Chapter 11
Groups Online: Hacktivism and Social Protest

Helen Thackray
Bournemouth University, UK

John McAlaney
Bournemouth University, UK

ABSTRACT
This chapter provides a brief introduction to hacktivism and social protest online and highlights some of the socio-psychological and cognitive factors that can lead to individuals taking part in hacktivism groups. Hacktivism is an ill-defined area which some claim as a legitimate form of protest in the online world and others regard as illegal hacking; there is truth to both arguments, and those who believe it should be protected will continue to work for it to be recognised. The chapter explains how the depth of social ties and influence are still being examined, and whilst cognitive biases are recognised, strategies to mitigate and combat the vulnerability they present are still being developed.

INTRODUCTION
The internet is a significant aspect of global social change, and has greatly altered the nature of collective action and social movements (Jensen, 2015, Postmes & Brusting, 2002). Hacktivism, a term combining ‘hacking’ and ‘activism’, is the use of various computer hacking tactics for political, social, and ideological motivations; hacktivists use nonviolent but often illegal digital tools to achieve these goals (Hampson, 2012, Krapp, 2005, Solomon, 2017). The common methods of hacktivism include defacing websites, using DDoS attacks, and other types of internet disruption (see Table 2, Hanna et al, 2016). The use of these tactics has led to challenges in distinguishing between hacktivism and hacking, as it can be that only the individuals’ motivation is different. This chapter will discuss the current understanding and context surrounding hacktivism, before examining the cognitive and social psychological factors that can influence those involved in hacktivism and online social protest.

BACKGROUND

It is important to remember that cybersecurity incidents occur within a social context; even if it is not face to face, online interactions fulfil and rely on the same social or task needs as offline interaction with others (McKenna & Green, 2002). There remains, however, a lack of insight into the influence of psychological factors and social norms online, especially in the case of hacktivism. All actors within cybersecurity incidents interact with each other and within each group. Whilst hacktivism is regarded as a contested area, stuck between definitions of justified civil action and illegal hacking, there remains a strong need to challenge the stereotypes around it. The conflation of the terms “hacker” and “hacktivist”, with “cybercriminal” and “cyberterrorist” adds to the confusion surrounding the different typologies identified (see Table 1). A divisive and complex issue, there are many governments and businesses see hacktivism as a threat, akin to cyber-terrorism and cybercrime (Drucker & Gumpert, 2000, Kubitschko, 2015, Manion & Goodrum, 2000, Shaw, 2006); others argue that social protest and change have always been a part of society (Scheuerman, 2016, Schrock, 2016), and that hacktivism is the progression of social protest (Kubitschko, 2015, Postill, 2014, Solomon, 2017).

Hacktivism is not a 21st century addition to the internet. The origins lie in computer based activism as early as the mid-1980s (Wray, 1998). One of the first known instances of a DDoS attack occurred in 1995, when a group of Italian artists blocked websites of the French government, in protest of the decision to undertake a series of nuclear tests (Milan & Atton, 2015). Hacktivism was not, however, a well-known phenomenon until the mid to late 2000s. One of the more predominant groups, Anonymous, began to use media attention as part of their strategy; previously activist groups had preferred to remain undetected in order to protect their projects from law enforcement (Milan & Atton, 2015). As such Anonymous is probably the most widely known hacktivist group by the general population.

Since the mid-1990s the continued rise of hacktivism has surprised and worried many; but its’ growth in popularity can be attributed to several reasons. The ease of contributing from one’s home or place of choice means that distance is no longer an issue in supporting a cause, even if it is quite literally the other side of the world. Hacktivism also comes with a lower level of risk when compared to physical public demonstrations, whilst still allowing their messages and protests to be seen by the public across the internet – although this is not to say that it is risk free as some once perceived it to be (see cognitive

<table>
<thead>
<tr>
<th>(Computer) Hacker</th>
<th>One with the ability to access a computer or system without admission (Raymond, 1996).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hacktivism</td>
<td>A method to express dissatisfaction with elements of political and social reality using online resources (Milan &amp; Atton, 2015).</td>
</tr>
<tr>
<td>Slacktivism</td>
<td>Critical term for low-profile online activism, such as signing petitions and using online badges (Hanna et al, 2016).</td>
</tr>
<tr>
<td>Whistle-blowing</td>
<td>The leaking of confidential information to the public as a form of raising awareness about a contentious issue (Hanna et al, 2016).</td>
</tr>
<tr>
<td>Cyberterrorist</td>
<td>One who uses computer/network technology to terrorise opponents to further political or social objectives (Rogers, 2003).</td>
</tr>
<tr>
<td>Cyber delinquent</td>
<td>One who engages in illegal behaviours, such as verbal violence, hacking, and illegal copying of software in online environments (Hong &amp; Kim, 2011).</td>
</tr>
</tbody>
</table>
Related Content

An Internet-Mediated Pathway for Online Radicalisation: RECRO
[www.igi-global.com/chapter/an-internet-mediated-pathway-for-online-radicalisation/213299?camid=4v1a](www.igi-global.com/chapter/an-internet-mediated-pathway-for-online-radicalisation/213299?camid=4v1a)

Preparing for Cyber Threats with Information Security Policies
[www.igi-global.com/article/preparing-for-cyber-threats-with-information-security-policies/105189?camid=4v1a](www.igi-global.com/article/preparing-for-cyber-threats-with-information-security-policies/105189?camid=4v1a)

Realized Applications of Positioning Technologies in Defense Intelligence
[www.igi-global.com/chapter/realized-applications-positioning-technologies-defense/5150?camid=4v1a](www.igi-global.com/chapter/realized-applications-positioning-technologies-defense/5150?camid=4v1a)

Punching Above Their Digital Weight: Why Iran is Developing Cyberwarfare Capabilities Far Beyond Expectations
[www.igi-global.com/article/punching-above-their-digital-weight/204418?camid=4v1a](www.igi-global.com/article/punching-above-their-digital-weight/204418?camid=4v1a)