The Heartbleed bug : insecurity repackaged, rebranded and resold

BANKS, James <http://orcid.org/0000-0002-1899-9057>

The Heartbleed bug: Insecurity repackaged, rebranded and resold

Introduction

On 7 April 2014, much of the world's media reported on a security vulnerability said to effect in the region of half a million of the Internet's secure web servers certified by trusted authorities (Woodward, 2014). Identified almost simultaneously by both Google Security and a Finnish cybersecurity company, Codenomicon, the vulnerability, dubbed the 'Heartbleed bug', has the potential to expose the personal and financial data held by a wide range of online operators. Exploiting vulnerable versions of OpenSSL[1]software, the Heartbleed bug enables individuals to read the memory content of systems by compromising the 'secret keys' which are employed in the identification of service providers, the encryption of traffic, usernames and passwords, and the content of messages (Codenomicon, 2014). This vulnerability provides significant opportunity for individuals to decipher communications, steal information and impersonate services and their users.

Whilst patching the vulnerability is a fairly simple task for system administrators, the sheer volume of organisations and services affected means that executing such change is likely to be both time consuming and costly. Incorporated into the June 2012 release of OpenSSL, the bug remained undiscovered for nearly two years, although there is little evidence to suggest that it had been maliciously exploited. Vulnerabilities such as Heartbleed are nothing new, having occurred since the early 1970s when programming language C, in which OpenSSL is written, was first introduced (Merkel, 2014). Most cyber security experts are in agreement that the periodic occurrence of network anomalies and vulnerabilities represent a long term technological trend, as digital communication services continue to shape both the economy and wider society (Deverell, 2014; Ralph, 2014). Yet despite the

regularity with which such threats are discovered, the first major news release on April 7 united the Heartbleed bug with an all too familiar apocalyptic message: 'We are doomed' (Buchanan, 2014).

This paper examines the social construction of the Heartbleed bug across various news media, demonstrating how neoliberal discourses of cybercrime control are packaged, branded and sold. By way of introduction, the paper considers the arrival of a post-industrial information economy shaped by and around networked communication technology. It details how the increased use of digital communications and networked database resources present opportunities for the misappropriation of electronic information. The global media have reported on a series of data breaches throughout the twenty-first century, instilling in the public consciousness an anxiety regarding the vulnerability of information systems and the security of online environments. This has provided fertile ground upon which the crime control industry can market computer and information security to both businesses and consumer citizens alike.

Discussion then turns to explore the ways in which the computer crime control industry utilise the media to sell insecurity through an examination of the Heartbleed bug. In such imagery, the dystopic potential of the Internet is fused with pre-crime prudentialism to responsibilise the consumer citizen for their online safety. It is argued that the maintenance of insecurity and fear, through the 'reinvention' of cyber-threats, is vital to the profitability of private security firms. Analysis demonstrates how the crime control industry and news media contribute to maintaining a 'reassurance gap' (Innes 2004) that emerges between the public's perceived vulnerability and the state's ability to protect the public, whilst simultaneously positioning private security services as being able to offer consumer citizens antidotes for such ills.

The information economy, data vulnerability and public fear

The emergence of a post-industrial information economy has necessitated a new order in which economic productivity is shaped by the generation, utilisation and consumption of information (Yar, 2008). Castells (1996: 7) charts the rise of 'informational capitalism' wherein economic growth is determined by the 'qualitative capacity to optimize the combination and use of factors of production on the basis of knowledge and information.' The spread of communication networks across the globe have enabled businesses to adopt devolved, decentralised and flexible management structures that are dependent upon information to maximise profits (Castells, 2001). As such, core economic activities are shaped by and around information and communication technologies, most conspicuously the Internet, which underpins a wide array of business endeavours, from the production and marketization of goods and services through to their distribution and consumption (Ibid.). Financial services have adopted a similar modality, with the computerisation of the banking industry and the virtualisation of money transforming capital markets, as well as consumer practices (Miller, 2010). For many, online banking and shopping have become routine daily activities, with networked information technologies an integral, if unremarkable, aspect of a large number of individuals' social and working lives.

