# Hacktivism - Controlling The Effects

MR Colesky
Nelson Mandela Metropolitan University
Port Elizabeth
South Africa
s209090185@live.nmmu.ac.za

J Van Niekerk
Nelson Mandela Metropolitan University
Port Elizabeth
South Africa
Johan.VanNiekerk@nmmu.ac.za

**In light of the recent peak in Hacktivist activity, Hacktivism has become a global issue in which many countries have invested to mitigate. While the traditionalist Hacktivists follow standards akin to typical activism, the new age Hacktivists execute daring and outlandish attacks to demonstrate their views. These various forms of Hacktivism are not only damaging to electronic infrastructure; they are also notoriously difficult to control. This paper examines the possible alleviation of Hacktivism effects through a trinity of control dimensions.**

**Keywords:** Hacking, Activism, Hacktivism, Control, Framework

## 1. Introduction

Towards the end of 2010 “WikiLeaks” released highly confidential U.S. State department diplomatic communications in redacted format to the world at large. This triggered major concerns regarding US national security and lead to widespread publicity regarding the phenomenon known as Hacktivism (Calabresi 2010).

Much controversy surrounds recent interest and enthusiasm for politically motivated cyber-attacks (Mezzofiore 2011). On the one hand, Hacktivist supporters believe Hacktivism plays a necessary role in the strive for transparent democracy in this digital age. However, on the other hand, government and corporate agencies as well as other proponents of confidentiality argue that Hacktivism is no more than glorified cybercrime (Pascucci 2012). Collective understanding around terms, ideals, and rationalisation for hacktivist activities, however, remains limited to mainstream propaganda.

Whether generalised Hacktivism aims to do “good”, or to simply cause chaos depends on many factors. Some Hacktivist collectives aim to generate extensive hype through displays of mischievous and malicious acts, whilst others actively

encourage legally sound demonstrations. In this sense, Hacktivists are much like traditional activists. These groups draw their own lines between legal and ethical boundaries, however not all ensure that what they do is in fact 'for the greater good'. As with traditional protests, and as with many public figures who have helped shape the world for the better, change requires action. Action is the tool in which organisations, governments and even the way society thinks may successfully be altered. The Internet is simply one more medium for taking such action.

As a medium, however, the Internet differs substantially from the more traditional forms of public protest. Originally governments could take measures to control activism through legislation. On the Internet, even though a government can pass laws which make online disclosure of state secrets illegal, it proves very difficult to enforce such a law.

This paper examines hacktivism and its potential underlying motives. The following sections will examine the roots of Hacktivism and will elaborate on the social, technical & legal control dimensions therein. Finally a framework to limit the negative effects of Hacktivism will be suggested.

## 2. Research Problem and Methodology

This research attempts to determine whether the effects of Hacktivism can be countered. The research aims to suggest a framework for the mitigation of the negative effects of Hacktivism.

The research is primarily based on an explorative literature review. The results of this review were used in support of both evidential and interpretative argumentation methods, as described by Mason (1996), toward the formulation of the suggested framework.

## 3. The Roots of Hacktivism

The first recorded instance of electronic activism predated the birth of the Internet; a politically motivated worm found its way into NASA systems, courtesy of Nahshon Even-Chaim and Richard Jones via a packet switched X.25 Wide Area Network (di Chiera 2003; The Sunday Age 2003). The attack, although only politically motivated through 'naïve idealism', was in response to the soon to launch Galileo Space Probe - which used plutonium as a power source. Thus began the first political protest over communication networks.

Internet Activism has become more prominent since. Online, anonymity still presents the tools needed to go too far and for no penalty. Collectively, online activists have the power to cripple corporations, whilst remaining anonymous – a power easily abused. Traditional protests aiming at the interruption of organisational activities may have comprised of sit-ins, hampering the productivity of their targets. However, those

partaking put themselves at risk. Law enforcement would make arrests, leaving activists punishable by the laws they broke.

