attacks governments and corporations for environmental reasons and included shutting down websites for French conglomerate Areva over its plans to build a nuclear power station stating: 'Areva can't even secure their website, how can they secure their nuke?' (Hackett 2015). However, there is no justification in that there is no threat to someone's vital interests and in fact these actions represent a clear threat to some people's right to privacy.

6 Conclusion

The use of political hacking clearly raises some important ethical questions around who can use political violence and to what ends. For some, hackers act outside the state and so do not have the moral authority to use violence, and that there are no clear and systematic cultural or ethical guidelines for shaping and informing behaviour. However, it has been argued that there are instances where the state has either failed in its role or is a source of a threat in people's lives, and so limiting the right to defend oneself or other is not ethically correct. It has been argued that even states that have extensive established human rights protections in place can fail in specific cases and so justify some form of response from a non-state actor. As such, individuals, groups and collectives can act as ethical agents; they can act to prevent others from violating our core vital interests and that by being outside the state does not automatically discount this. However, hacking is a complicated, multifaceted and fluctuating phenomenon. A variety of agents, acting for a variety of causes with open and fluid opportunities for others to engage makes developing any systematic review incredibly difficult. The Anonymous of today could be different to the Anonymous of tomorrow. However, this ethical framework gives us a place to start: by examining the activities of a hacking agent in relation to political

situation through the distilling their actions and the mapping of them to our core rights we can start making ethical judgements and statements about their actions as a form of defending people against some of those threats which others have failed to prevent. This can then inform both those on the outside and within on how to react and what the next set of steps should be. This ethical framework is the first step in understanding what an ethical hacker looks like and can form the basis of a new ethical hacker culture.

References

Alexander L (1976) Self-Defence and the killing of non-combatants: a reply to Fullinwider. Philos Public Aff 5(4):408–415

Anderson L (2011) Demystifying the Arab spring: parsing the differences between Tunisia, Egypt, and Libya. Foreign Affairs 90(3):2–7

anon2world. 2011. Anonymous: Operation BART. *YouTube* August 14. https://www.youtube.com/watch?v=lG0C4lhE6bg

Anonymous. 2011. AnonNews.org: everything anonymous AnonNews.org: Everything Anonymous. http://anonnews.org/press/item/199/

Anonymous France. 2015 [FR] anonymous - #OpCharlieHebdo YouTube January 10 https://www.youtube.com/watch?v=Z_QxrqjpWcE&feature=emb_logo

Auty C (2004) Political hacktivism: tool of the underdog or scourge of cyberspace? New Information Perspectives 56(4):212–221

Bangkok Post. 2015. International Hackers Strike. *Bangkok Post* 22 October. Available at http://www.bangkokpost.com/tech/local-news/739884/anonymous-steps-up-single-gateway-protest

Bansal A, Arora M (2012) Ethical hacking and social security. Journal of Radix International Educational and Research Consortium 1(11):1–16

Barber R (2001) Hackers profiled – who are they and what are their motivations? Computer Fraud and Security 2(1):14–17

BBC News, 2007 'Estonia hit by 'Moscow cyber war', *BBC News,* May 17. http://news.bbc.co.uk/1/hi/world/europe/6665145.stm

Bellaby R (2018) Extraordinary rendition: expanding the circle of blame in international politics. The International Journal of Human Rights 22(4):574–602

Blomfield A (2007) 'Estonia calls for NATO cyber-terrorism strategy', *The Telegraph,* May 18 https://www.telegraph.co.uk/news/worldnews/1551963/Estonia-calls-for-Nato-cyber-terrorism-strategy.html

Boone J. (2013). In Defence of LGBT Rights, Anonymous Adopts 'Scorched Earth Policy' for Ugandan Online Infrastructure. *The World* January 10, https://www.pri.org/stories/2013-01-10/defense-lgbt-rights-anonymous-adopts-scorched-earth-policy-ugandan-online

Borsook P (2000) Cyberselfish: a critical romp through the terribly libertarian culture of high tech. PublicAffairs, New York