Under these conditions, personal information is an extremely valuable commodity, with digital communications and networked database resources providing the principal means through which such information is stored, shared and sold. Both the state and a host of private agencies generate, collect and collate significant amounts of information regarding citizens' life history, financial status and personal preferences, utilising such data to various ends (Finch, 2002). Haggerty and Ericson (2000: 609) explore the dynamic of this emerging

'surveillant assemblage', which exists at the intersections of various media, energising and serving state and non-state 'desires for control, governance, security, profit and entertainment.' This intensification or 'creeping' of technologized surveillance systems is a late modern force that transforms an ever greater number of human bodies into 'pure information' (Ibid. 613). Through a multiplicity of nodes, distributed across an array of technologies and social practices, human bodies are abstracted into discrete 'flows' of information which are then reassembled as 'data doubles' (Ibid.). Such doubles are scrutinized and exercised by government and corporate agents, in order to achieve a range of different objectives.

In electronic commerce, the Internet's interactivity acts as a powerful consumer information gathering tool, enabling online retailers to collect data when individuals browse their site or purchase their goods or services. This, in turn, permits commercial businesses to build consumer profiles, track online behaviour and monitor feedback, in order to develop appropriate branding and niche marketing strategies and, ultimately, maximise their sales return. Social networking sites, such as Bebo, Facebook and MySpace, also hold vast swathes of users' autobiographical information[2], whilst the widespread availability of electronic banking systems means that citizens' credit card and bank account details are held by an assortment of different organisations. Moreover, some companies specialise in collecting valuable personal information which is then sold on to other commercial operations for considerable profit.

Today, networked technologies are used to collect, store and transact voluminous amounts of data. The democratisation of digital technology and dependence upon its ability to warehouse and disseminate information presents 'unprecedented opportunities for crimes of acquisition' (Grabosky, Smith and Dempsey, 2001: 1). Moreover, a contradiction lies at the heart of efforts to protect personal data, as techniques of identification require individuals to

submit vast amounts of personal information when registering in order to engage in 'secure transactions' with commercial organisations and state agencies (Smith 2010: 276). For Monahan (2009: 156), identity theft 'thrives' in the structural conditions caused by post-industrialisation, as personal data is stockpiled and traded and regulatory 'red tape' governing its protection is rescinded. This sees the threat posed to individuals' personal information being lost or stolen exacerbated by rudimentary encryption and liberal data management processes (O'Harrow, 2005). Thus, as Wall (2008a: 49) recognises: 'The main concerns about infrastructure are not so much the [online] environment itself, but the management of the large amounts of critical information within it, especially when concentrated within one source such as a database.' As such, the accidental leakage or deliberate harvesting of information, via either hacking or social engineering, present real threats to a wide range of individuals, businesses and online operators, with opportunities for computer criminals to misappropriate electronic information for nefarious activities emerging right across the online landscape.

Identity certainly appears to have become 'the new money' (Crosby, 2008: 3), as the online marketplace for hacking tools, personal information, credit card numbers, bank accounts, pin numbers and passwords continues to grow (Thomas and Martin, 2006; Holt and Lampke, 2010; Motoyama et al., 2010; Holt, 2012). This is unsurprising given the profitability of online identity theft, which is estimated to have an annual value globally of in the region of US$1billion and affect approximately 1.5 million people (UNODC, 2010). The theft of individuals' identity is certainly easier than ever before, given that significant volumes of personal information are stored on and transferred via computer networks. As Finch (2007) highlights, the collection of an individual's personal information is no longer an arduous process which may take weeks or months and involve sifting through a victim's rubbish or other repositories of data in order to accumulate the documentation necessary to

steal their identity. Instead, the advent of virtual communications has placed such vital information but a 'few keystrokes away' (Ibid. 38).