Some Hacktivists do ensure their identities are no mystery, though most insist they remain anonymous. One could speculate that punishments are too severe to expect Hacktivists to step forward, though in contrast perhaps the means used to protest are themselves too severe. Some Hacktivists do not simply aim for the greater good. This separates an online activist from those who disagree with everything, those who believe they deserve everything and those who truly do it to further their own agendas. These various motivations negatively impact the way society sees Hacktivists, and warps the concept into its various negative connotations.

Are typical Hacktivists worth all the worry their hype presents, or are they simply the wake-up call needed to force organisations to secure themselves more adequately? Distributed Denial of Service attacks may be capable of taking a website offline, and website defacements certainly can leave organisations embarrassed, yet neither financially cripples their targets (Goldman 2011). It is when systems are hacked and data is stolen that significant damages occur. And when this is the case, personal information leading to identity theft or financial theft is possible. These are more often individuals motivated by money, rather than social or political opinion.

## 4. Background

Hacktivism stems from a combination of activism and hacking. And at first, “the hack” was only a hardware engineering achievement (Levy 2010). Hacking was a means to solving a problem; an at first ‘inelegant’, but innovative and out-of-the-box way of thinking (Alleyne 2011). As the hacker sub-culture developed around scholars, such as those at the Massachusetts Institute of Technology, the sense of inelegance fell away. These early hackers were instrumental in many of the achievements of that time. One such achievement was the development of ARPANet (Lunceford 2009).

‘Old-time’ hackers portrayed aspects which many current hackers still believe are integral. As identified by Turkle and Papert (1990), traditional hackers show qualities of ‘creativity, individuality, adaptability, and originality’. Lunceford (2009) continues that inquisitiveness, inner incentive and poor adherence to typical boundaries are also common attributes. It was not long after the conception of hacking before hackers were subjected to mass media attention.

Taylor and Jordan (1998; Jordan 2004; Taylor 1999 2005), identified two distinct understandings of hackers regarding social perception: cyber criminals and Hacktivists. The media did not hesitate to publicise the more negative of the two. Cast in the shadow of its darker side, Hacktivism remained restricted to Usenet newsgroups and other cut off mediums in the form of grassroots activism. As early as the nineties the public were only cognisant of hackers. Alleyne (2011) notes the increased anxiety that followed. The idea of ‘hackers’ became synonymous with all the connotations it now possesses.

The enigmatic Black Hat hackers were made representative of hacking. To contest this, the term ‘cracker’ (Garrett 2012) was defined by hackers to maintain distinction between those who seek to further their own goals, and those who seek to further mankind. Unfortunately this did not succeed. The contrasting White and Black Hat instead became popular; White Hats who legally serve under employment and Black Hats who hide, deceive and subvert. Black Hats are stereotyped as the ‘evil’ hackers, though as noted by Alleyne (2011), this serves more to contrast with the legislative openness of White Hats than to label Black Hats as bad intrinsically.

With hacking generalised as ‘*unconventional creation of a working solution*’, Hacktivism as a whole easily fits in the same kind of definition; ‘*innovative and effective unconventional social or political intervention*’. This is supported by Gunkel (2005) in his definition, Gibson (n.d.) in his thesis on Anonymous, and in Garret’s mention of the Hacktivism instance; The Transborder Immigrant Tool (TBT) (2012).

Hacking differs from Hacktivism in terms of its purpose, or context, lying closer to individualistic problem solving rather than an appeal to society. A hacker who works to expose a perceived social or political injustice hacks in the context of activism and can therefore be described as a Hacktivist.

## 5. Context

Hacktivism is not a clear cut field; there are various forms within Hacktivism which in their own right are a form of activism apart. Distinct differences can be seen in the levels of Hacktivism; from early grassroots, to Internet Activism, to Cyberwarfare. These numerous forms hold varying levels of intent, legality and ethics and will thus be briefly examined. The following four levels of Hacktivism has been selected from Stefan Wray’s (1998) Five Portals of ‘Extraparliamentarian Direct Action Net Politics’ based on their direct relation to Hacktivist ideals.