Braham M, van Hees M (2012) An anatomy of moral responsibility. Mind 121(483):601–634

Breckenridge AC (1970) The right to privacy. University of Nebraska Press, Lincoln

Brownlee K (2016) The civil disobedience of Edward Snowden: a reply to William Scheuerman. Philosophy and Social Criticism 42(10):965–970

Cardwell T (2011) Ethical hackers: putting on the white *Network Security* July: 1–13

Celikates R (2016) Democratizing civil disobedience. Philosophy and Social Criticism 42(10):982–994

Cha A, Nakashima E (2010) Google China Cyberattack part of vast espionage campaign, Experts Say, The Washington Post Available at: http://www.washingtonpost.com/wpdyn/content/article/2010/01/13/AR2010011300359.html?sid=ST2010011300360

Christopher R (1998) Self-defense and defense of others. Philos Public Aff 27(2):123–141

Cohen C (1970) Defending civil disobedience. Monist 54(4):469–487

Coleman G (2011) Hacker politics and publics. Publ Cult 23(3):511–516

Coleman G (2014) Hacker, hoaxer, whistleblower, spy: the many faces of anonymous. Verso, London

Conway M (2003) Hackers or terrorists? Why it Doesn't compute. Computer Fraud and Security 12:10–13

Crosston, M. 2017 'The fight for cyber Thoreau: distinguishing virtual disobedience from digital destruction' in *Threat Mitigation and Detection of Cyber Warfare and Terrorism Activities*, edited by Korstanje, M. IGI global: 198-219

Delmas C (2018) Is Hacktivism the new civil disobedience? Raisons politiques 69(1):63–81

Denning D (2000) Activism, Hacktivism, and Cyberterrorism: the internet as a tool for influencing foreign policy in *Networks and Netwars: The Future of Terror, Crime, and Militancy*, Arquilla, J. and Ronfeldt, D. Rand,: 239–288

Dittrich D, Himma K (2006) Hackers, crackers and common criminals in *Handbook of Information Security: Information Warfare; Social Issues, Legal and International Issues; and Security Foundations, Vol.2* edited by Bidgoli, H. New Jersey, NJ: Wiley: 154-171

Duff A (2011) 'Retrieving retributivism' in *Retributivism: Essays on Theory and Policy* edited by white, M. Oxford University Press, Oxford

Dumsday T (2009) On cheering Charles Bronson: the ethics of vigilantism. South J Philos 47(1):49–67

Eleftheriou-Smith L (2015) Anonymous calls for activists to help expose international paedophile networks with 'Operation DeathEaters. *The Independent* January 2015. https://www.independent.co.uk/news/uk/home-news/anonymous-calls-activists-help-expose-international-paedophile-networks-operation-deatheaters-9998350.html

Emspak J (2011) Update: Egyptian Gov't Web Sites Under Attack, *International Business Times*, January 26, http://www.ibtimes.com/articles/105329/20110126/update-egyptian-gov-t-web-sites-under-attack.htm

Fabre C (2008) Cosmopolitanism, Just War Tradition and Legitimate Authority. *Int Affairs* 84(5):936–976

Fabre C (2012) Cosmopolitan war. Oxford University Press, Oxford

Fairfield P (2005) Public/Private. Rowman & Littlefield Publishers, London

Farsole A, Kashikar A, Zunzunwala A (2010) Ethical hacking. Int J Comput Appl 1(10):14–20

Farwell J, Rohozinski R (2011) Stuxnet and the future of cyber war. Survival: Global Politics and Strategy 53(1): 23–40

Feinberg J (1973) The idea of a free man, in *Educational Judgments: Papers in the Philosophy of Education* edited by Doyle, J. F. London: Routledge: 143-165

Feinberg J (1984) Moral limits of the criminal law: Vol.1 harm to others. Oxford University Press, Oxford

FLSnag (2011) I am one anonymous, *YouTube,* July 23, 2011, http://www.youtube.com/watch?v=aEcvaoDIKtU