Numerous data breaches have occurred throughout the twenty-first century, with a wide range of state and commercial organisations unintentionally disclosing information, losing data or having it stolen from their computer systems. In October 2013, Adobe Systems confirmed that a 'sophisticated' cyber-attack had resulted in 2.9 million of its customers having their private information stolen, including encrypted customer passwords and payment card numbers (BBC News, 2013). Similarly, in what could well be the largest credit and bank card breach of all time, American retailing company Target Corporation reported the theft of personal and/ or payment data of between 70 and 110 million customers from November to mid-December 2013 (Harris and Perlroth, 2014). Within the UK, various central and local government departments and agencies, as well as private sector contractors have been implicated in a host of different cases of data loss and data theft. Most significantly, in 2007, HM Revenue and Customs lost a data disc containing financial details of 25 million recipients of child benefit (BBC News, 2007). Data breaches have also been recorded by the Ministry of Defence, the Ministry of Justice, the Serious Fraud Office, the National Offender Management Service, NHS trusts and local county councils, amongst others, demonstrating the sheer breadth of agencies affected by the difficulties posed by the management of sociotechnical forms of data.

Such events have formed the basis of media reportage that routinely raises questions regarding the security of digital data and online environments and the safety of citizens' personal and financial information. As part of a wider print and broadcast media discourse that constructs cybercrime as 'immensely prevalent and threatening', such imagery heightens public insecurities about the safety of personal data (Wall, 2008a: 46). This imagery is melded with broader cultural representations of cybercrime and cybercriminals that reinforce

a ‘culture of fear’ (Furedi, 2002) concerning the threat posed by virtual environments (Wall, 2008b, 2012). With concern outpacing reliable information, anxiety and vulnerability regarding online crime and victimisation characterise the public psyche and underpin calls for effective action from the state to protect citizens, apprehend and prosecute virtual villains, and limit associated harms. For Wall (2012, 2013), a 'reassurance gap' (Innes, 2004) has emerged between the public’s expectations and the police and government's ability to provide safety and security online. In part the product of the inflation and amplification of cyber fears, this disparity offers great opportunity for private purveyors of crime control.

Computer crime control as industry

Privatised forms of crime control are prevalent throughout the western world. The privatization and commercialisation of criminal justice practice that began in the US and Britain in the mid-1980s, increasingly sees the provision of security left to market forces (Garland, 2001). Private policing or para policing is now a common site across leisure, entertainment and retail facilities, business centres and transport terminals (Aas, 2007), whilst private prisons, correctional facilities and immigration detention centres have become established components of the penal apparatus of a number of industrialised countries, including the US, UK, Australia and South Africa (Ericson, McMahon and Evans, 1987; Christie, 2000; Stern, 2006). Commercial outfits also market a range of security services and products directly to citizens, from car steering locks and gated communities to closed circuit television cameras and private patrols. More recently, Yar (2008: 190) has documented the emergence of an ‘extended market-led sector that sells security against the threats and predations that are seen to pervade contemporary cyber-worlds’. Invariably, computer crime control products are focused upon ensuring that computer systems remain operational,

preventing unauthorised intrusion and the theft, alteration or destruction of data. This industry is highly lucrative, with the global spend on cyber security in 2011 estimated to be in the region of US$60 billion and forecast to grow by ten per cent per annum over the next three to five years (PwC, 2011).

In conjunction with the corporatisation and commodification of crime control, citizens have been responsibilised with their own personal safety, risk avoidance and crime prevention in a variety of spheres of their life, including their online activities (Whitson and Haggerty, 2008). As O'Malley (1992, 1996) has recognised, this 'new prudentialism' instructs citizens to safeguard themselves and their families against the numerous risks and insecurities of everyday life. This has, in turn, buttressed a consumerist orientation toward cyber security by providing an ever expanding computer crime control industry with a receptive marketplace of (anxiety ridden) consumer citizens looking to guard against criminal victimisation.