### 5.1. Computerized, Internet or Cyber Activism

The first level of Hacktivism, *Internet Activism*, began before the days of the World Wide Web. Making use of Newsgroups, Bulletin Boards and the like, electronic mediums were used to communicate passively about social or political issues. Strategies can be unconventional, and this form is still seen around social networking media. This form of Hacktivism may be used mostly for teambuilding and fundraising, though also is used for organisation of other forms of Hacktivism. Nevertheless, this is the most ‘White Hat’ form of Hacktivism.

### 5.2. Information Warfare

The second of these “portals” refers to active and aggressive publicity, inciting those affected to act. This concept, Information Warfare, is described by Wray as *‘Grassroots Infowar’*. This level takes a step further, pushing words towards action. This form builds camaraderie and strength in numbers to assert the confidence to

begin physical action. This relates closely to the release of usually restricted, secret or top secret information with intent to embarrass, enlighten, or to pose a visible threat to security and order. The Protection of State Information Bill, commonly referred to as the 'Secrecy Bill' is an attempt within South Africa to criminalise this release of restricted information. The Bill has received widespread criticism.

### 5.3. Electronic Civil Disobedience (ECD)

ECD entails obstructing social and political bodies, or representatives, from continuing activity in an active, but generally non-violent manner. ECD was first coined by Critical Art Ensemble in their book, The Electronic Disturbance (Wray 1998). Although Passive Civil Disobedience may be regarded ethically viable, it is not recognised as a lawful. ECD is regarded as less ethical, and it is often argued that it does not display the same dedication as its physical counterpart. Thus ECD is sometimes performed publically, where participants accept responsibility. However, important to note is that ECD is more difficult to control. It does generally cause valid public response, and as such is used often.

### 5.4. Politicized Hacking

The use of unauthorized access to convey a politically motivated message is known as *Politicized Hacking*. Politicized Hacking treads closer to 'cyberwarfare' in that it seeks to alter, disclose, disrupt or damage the target. Unquestionably illegal, those engaged in Politicized Hacking generally try to remain anonymous, unlike ECD activists who typically enjoy the spotlight. Wray (1998) also notes the use of cyber espionage and warfare, which employ politicized hacking. This can also include cyber terrorism. Though these terms are usually used more as a media hyperbole, as the world has yet to witness a true instance of cyber terrorism (Shackelford 2012).

Figure 1: Types of Hacktivism by repercussions based on Wray (1998)

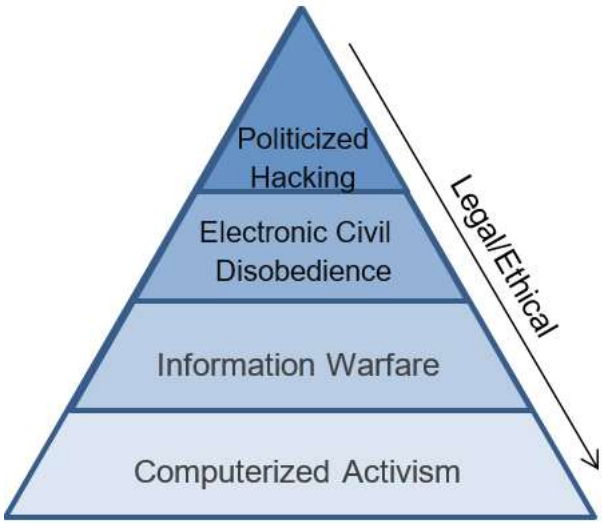


Figure 1 demonstrates the grading of Hacktivism severity, where Politicized Hacking encompasses instances of cyber terrorism, espionage and warfare. Examples of

possible cyberwarfare, terrorism and espionage have been suggested. The attacks on Estonia, Kyrgyzstan, Lithuania, Chechnya, and Georgia as well as various cyberattacks within China grey the lines between self-motivation and government supported attacks (Applegate 2011). Kaspersky has identified with these concepts in a recent Tel Aviv conference. To date there has been no effective global collaboration against Hacktivism (Gattegno 2012).