Ford Z (2012) Anonymous hacks Ugandan government in retaliation for anti-LGBT policies Think Progress 14 August. https://thinkprogress.org/anonymous-hacks-ugandan-government-in-retaliation-for-anti-lgbt-policies-8d31d15aa874#.cbrcmbr9c

Frankfurt H (1971) Freedom of the will and the concept of the person. J Philos 68(1):5–20

Fried C (1969) Privacy: a moral analysis. Yale Law Review 77(1):475–493

Fuchs C (2013) The anonymous movement in the context of liberalism and socialism. Interface 5(2):345–376

Goode L (2015) Anonymous and the political ethos of Hacktivism. Pop Commun 13(1):74–86

Gray PW (2013) Leaderless resistance, networked organization, and ideological hegemony. Terror Polit Violenc 25(5):655–671

Greenberg A (2012a) This machine kills secrets: Julian Assange, the Cypherpunks, and their fight to empower whistleblowers. Penguin Group, New York

Greenberg A (2012b) Anonymous hackers swat at Syrian government websites in reprisal for internet blackout Forbes 30 November. Available at http://www.forbes.com/sites/andygreenberg/2012/11/30/anonymous-hackers-swat-at-syrian-government-websites-in-reprisal-for-internet-blackout/#105975b4418f

Gross H (1971) 'Privacy and autonomy' in *Privacy: Nomos XIII* edited by Pennock, J. R. and Chapman, J. W. New York: Atherton Press

Hackett R (2015) 'World Trade Organization officials and delegates should prepare to be phished' Fortune 7 May 2015. Available at http://fortune.com/2015/05/07/wto-hacked-anonymous/

Hampson N (2012a) A new breed of protest in a networked world. Boston College Int Comparative Law Rev 35(2):511–542

Hampson N (2012b) Hacktivism: a new breed of protest in a networked world. Boston College Int Comparative Law Rev 35(2):511–542

Herman B (1996) The practice of moral Judgement. Harvard University Press, Cambridge

Hill E (2011) How 'Rebel' Phone Network Evaded Shutdown. *Al Jazeera* 23 April. Available at http://www.aljazeera.com/indepth/features/2011/04/20114233530919767.html

Hirsch A (2000) The ethics of public television surveillance, in *Ethical and Social Perspectives on Situational Crime Prevention* edited by Hirsch, a., Garland, D. and Wakefield, A. (Oxford: hart publishing): 59-76

Hobbes T (1985 [1651]) Leviathan. Penguin Classics, London

Hohfeld, W. N. 1913. 'Some fundamental legal conceptions as applied in judicial reasoning' *Yale Law Journal* Vol.23 pp. 16–59

Holt T, Freilich J, Chermak S (2017) Exploring the subculture of ideologically motivated cyber-attackers. J Contemp Crim Justice 33(3):212–233

Horsey HR (1994) The duty of care component of the Delaware business judgment rule. Del J Corp Law 19(3):971–998

Information Warfare Monitor. (2009) Tracking Ghostnet: investigating a cyber espionage network. March 29. http://www.nartv.org/mirror/ghostnet.pdf

Jackson R, Pisoiu D (2018) Contemporary debates on terrorism. Routledge, Abingdon

Johnston L (1996) What is vigilantism? Br J Criminol 36(2):220–236

Jordan T (2014) Internet, society and culture communicative practices before and after the internet. Bloomsbury, London

Jordan T, Taylor P (2004) Hacktivism and Cyberwars: rebels with a cause? Routledge, London

Karagiannopoulos V (2018) Living with Hacktivism: from conflict to symbiosis. Palgrave Macmillan, Cham

Kasachkoff T (1998) Killing in self-defense: an unquestionable or problematic defense? Law Philos 17(5–6):509–531

Klein A (2015) Vigilante media: unveiling anonymous and the Hacktivist persona in the global Press. Commun Monogr 82(3):279–401