Monahan (2009: 160) identifies 'three dominant modes of consumption' that shape the neoliberal regime of governance and are highly applicable to the field of cybercrime control. First, consumer citizens can purchase an array of computer crime control products and services through which to protect themselves and their identities. Software designed to counteract hacking or unauthorised entry, anti-virus programs that detect and remove malicious software, and authentication and access tools are part of a much wider assemblage of safeguarding systems and services available for consumption. Second, consumer-protection information is sought by citizens looking to prevent online victimisation. Thus, citizens not only purchase crime control products and services but they also alter their behaviour by pursuing and consuming the requisite information required to adequately protect themselves and their families from becoming victims of online crimes. 'In this way, these two modes of consumption both overlap and reinforce one another.' (Ibid. 161). Third,

individuals consume fear. For Monaghan (2009: 161), fear is a 'critical component' that 'is not simply transmitted from the media to the public. Instead, it involves the collaborative cultivation of subjects who are receptive to moral panics as compelling explanations for everyday insecurities. *A consumerist orientation to messages of fear facilitates this process*.' (emphasis my own). The mainstream media does, however, act as the principal source for these 'goods' that help amplify individuals' fears and insecurities. Stories of cybercrime and cybercriminals feature regularly in the news, preserving the public's ongoing concerns about the dark dimensions of the Internet and the potential for their victimisation by criminal and deviant elements lurking 'within'. Cinematic representations of cybercrime also contribute to shaping public insecurities, by exaggerating the potential for 'dystopic and catastrophic events' (Wall, 2008a: 58). Thus, a consciousness of crime 'is moulded by popular culture and institutionalised in the organisation of everyday life' (Furedi, 2006: 3).

This paper demonstrates how cues for encouraging these forms of consumption are embedded throughout the media's reporting of the Heartbleed security bug and underpin messages for citizens to protect themselves from identity theft and cybercrime more generally. It is these consumption cues which structure the results section.

Method

A qualitative thematic analysis of Internet news reports and accompanying imagery forms the basis of this research. Relevant news items were drawn from the media search engine Google News (http://news.google.com) across a week period beginning on the 7 April 2014 when media reporting on the Heartbleed bug first began. The keyword 'Heartbleed' was employed to identify the necessary metadata, returning a large quantity of page rankings relating to the security vulnerability. This sample was reduced to those news items appearing in the first ten

pages, whilst duplicated stories were also excluded from the data corpus. This resulted in a data set of 87 news items for analysis. Adhering to the method outlined by Braun and Clarke (2006), initial codes were derived and categorised from the data set. Codes were then sorted and assigned to a specific theme, in accordance with their semantic meaning. Some candidates themes were abandoned and assigned codes relocated, as the iterative process for checking the validity of assignments was undertaken.

Accompanying imagery was also subject to analysis. More often than not, images have been regarded as secondary to texts by many media researchers, possessing merely a supportive role in terms of the textual message (Kress and Leeuwen, 1996). Yet, as Greer (2003: 79) recognises, images transmit 'powerful ideological messages' about specific situations, social conditions or events. In response, criminologists have sought to reframe their analyses, focusing upon photographic images and visual representations (Jones and Wardle, 2008; Hayward and Presdee, 2010; Ayres and Jewkes, 2012; Banks, 2012). In accordance with these studies, this paper not only examines the discursive construction of the Heartbleed bug, but also reflects upon the ways in which it is visually represented in reporting. Consideration is given to the contents, framing, colour, quality and composition of the image itself, the image's relation to other images and the image's relation to text (Jones and Wardle, 2008). Thus analysis examines individual news pages, exploring both the inter and intra relationships between images and texts, in order to better understand how news reporting of the Heartbleed bug is 'interpretatively coded' (Hall, 1973: 232).

As investigation progressed, three distinct themes emerged: First, news items placed emphasis on the insecurity of both individual web sites and the Internet more generally, enabling readers to consume fear; second, that readers should seek out and consume consumer-protection information was repeatedly intimated throughout reporting, and; third, news items were linked, discursively and physically, to opportunities for citizens to consume

computer crime control products and services in order to better protect themselves and their loved ones. The results section below explores each of these themes in turn, first considering how Heartbleed's name, insignia and web domain both shaped and contributed to news reporting that emphasises the dangers posed by the bug and then exploring how this media coverage promotes, reinforces and facilitates a discourse that responsibilises citizens for their computer crime control.