## 6. Perspectives

This section will examine arguments with regard to perspective angles as to whether Hacktivism can be reduced, whether it is worth the effort, why it is necessary, and how it can be done.

### 6.1. Socio-philosophical

#### 6.1.1. Necessity

Socio-philosophical is the first control dimension to be examined. This aspect is important in regard to Hacktivism because it encompasses both the impact of society on Hacktivism as well as the impact Hacktivism has on society. This factor influences whether Hacktivists are likely to choose any particular victim over another, or any at all. Hacktivism in a broad sense has social goals, or political goals met by social means. Without the social dimension, an important aspect to consider in Hacktivism control is overlooked.

#### 6.1.2. Issues

The aspects identified governing the typical hacker characteristics included individuality and camaraderie. In terms of society as a whole, these attributes impede on society's ability to affect Hacktivists by means of social rejection. This is because hackers have a contradicting tendency to have little need of social approval, yet band well together when their needs are compatible. This fact also allows those hackers who are an exception to either rule to find solace in the other. This means that even world-wide disfavour would have little or no effect on larger or even highly specific collectives.

#### 6.1.3. Solution

What does have effect is society's perception of external entities. When social or political flaws are perceived, a social responsibility is inferred. A fundamental motivator for Hacktivists is self-righteous or virtuous prosocial behaviour. Prosocial behaviour defines how people, in this context believe it is their duty to act according to what they personally or collectively believe is right for society (Thomson & van Niekerk 2012).

Another aspect fundamental to target selection is prospective hype. A driving force for certain Hacktivism collectives, for example Anonymous, exists in how much publicity they can generate. As with traditional activists, Hacktivists further their cause more effectively when broadcast to a greater audience. This is because a larger audience offers more would-be recruits for the cause as well as an increase in awareness, which plays a major role in swaying the public to believe as they do.

In light of this, as far as society is concerned, the reduction of hype and incentive for prospective attacks is the surest makeshift solution to the problem. This holds true because reduced motivation results in less action. Furthermore, a lack of prospective hype presents little reward for any one attack. Achieving these goals requires effort from those who would otherwise become victims.

### 6.1.4. Implementation

In order to reduce prospective hype a common tactic is used. Downplay and dismissal are well practised by victims of Hacktivism (Sterner 2012; Leyden 2012; Yin 2012; Van Dervoort 2012). This tactic works well where implemented properly. It can, however, also backfire. These tools are often regarded as denial or attempts to cloak embarrassment. This is counter-productive, as it merely furthers Hacktivist agendas when corporations are transparent in their attempts to save face.

Secondly there is the prospect of lowered incentive. In order to achieve a lowered motivation several courses of action may be considered. For one, an entity could take measures to be impenetrable – a solution which would surely deter less determined individuals. However, as this paper will indicate in the next section, this is not a fool proof solution, nor is it necessarily worth the costs involved.

On the other hand, the entity could abstain from any and every questionable activity, or appear to do so. While effective for remaining ‘under the radar’, this tactic may present unrealistic competitive difficulty and some Hacktivist demands may be too overreaching. It bodes well to abide by the law, but when the law is defined by uncompromising collective opinion, this effort may also be unworthy of its costs.

An additional tactic lies in positive publicity, aimed at making the entity an undesirable target. This can be achieved with openness, public approval, good appearance and attitude. Because Hacktivists are reactive in nature (Levinson 2011; Menn 2011), any negative provocation or response is retaliated against. A positive attitude lessens motivation for a cyberattack. Combined with downplays, which are a negative outlook on an activity, positive nature allows a company to maintain its integrity while deterring future attacks.

The above is not necessarily trivial to uphold. A simplistic goal for the lessening of Hacktivism effects would be to create a society where Hacktivism is not necessary. Society should not want or need to become Hacktivists. Instead, individuals should be heard, should listen, and be open-minded. But this is not always human nature.