Krauth A (2012) Anonymous in Portmanteaupia. *Social Alternatives*, 31/2 p.27–32

Kumar, M. 2011 'Anonymous Open Letter to Citizens of United States of America!' *The Hacker News* March 24. https://thehackernews.com/2011/03/anonymous-open-letter-to-citizens-of.html

Lackey DP (1989) The ethics of war and peace. Prentice Hall International, London

Landler M, Markoff J (2007) In Estonia, what may be the first war in cyberspace, *The New York Times,* May 28 https://www.nytimes.com/2007/05/28/business/worldbusiness/28iht-cyberwar.4.5901141.html

Laugerud S (2019) Narrating the harm of rape: how rape victims invoke different models of psychological trauma. *BioSocieties* December

Lee H (2018) A new societal self-defense theory of punishment – the rights-protection theory. Philosophia 46:337–353

Lefkowitz D (2007) On a moral right to civil disobedience. Ethics 117(2):202–233

Lepora C, Goodin RE (2013) On complicity and compromise. Oxford University Press, Oxford

Leverick F (2006) Killing in self-Defence. Oxford University Press, Oxford

Levy S (2000) Hackers: heroes of the computer revolution. O'Reilly Media, Sebastopol

Lindley R (1986a) Autonomy. Macmillan, Basingstoke

Lindley R (1986b) Autonomy. Macmillan, Basingstoke

Littauer D (2013) Anonymous hacks Nigeria's government website over anti-gay bill LGBTQ Nation 5 July. Available at http://www.lgbtqnation.com/2013/07/anonymous-hacks-nigerias-government-website-over-anti-gay-bill/

Liu A (2004) *The Laws of Cool: Knowledge Work and the Culture of Information*. Chicago, IL: University of Chicago Press: 361-367

Locke, J. 1988[1689]. *Two Treatises of Government*. Cambridge: Cambridge texts in the history of political thought

Lowes D (2006) The anti-capitalist dictionary: movements. Fernwood Publishing Ltd, Histories & Motivations

Lu D (2015) When ethical hackers Can't compete. The Atlantic 8 December 2015. Available at https://www.theatlantic.com/technology/archive/2015/12/white-hat-ethical-hacking-cybersecurity/419355/

Ludlow P (2013) Aaron Swartz Was Right. *The Chronical of Higher Education,* 25th February Available at https://www.chronicle.com/article/Aaron-Swartz-Was-Right/137425

Mangan J (1949) An historical analysis of the principle of double effect. Theol Stud 10:41–61

Manion M, Goodrum A (2000) Terrorism or civil disobedience: towards a Hacktivist ethic. *Computers and Society:* 14–19

Markel D (2011) What might retributive justice be? An argument for the confrontational conception of retributivism in *Retributivism: Essays on Theory and Policy* edited by white, M. Oxford University Press, Oxford

Marx G (1998) Ethics for the new surveillance. Inf Soc 14(3):171–185

Marx G (2004) Some concepts that may be useful in understanding the myriad forms and contexts of surveillance. Intell Natl Secur 19(2):226–248

McCormick T (2000) Anthropology of an idea: Hacktivism. *Foreign Policy* 200:24–25

McGoogan C (2017) What is WannaCry and how does Ransomware work The Telegraph May 18. http://www.telegraph.co.uk/technology/0/ransomware-does-work/

McReynolds P (2015) How to think about cyber conflict involving non-state actors. Philosophy and Technology 28:427–448

Menn J (2019) Cult of the dead cow: how the original hacking Supergroup might just save the world. Public Affairs

metac0m, (2003) What is Hacktivism 2.0. The Hacktivist December 2003. Available at http://edshare.soton.ac.uk/8762/2/whatishacktivism.pdf

mmxanonymous (2011) OPERATION EGYPT: ANONYMOUS PRESS RELEASE – 26/01/2011, Youtube, January 26, http://www.youtube.com/watch?v=yOLc3B2V4AM;

Montague P (1989) The morality of self-defense: a reply of Wasserman. Philos Public Aff 18(1):81–89

Moore M (2010) Placing blame: a theory of criminal law. Oxford University Press, Oxford