Selling insecurity, consuming fear

The relatively short social history of the Internet is replete with numerous cases of computer viruses, worms, Trojan horses, malware, ransomware, bugs and other vulnerabilities, represented by a host of appellations, that have, at times, invoked images of disease, doom and destruction. CyberAids, Festering Hate, Freddy Krueger, MyDoom, Zeus and Cryptolocker are but a few of the cyber-threats that have faced online operators since the 1980s and been employed to conjure visions of the virtual environment as an e-dystopia that is 'monstrous, unconstrained and out-of-control' (Yar, 2012: 193). The Heartbleed bug represents a new stage in the evolution of how cyber-threats are conveyed to the public at large. Codenomicon masterfully communicated the vulnerability, the product of a simple coding error, through its name, a logo and an accompanying website, in turn, shaping news coverage across the mainstream media and beyond.

What's in a name?

There appears to be no predominant naming conventions for the myriad of computer bugs, viruses and other vulnerabilities that are often conflated and confused in popular discourse[3].

Typically, the security industry use letter and number formulas, not names, to refer to new online threats (McKenzie, 2014). Based upon the 1991 New Virus Naming Convention[4], a simplified version of this schema is commonly used and includes: 1) a prefix, which denotes the platform on which the virus replicates or the type of virus; 2) the name, which refers to the family name of the virus, as many viruses are variants of one particular strain, and 3) a suffix, which may be necessary to distinguish between variants of the same family and will typically include either numbers denoting the size of the virus or letters (Symantec, 2014). More recently, in January 2014, MITRE[5] began compiling a list of information and security vulnerabilities employing a 'common enumeration' identification system, in order to make it easier to share data across separate vulnerability capabilities. The common vulnerabilities and exposures identification syntax consists of: 1) the abbreviation CVE; 2) the year in which the vulnerability was first identified, and; 3) four or more arbitrary digits.

However, many viruses and vulnerabilities receive an alias that acts as a more common reference through which to communicate the threat more broadly. Such names are likely to stem from the researcher or research team that discovers and announces them and whilst this is often derived from the distinctive characteristics of the threat this naming process can be far more idiosyncratic (Lyman, 2002). For example, the Code Red computer worm discovered by eEye Digital Security employees Marc Maiffret and Ryan Permeh was named after the Mountain Dew soft drink they were consuming whilst examining the corruptive code. The Melissa virus was named after a stripper programmer David Smith met in Florida, whilst Koobface and Vundo take their names from the medium through which they are spread (Mosendz, 2014). The appellant Koobface is an anagram of Facebook, the social media site across which the worm was transmitted. Similarly, the Vundo Trojan horse, which was distributed through virtual communities, is a combination of the word 'Virtual' and Spanish term 'Mundo' (meaning 'world'). Other threats and vulnerabilities have been

named after the title of the infected file attachment, media and sporting celebrities or the developer themselves.

In this case, the designation Heartbleed is underpinned by the 'technical reality of the vulnerability, which is data leakage during a heartbeat protocol' (McKenzie, 2014). Much like the human body, computer servers employing the encryption standard OpenSSL have a heartbeat. During a transaction between any two servers, the encryption standard acts as a human heart with the beat communicating connectivity and validating the continuation of the transaction. Due to a flaw in the coding, it is this heartbeat that may be identified and appropriated by an attacker who can either steal information or impersonate either of the servers engaged in the transaction. However, in contrast to its official classification, CVE-2014-0160, the alias 'The Heartbleed Bug' also powerfully communicates insecurity, vulnerability, fear and danger. It was this alias that was carried across all media reporting of the vulnerability, serving to transmit worldwide worry about a 'deadly' and 'potentially catastrophic' online bug (*The Guardian*, 9 April 2014; *Times of India*, 12 April 2014; *Time*, 13, April 2014).

Evoking images of the heart, the most vital of organs, the centre of the entire circulatory system and functioning structure of invertebrates, emphasises the severity of danger posed. As *The Economist's* (9 April 2014) headline, 'A digital heart attack', demonstrates 'the Heartbleed Bug sounds like a particularly nasty coronary complication'. The identifier Heartbleed is representative of a wider trend of 'biologizing technology' (Dunn Calvety, 2013: 110), with cyber security rhetoric frequently drawing upon biological science as an effective discourse through which to communicate threats to the less technically minded. Like the term 'cybercrime', viruses, worms and bugs are constructions that have 'come to symbolise online insecurity and risk' in the public imagination and their everyday usage (Wall, 2012: 6). Health related metaphors are prevalent throughout cyber-security discourse

and are fed by public anxieties of pollutants, dirt and disease, which represent a threat to our physical and ontological security (Douglas, 2002). Parikka (2007) notes how parallels are both implicitly and explicitly drawn between biological viruses, most notably sexually transmitted diseases such as AIDS, and computer viruses in cyber-security discourse. This has been effective in spreading fear and anxiety amongst digital populations, as Dunn Calvety (2013: 111) recognises:

> Given the special place viruses have in history as one of the scourges of mankind, fear from infectious disease, virtual or real, is deeply ingrained in the human psyche, so that employing viral metaphors for things we are scared of, especially "known unknowns", seems to come naturally to us.

Like other viral metaphors, the Heartbleed bug transmits messages of illness, contagion and serious consequences for those infected. The haemorrhaging of personal and financial information is depicted as life threatening to individual's 'data double' (Haggerty and Ericson, 2000), with the immune system that protects in the region of half a million of the Internet's secure web servers falling apart: 'Web data BLEEDOUT: Users to feel the pain as Heartbleed bug revealed' (*The Register*, 9 April 2014) Such imagery is reinforced by Heartbleed's 'insignia', which removes CVE-2014-0160 from its cloak of technical jargon and reveals a powerful, memorable and jarring logo.

Branding insecurity

Bugs, viruses and other vulnerabilities are largely invisible to the average computer user and do not typically offer opportunities for the graphic imagery so desired by the news media and prevalent in their reporting of crime and criminal justice. The Heartbleed bug is reified

through a visual representation that was employed and adapted across the vast majority of media reporting of the vulnerability (see, for example, *BBC News*, 8 April 2014; *The Wall Street Journal*, 8 April 2014; *Al Jazeera*, 9 April 2014; *The Telegraph*, 9 April 2014; *The Guardian*, 9 April 2014; *Daily Mail*, 10 April 2014; *Fox News*, 10 April 2014). The minimalist design, which is bold and literal, consists of a deep blood red heart from which five dripping, bloody stalactites descend (see Figure 1).

[PLEASE INSERT FIGURE 1 HERE]

Figure 1. The Heartbleed bug logo that appears on the heartbleed.com domain and throughout media reporting of the vulnerability.

Whilst reaffirming the literal meaning of Heartbleed, the image also acts to magnify the perceived severity of the threat by making it something 'real' and tangible. As Cohen (2002: 10) recognises, images of folk devils are 'invariably tied up to a number of highly visual scenarios associated with their appearance'. Thus, the visual representation of the Heartbleed bug acts to objectify something that may otherwise seem abstract and therefore unimportant to vast swathes of the public. Combined and juxtaposed with headlines, by-lines and captions that emphasised how this 'serious vulnerability' (*The Huffington Post*, 8 April 2014), which is 'scaring the Internet' (*The Wire*, 8 April 2014), could be exploited by cybercriminals to access internet users 'personal data as well as a site's cryptographic keys, which can be used to impersonate that site and collect even more information' (*CNN*, 9 April 2014), imbues the Heartbleed image with a connotative message of insecurity, danger and

personal risk. This image was reused and adapted across media coverage, playing a vital role in communicating the threat posed by the vulnerability.

Heartbleed is unique in that it is: 'A bug with its own logo' (*The Telegraph*, 10 April 2014). Representing one of cybersecurity's 'first "branded" exploits', the Heartbleed vulnerability 'has been…carefully curated [and] professionally packaged for easy mass consumption' (Briggs, 2014). This branding rather than offering a 'recognised sign of value' (Castells, 2001: 76) offers a recognised sign of insecurity.

> Why spend the extra money for a logo? Because it suggests professionalism and dedicated effort, because it will be used exhaustively in media coverage of the vulnerability, because it further deepens the branding association of the vulnerability, the name, the logo, and the canonical web presence, and *because it also suggests danger*. (McKenzie, 2014, emphasis my own).