## 6.2. Technical

### 6.2.1. Necessity

The technical control dimension is next examined. Technical controls govern security, and security is a fundamental deciding factor in whether an act of Hacktivism directly affects any prospective victim. This factor influences the likelihood of an attack being successful, and as such holds vast importance in effect prevention.

### 6.2.2. Concerns

The most central flaw regarding technical security is the concept of human error. This holds true in two regards; first, that of software 'bugs'. Bugs are errors in code which present technical vulnerabilities for exploitation by malicious hackers and their tools.

The Ethical Hacker's Handbook (Harris, Harper, Eagle, & Ness 2008) stipulates that per every thousand lines of code (LOC) anywhere between five and fifty software faults may exist. Entire operating systems easily number in the tens of millions of LOC, and beyond this, software which builds on to these systems presents further defect opportunities. Any weakness in any one of these avenues presents a potentially devastating vulnerability, especially where these applications intercommunicate. On any given day, as many as sixty thousand new instances of malware are introduced (Ryan 2012). No amount of dedication or care can account for every modification and attachment to a system unless all of it is marshalled carefully, and even then only so many possibilities can be accounted for.

Also specified in Harris et al (2008) was the aspect of cost-cutting, which often sees businesses avoiding the necessary level of security to protect from intrusion. Another aspect includes potentially poor threat management. Some companies who identify vulnerabilities later than acceptable would rather keep this information from their customers for fear of their image, and only repair it much later. In this time however, a multitude of customers could be subjected to the threat that stems from that vulnerability. Harris mentions one such example where Michael Lynn publicised an unresolved weakness in Cisco IOS; Rather than simply fixing the error, Cisco threatened to take legal action.

The second aspect pertaining to human error is Social Engineering. This describes the art of manipulation to obtain unauthorised access through the exploitation of human vulnerabilities (Bezuidenhout, Mouton, & Venter 2010). While an entity may invest in impenetrable technical security, the human side can and often does present heavy weakness for manipulation. Even the smartest individuals can be misled by a well-planned con. Parnell (2012) describes one such instance via iCloud where an individual was able to gain access to and wipe data from all of a victim's Apple devices as well as gain access to the victim's Twitter account.

### 6.2.3. Resolution

A recent report by Bit9 (2012) indicates that 61% of IT Professionals fear their companies will soon be subjected to cyberattack. Only 18%, however, believe technical defences are inadequate. Instead, most professionals agree that best practises and policies are where corporations fall short. By this extent, it is fair to acknowledge that technical security itself is already being implemented adequately. Further technical security advances take place regularly, though advances in malicious software are also apparent. To compete in this would only solve one aspect of the problem, and would require a vast pool of resources.

Short comings regarding best practise and policy implementation, however, should be addressed. By enhancing best practises and awareness, a company is better equipped to promptly address identified weaknesses as well as attacks of Social Engineering. As stated recently by Symantec's Francis deSouza, “It's not a question of if or when companies will face an attack, but how they're going to defend against it,” (Field 2012). It is up to the organisation to ensure the policies and procedures are in place in order to best handle the attacks of Hacktivism and to minimise the damage.

## 6.3. Legislative

### 6.3.1. Necessity

The legal perspective is the third and final of the control trinity. The importance of a legislative angle is based off the same principles used to control any crime. Cyberattacks are one such crime and as such, the enforcement against them is critical. On the other hand, as reported by Bit9 in their 2012 surveys, only 9% of security professionals believe that law alone has what it takes to control cyberattacks.

### 6.3.2. Applicability

Sommer (2000) argues that cyberlaw is not a valid division of law in itself. Rather, general law adequately provides for the injustices committed electronically and any attempt to create specific law is detrimental to the effectiveness of its enforcement. However, Applegate (2011) reasons that without specific law to account for cybercrime, adequately classifying and attesting defendants will be hampered by the anonymous nature of the Internet. This is also affected by the vague applicability of human rights to privacy.