Nagel T (1986) The view from nowhere. Oxford University Press, Oxford

Hampson NCN (2012c) Hacktivism: a new breed of protest in a networked world. Boston College Int Comparative Law Rev 35:511–542

Norman R (1995) Ethics, killing and war. Cambridge University Press, Cambridge

Nozick R (1974) Anarchy, state, and utopia. Basic Books, New York

Nussbaum M (2000) Women and human development: the capabilities approach. Cambridge University Press, Cambridge

O'Malley G (2013) Hacktivism: cyber-activism or cyber-crime? Trinity College Law Rev 16:137–160

O'Neil L (2015) Anonymous plans to 'unhood' 1,000 Ku Klux Klan members online. CBC-News, October 29, https://www.cbc.ca/news/trending/anonymous-plans-to-reveal-the-identities-of-1-000-kkk-members-1.3295523

Otsuka M (1994) Killing the innocent in self-defense. Philos Public Aff 23(1):74–94

Paine S (2000) Endangered spaces: privacy. CAMC Publications, Law and the Home

Parent WA (1983) Privacy, morality and the law. Philos Public Aff 12:94 (1983)

Pattison J (2018) The alternatives to war: from sanctions to nonviolence. Oxford University Press, Oxford

Pavli, A. 2019. 'Beneath this mask there is more than flesh, beneath this mask there is an idea': anonymous as the (super)heroes of the internet?' International Journal for the Semiotics of Law, March

Pfaff T, Tiel J (2004) The ethics of espionage. The Journal of Military Ethics 3(1):1–15

Posner, G. 2010. 'China's secret Cyberterrorism', The daily beast Available at http://www.thedailybeast.com/articles/2010/01/13/chinas-secret-cyber-terrorism.html

Quinn, B. 2011. 'PlayStation network hackers access data of 77 million users' The Guardian April 26. http://www.telegraph.co.uk/technology/news/8475728/Millions-of-internet-users-hit-by-massive-Sony-PlayStation-data-theft.html

Rawls J (1971) Theory of justice. Harvard University Press, Cambridge

Rawls J (2009) The justification of civil disobedience, in Arguing About Law ed. Aileen Kavanagh and John Oberdiek. Oxon: Routledge

Rescher N (1972) Welfare: the social issue in philosophical perspective. University of Pittsburgh Press, Pittsburgh

Reuters, 2014. 'JPMorgan hack exposed data of 83 million, among biggest breaches in history' October 3. https://www.reuters.com/article/us-jpmorgan-cybersecurity-idUSKCN0HR23T20141003

Reynolds P (2015) How to think about cyber conflicts involving non-state actors. Philos Technol 28(3):427–448

Rogers A (2014) What anonymous is doing in Ferguson. Time 21 August. Available at http://time.com/3148925/ferguson-michael-brown-anonymous/

Sanger D (2012) Obama Order Sped Up Wave of Cyberattacks Against Iran, The New York Times, 1st June, http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html

Sankowski E (1992) Blame and autonomy. Am Philos Q 29(3):291–299

Sauter M (2014) The coming swarm – DDoS actions, Hacktivism, and civil disobedience on the internet. Bloomsbury, New York

Scanlon TM, Daney J (2000) Intention and Permissibility. Supplement to the Proceedings of the Aristotelian Society, 74(1) 2000: 301–317

Scheuerman W (2016) Digital disobedience in the law. New Polit Sci 38(3):299–314

Serracino-Inglott P (2013) Is it OK to be an anonymous? Ethics Global Politics 6(4):217–244

Sheoran P, Singh S (2014) Applications of ethical hacking. Int J Enhanced Res Sci Technol Eng 3(5):112–114

Shils E (1966) Privacy: its constitution and vicissitudes. Law and Contemporary Problems 31(2):281–306