Fear-arousing imagery is widely employed, both in media reportage and advertisement campaigns by commercial organisations, governments and charitable groups, in order to fulfil their strategic aims. Exploiting the late capitalist condition wherein anxiety, fear and self-interest are citizen's overriding emotional responses to the insecurities that pervade their everyday existence, fear is increasingly drawn upon and utilised by private companies in the sale of security and crime control commodities (Hayward, 2004; Hall and Winlow, 2005). Like the contemporary urban experience Hayward (2004) documents, online activities are also shaped by fear and desire, with products and services that make us feel safer sought out and consumed. Thus, the maintenance of consumer citizens' fear, anxiety and perceived vulnerability is an essential element of computer capitalist culture. The Heartbleed bug is but one of many 'signal events' that exerts 'a disproportionate impact upon public beliefs and attitudes when compared with their "objective" consequences' (Innes 2004: 151) and helps

maintain the public's concern regarding the dangers posed to their personal and financial information, particularly when it is held in digital environments. Its easily digestible and replicable branding undoubtedly plays an important role in communicating the vulnerability beyond the IT community to the public at large. Described by its curator Leena Snidate as having "a life of its own", the Heartbleed logo is certainly simple, ubiquitous and powerful, acting as a 'truncated version' (Hall 1973: 227) of cultural code; expressing, reinforcing and appearing to inherently connote the insecurity embedded in the textual construction of the vulnerability.

What is the CVE-2014-0160?

A simple, single (self) serving web page enabled Codenomicon to adroitly communicate the threat posed by the Heartbleed bug. Extracts of the information presented on the web domain were frequently quoted verbatim in the news reports examined and played a key role in constructing the Heartbleed bug as a highly 'pernicious flaw' (*NBC News*, 11 April 2014) that 'may imperil hundreds of millions of Internet users' (*The Oregonion*, 10 April 2014). Using a straightforward question and answer formula, Codenomicon was able to respond to the most prescient of questions regarding the vulnerability, including: 'What is the CVE-2014-0160?', What is being leaked?', 'Am I affected by the bug?', 'How can OpenSSL be fixed?', and 'Is there a bright side to all this?'.

Across the thirty-five questions and answers that constitute heartbleed.com the 'tone of the discourse vacillates between alarmist and reassuringly benevolent.' (Whitson and Haggerty, 2008: 577). Written in a style befitting a journalist, the Heartbleed web page effectively communicates the threat, as it is technically precise, yet comprehensible to a layperson:

> The Heartbleed Bug is a serious vulnerability in the popular OpenSSL cryptographic software library. This weakness allows stealing the information protected, under normal conditions, by the SSL/TLS encryption used to secure the Internet. SSL/TLS provides communication security and privacy over the Internet for applications such as web, email, instant messaging (IM) and some virtual private networks (VPNs).
>
> The Heartbleed bug allows anyone on the Internet to read the memory of the systems protected by the vulnerable versions of the OpenSSL software. This compromises the secret keys used to identify the service providers and to encrypt the traffic, the names and passwords of the users and the actual content. This allows attackers to eavesdrop on communications, steal data directly from the services and users and to impersonate services and users. (Codenomicon, 2014)

Moreover, by presenting a scenario in which Codenomicon acted as both the attacker and the attacked, the security company was able to emphasise the ease with which information may be stolen by interlopers:

> We have tested some of our own services from attacker's perspective. We attacked ourselves from outside, without leaving a trace. Without using any privileged information or credentials we were able steal from ourselves the secret keys used for our X.509 certificates, user names and passwords, instant messages, emails and business critical documents and communication. (Codenomicon, 2014)

This scenario was either quoted verbatim or paraphrased in a number of news reports, in order to underline the severity of the situation facing computer users (see, for example,

International Business Times, 7 April 2014; *TechCrunch*, 7 April 2014; *Al Jazeera*, 9 April 2014; *Reuters*, 9 April 2014; *The Telegraph*, 9 April 2014).