This new law would arguably impede on society’s right to privacy or to access of information. Several laws along this line have been suggested, however, each has received international negative response. One in particular focused on criminalising access and disclosure of confidential, secret or top secret government information.

South Africa's Protection of State Information Bill has recently received a softened stance from the current ruling party (Pana 2012).

Applegate continues to note that litigation against cybercrime is especially difficult when considering the prospect of cybermilitias, where cyberattacks are secretly sponsored by entire governments.

### 6.3.3. Issues

The prospect of cyberwarfare has further increased the attention awarded by the FBI to cyberattacks. As mentioned in the article by Cilley (2012), the FBI is likely to put cyberattacks above terrorism as their top priority.

The issue most prominent in legal applications is the inherent lack of control which comes with anything relating to the Internet, and with it, anonymity. Because of this, laws made to handle acts of Hacktivism are in most cases too difficult to fairly enforce. When handled disproportionately, such as in minority arrests, the remainder simply detach themselves and continue their actions. This can be seen in the denouncement of LulSec's arrested members (Schwartz 2012) and the retaliation that followed (Suciu 2012).

Without working controls law may discourage, but will not necessarily prevent. The typical dedication most activists have for their cause may provide insight as to whether a Hacktivist might also believe penalties are worth the risk. This proposition presents further issues as making examples of specific participants may not be so effective.

The vast participant count and spread of potential suspects also marks investigation as well as prosecution expensive. Attesting transgressions, especially in regard to international crimes is by no means trivial. Questions regarding jurisdiction also present obstacles for enforcers to overcome. As Hacktivists may take part in cyberattacks from various simultaneous locations throughout the world, taking measures to control them requires a similar effort by all legal bodies concerned. As mentioned previously, no such collaboration has been successful (Gattegno 2012).

Finally, Hacktivists vary in levels of skill. This skill ranges from the likes of 'script kiddies' to fully fledged political hackers. Because of this authorities cannot work off a generalised profile. More instrumental members are likely to be difficult to snare. These more senior members specialise in breaching security, making them well versed in carefulness as well as discretion. These are the individuals who are most threatening. To successfully control them will require even greater resources. Furthermore, preventing one Hacktivist does not necessarily stop another from taking his/her place.

## 7. Framework

This section will present and describe the resulting framework identified by this paper. The alleviation of Hacktivism effects has been explored through a trinity of socio-philosophical, technical and legislative means. This has been set out in a manner intended to be easily understood, modelled via a three dimensional control trinity.

Figure 2: Control Trinity & their best defences against Hacktivism


The trinity may be presented as depicted in Figure 2. As identified throughout the previous sections, each dimension is represented within the light blue triangle. Along with these, the control best suited according to this study to defend against the effects of Hacktivism surrounds the dimensions with an outer blue wall.

**Euphemism** represents the lessening of attention and importance, seeking an optimistic impression for both the potential victim and acts of Hacktivism in general.

**Cooperation** is the most effective tool at law enforcement's disposal. This includes international - as well as local - cooperation between Internet Service Providers, security firms, law enforcement, and corporations.

Finally the best tool for ensuring effective technical security is correctly implemented **Best Practise**. This includes continual improvement of policies to better protect against threats. These are also presented as a means to best reduce the effects of social engineering on technical security.

In order to maximise the reduction of Hacktivism effectiveness, it is essential that each dimension tightens its defences and that a balance be achieved. Any weakness in this trinity will likely be exploited, allowing Hacktivism to thrive further.

## 8. Conclusion

The effects of Hacktivism **can** be alleviated, and in some cases prevented. Hacktivism itself, however, **cannot**. This means that society must learn to cope with electronic disruption the same way it copes with traditional activism. The information

age is a step forward, an ‘evolution’ of mankind, and Hacktivism is the electronic evolution of activism. It has the same fundamental goals in most cases, though there will be those who take part purely for attention or self-gain.