Shirky C (2008) Here comes everybody. Penguin Press, New York

Shukla S, Bhakta P, Bureau E. (2016) '3.2 million debit cards compromised; SBI, HDFC Bank, ICICI, YES Bank and Axis worst hit' The Economic Times October 20. https://economictimes.indiatimes.com/industry/banking/finance/banking/3-2-million-debit-cards-compromised-sbi-hdfc-bank-icici-yes-bank-and-axis-

worst-hit/articleshow/54945561.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst

Smallridge J, Wagner P, Crowl J (2016) Understanding cyber-vigilantism: a conceptual framework. J Theoretical Philos Crim 8(1):57–70

Squires J (1968) Blame. Philos Q 18(70):54–60

Stone M (2011) Operation BART: anonymous protests san Fran cell phone censorship. August 14, 2011, *Examiner.com*, http://www.examiner.com/anonymous-in-national/operation-bart-anonymous-protests-san-fran-cell-phone-censorship

Stone J (2014) Tamir Rice Shooting Inspires Anonymous Hack On Cleveland Websites. *International Business Times* 24 November. Available at http://www.ibtimes.com/tamir-rice-shooting-inspires-anonymous-hack-cleveland-websites-1728681

Tanczer L (2017) The terrorist – hacker/Hacktivist distinction: an investigation of self-identified hackers and Hacktivists, in *Terrorists' Use of the Internet*. Conway, M., Jarvis, L., Lehane, O., Macdonald, S. and Nouri, L. (Eds) Amsterdam: IOS Press,: 77-92

Taylor P (2004) Hackers and Cyberwars: rebels with a cause? Routledge, London

Taylor P, Harris J (2006) Hacktivism, in *Handbook of Information Security: Information Warfare; Social Issues, Legal and International Issues; and Security Foundations, Vol.2* edited by Bidgoli, H. New Jersey, NJ: Wiley: 172–182

Thomas D (2002) Hacker culture. University of Minnesota Press, Minneapolis

Thomson JJ (1975) The right to privacy. Philos Public Aff 4(4):295–314

Thomson JJ (1986) Rights, restitution and risk: essays in moral theory. Harvard University Press, Cambridge

Thomson JJ (1991) Self-Defence. Philos Public Aff 20(4):283–310

TOR (2015) Learning more about the GFW's active probing system. The TOR Project 14 September. Available at https://blog.torproject.org/category/tags/china

Traynor I (2007) Russia accused of unleashing Cyberwar to disable Estonia, May 17. *The Guardian*, http://www.guardian.co.uk/world/2007/may/17/topstories3.russia

Utterback J (2013) Cases of Hacktivism, *Hacktivism 101*, 28th May, Available at https://joymargret89.wordpress.com/2013/05/28/cases-of-hacktivism/

Vamosi R (2008) Anonymous Hackers Take on the Church of Scientology. *CNET* January 25 https://www.cnet.com/news/anonymous-hackers-take-on-the-church-of-scientology/

Wagenseil P (2011) Anonymous 'hacktivists' attack Egyptian websites. *Secur News Daily*, January 26, http://www.msnbc.msn.com/id/41280813/ns/technology_and_science-security/#.T3bs0r9SR7E

Walker P (2016) Gay men 'tortured and sodomised' by police in Uganda to 'prove they are gay. *The Independent* 3 November. Available at http://www.independent.co.uk/news/world/africa/uganda-gay-men-tortured-police-sodomised-beaten-a7395856.html

Walzer M (2000) Just and unjust wars: a moral argument with historical arguments. Basic Books, New York

Waqas (2012) Anonymous launch massive attacks on Department of Justice & other US government websites. Hack Read 20 January. *Available at* https://www.hackread.com/anonymous-launch-massive-attacks-on-department-of-justice-other-us-government-websites/

Wasserman D (1987) Justifying Self-Defense. Philos Public Aff 164(4):356–378

Westin A (1967) *Privacy and Freedom* London: Bodley head

Williams G (2003) Blame and responsibility. Ethical Thought and Moral Practice 6:427–445

Woodcock, B. 2011. 'Overview of the Egyptian internet shutdown' *Packet Clearing House* February. Available at https://privacywonk.net/download/Egypt-PCH-Overview.pdf