Hacktivism cannot be stopped any more than activism can. So long as people are free to express their opinions, they will continue to ensure that they are heard. At best, as this paper has demonstrated, society at large can reduce the impact of Hacktivism. This would however require a triangulated approach. For Hacktivism, there is no *silver bullet*.

## 9. References


Alleyne, B., 2011. We are all hackers: Critical sociological reflections on hacking.

Applegate, S.D., 2011. Cybermilitias and Political Hackers - Use of Irregular Forces in Cyberwarfare. *IEEE*, (October).

Bezuidenhout, M., Mouton, F. & Venter, H.S., 2010. Social engineering attack detection model: SEADM. *2010 Information Security for South Africa*, pp.1–8.

Bit9, 2012. *US And European Research: 2012 Bit9 Cyber Security Survey Results*, Available at: https://www.bit9.com/cyber-security-research-2012/.

Calabresi, M., 2010. WikiLeaks’ War on Secrecy: Truth's Consequences. *TIME Magazine*. Available at: http://www.time.com/time/magazine/article/0,9171,2034488,00.html [Accessed September 6, 2012].

di Chiera, F., 2003. *The Realm of the Hackers*, Film Australia.

Cilley, J., 2012. FBI Says Cyberthreats to Overtake Terrorism as Top Threat. *Bit9*. Available at: https://www.bit9.com/blog/2012/02/01/fbi-says-cyberthreats-to-overtake-terrorism-as-top-threat/ [Accessed June 16, 2012].

Van Dervoort, O., 2012. Yahoo Security Breach Compromises 450,000 Accounts: Yours Could Be Next. *policymic*. Available at: http://www.policymic.com/articles/11278/yahoo-security-breach-compromises-450-000-accounts-yours-could-be-next [Accessed August 7, 2012].

Field, T., 2012. Cyber Attacks: Not If or When, But Now. *BankInfoSecurity*. Available at: http://www.bankinfosecurity.com/interviews/cyber-attacks-if-or-when-but-now-i-1409 [Accessed August 10, 2012].

Garrett, M., 2012. Revisiting the Curious World of Art & Hacktivism. , (March).

Gattegno, I., 2012. “Cyberterrorism could mark the end of the world as we know it.” *Reuters*. Available at: http://www.israelhayom.com/site/newsletter_article.php?id=4594 [Accessed August 24, 2012].

Gibson, N., *Hacktivism and Performance: Creative acts of intervention in online spaces; "The hack" as a political, social and artistic tool in the work of Anonymous, Stelarc and ZeFrank*.

Goldman, D., 2011. LulzSec and Anonymous are the least of your hacker worries. Available at: http://money.cnn.com/2011/07/25/technology/lulzsec_anonymous_hackers/ [Accessed April 3, 2012].

Gunkel, D.J., 2005. Editorial: introduction to hacking and hacktivism. *New Media & Society*, 7(5), pp.595–597.

Harris, S. et al., 2008. *Gray Hat Hacking : The Ethical Hacker's Handbook, Second Edition*, McGraw-Hill.

Jordan, T. & Taylor, P, 1998. A sociology of hackers. *The Sociological Review*.

Jordan, T. & Taylor, PA, 2004. Hacktivism and cyberwars: rebels with a cause? Available at: http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:Hacktivism+and+Cyberwars:+Rebels+with+a+Cause?#0 [Accessed September 12, 2012].

Levinson, M., 2011. FBI Warns Hacktivists: You're Breaking the Law CIO.com. *cio.com*. Available at: http://www.cio.com/article/696793/FBI_Warns_Hacktivists_You_re_Breaking_the_Law_ [Accessed May 14, 2012].

Leyden, J., 2012. Anonymous Hacktivists Dump 1.7GB Load Slurped From DoJ Site. *theregister*. Available at: http://www.theregister.co.uk/2012/05/22/anon_crime_stats_site_hack/ [Accessed August 7, 2012].

Lunceford, B., 2009. Building Hacker Collective Identity One Text Phile at a Time: Reading Phrack. *Media History Monographs*, 2. Available at: http://facstaff.elon.edu/dcopeland/mhm/mhmjour11-2.pdf [Accessed September 12, 2012].

Mason, J., 1996. Qualitative researching. *SAGE Publications*.

Menn, J., 2011. "Hacktivists" retaliate against security expert. *ft.com*. Available at: http://www.ft.com/cms/s/0/0c9ff214-32e3-11e0-9a61-00144feabdc0.html#axzz232s3zcsu [Accessed August 9, 2012].

Mezzofiore, G., 2011. Anonymous Controversies: The Hacktivist Collective Goes Global. *IBTimes UK*. Available at: http://www.ibtimes.co.uk/articles/263913/20111208/anonymous-controversies-hacktivist-collective-goes-global.htm [Accessed September 6, 2012].

Pana, 2012. South Africa: ANC softens stance over Secrecy Bill. *afriquejet*. Available at: http://www.afriquejet.com/south-africa-anc-softens-stance-over-secrecy-bill-2012083043862.html [Accessed September 7, 2012].

Parnell, B.-A., 2012. Scribe's mobe, MacBook pwned after hacker "fast-talked Apple support." *reghardware.com*. Available at: http://www.reghardware.com/2012/08/06/icloud_hack_racist_tweets_idevice_wipe/ [Accessed August 9, 2012].

Pascucci, M., 2012. Hacktivism Debate: Security's Little Awareness Helper. *Infosecurity Magazine*. Available at: http://www.infosecurity-magazine.com/view/26605/hacktivism-debate-securitys-little-awareness-helper-/ [Accessed September 6, 2012].

Ryan, J., 2012. FBI Director Says Cyberthreat Will Surpass Threat From Terrorists - ABC News. *abcnews.go.com*. Available at: http://abcnews.go.com/blogs/politics/2012/01/fbi-director-says-cyberthreat-will-surpass-threat-from-terrorists/ [Accessed June 16, 2012].

Schwartz, M.J., 2012. Hacking Group LulzSec Denies Arrest Report. *Informationweek*. Available at: http://www.informationweek.com/security/attacks/hacking-group-lulzsec-denies-arrest-repo/230300007 [Accessed September 8, 2012].

Shackelford, S., 2012. In Search of Cyber Peace: A Response to the Cybersecurity Act of 2012. *Stanford Law Review Online*, 64, p.106.

Sommer, J., 2000. Against cyberlaw. *Berk. Tech. LJ*. Available at: http://heinonlinebackup.com/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/berktech15&section=48 [Accessed June 8, 2012].

Sterner, E., 2012. The Paradox of Cyber Protest. (April).

Suciu, P., 2012. It's Business As Usual For Anonymous As Panda Takes A Hit. *technewsworld.com*. Available at: http://www.technewsworld.com/story/74586.html [Accessed April 2, 2012].

Taylor, PA, 2005. From hackers to hacktivists: speed bumps on the global superhighway? *New Media & Society*. Available at: http://nms.sagepub.com/content/7/5/625.short [Accessed September 12, 2012].

Taylor, PA, 1999. Hackers: crime in the digital sublime. *Psychology Press*.

Thomson, K. & Van Niekerk, J., 2012. Combating information security apathy by encouraging prosocial organisational behaviour. *Information Management & Computer Security*, 20(1), pp.39–46.

Wray, S., 1998. Electronic civil disobedience and the World Wide Web of hacktivism. *Nova*. Available at: http://switch.sjsu.edu/web/v4n2/stefan/index.html [Accessed May 11, 2012].

Yin, S., 2012. HACKTIVISM 55,000 TWITTER ACCOUNTS BLOWN. *occupythebanks*. Available at: http://www.occupythebanks.com/2012/05/hacktivism-55000-twitter-accounts-blown.html [Accessed August 7, 2012].