With Heartbleed's name, branding and web domain carried across all of the media reporting examined, Codenomicon was clearly successful in positioning itself as *the* authoritative voice on the threat. Moreover, the precision and clarity of information presented on the heartbleed.com domain meant that Codenomicon was not only cited throughout media coverage of the vulnerability, but was also successful in shaping both the content and tone of this reporting. Despite there being no evidence that the vulnerability had been exploited for criminal gain, the threat posed by Heartbleed was magnified through Codenomicon's depiction of much of the web as being in imminent danger. This narrative shaped news headlines across the mainstream media:

> Massive OpenSSL bug 'Heartbleed' threatens sensitive data. (*The Wall Street Journal*, 8 April 2014)
>
> 'Heartbleed' bug in web technology threatens user data (*The Telegraph*, 9 April 2014)
>
> 'Heartbleed' bug exposes millions of websites to security risks (*NBC News*, 8 April 2014)
>
> 'Heartbleed: Hundreds of thousands of servers at risk from catastrophic bug' (*The Guardian*, 9 April 2014)

The severity of the vulnerability was reinforced by a host of other cybersecurity companies and security personnel. For example, Tony McDowell of Encription Ltd, which advises the Government's online security unit at GCHQ, stated that: 'This is 'Day Zero'. Tech giants spot the issue and fix it – but there's a gap when everyone is vulnerable.' (*Daily*

Mirror, 10 April 2010), whilst security expert Bruce Schneier is widely quoted, depicting the bug as disastrous for the online security of individuals' private information: '"Catastrophic" is the right word. On the scale of 1 to 10, this is an 11.' (*The New Yorker*, 9 April 2014). The enormity and longevity of the vulnerability was reaffirmed by a host of other professionals, such as security expert at Pen Test Partners Ken Munro, who claimed that the Heartbleed bug was 'the biggest thing I've seen in security since the discovery of SQL injection[6]' (*BBC News*, 8 April 2014), and Ty Miller of Threat Intelligence who suggested that: 'This vulnerability is going to be around for ten years' (*The Register*, 9 April 2014).

Proclamations of doom and destruction from cryptographers, software engineers and security professionals served to justify and reinforce the media's hyperbolic discourse. This was neatly encapsulated in a report by *TechCrunch*:

> I saw a t-shirt one time. "I'm a bomb disposal technician," it read. "If you see me running, try to keep up." The same sort of idea can be applied to net security: when all the net security people you know are freaking out, it's probably an okay time to worry. This afternoon, many of the net security people I know are freaking out. A very serious bug in OpenSSL — a cryptographic library that is used to secure a very, very large percentage of the Internet's traffic — has just been discovered and publicly disclosed. (*TechCrunch*, 7 April 2014)

News reports repeatedly drew upon Codenomicon's claim that two thirds of the Internet was vulnerable to data theft, as OpenSSL is used to 'protect' a vast proportion of the Internet's email servers, chat servers, virtual private networks, network appliances and client side software:

> Critical security bug 'Heartbleed' hits up to 66 Percent of the Internet (*The Huffington Post*, 8 April 2014)

> Catastrophic Heartbleed bug exposes 60% of private Internet data (*Examiner.com*, 8 April 2014)
>
> Major security alert over ‘Heartbleed’ eavesdropping bug that could have infected TWO THIRDS of sites (*Daily Mail*, 8 April 2014).

To further accentuate the danger posed to individuals and businesses, many reports, including those by *The Telegraph* (10 April 2014), *Time* (10 April 2014) and the *Daily Mail* (10 April, 2014), compiled lists of afflicted sites from across leisure, entertainment and retail sectors, including Amazon web services, Etsy, Flickr, Google, Gmail, Instagram, Pinterest, Tumblr, Minecraft, Netflix, Youtube and Yahoo! Similarly, the *New York Times* (8 April 2014) and *CBC* (9 April, 2014) highlighted the extensive usage of OpenSSL by government agencies like the Federal Bureau of Investigation and Canada’s tax agency, as well as devices such as Android smartphones, Cisco desktop phones and home Wi-Fi routers that are widely used by citizenry.

As the week progressed, news stories reported on how the ‘potential damage continues to spread’ (*The Financial Times*, 10 April 2010) as ‘the bleed continues’ (*The Wall Street Journal*, 11 April 2014). Security experts warned that: ‘Hackers could crack email systems, security firewalls and possibly mobile phones through the "Heartbleed" computer bug’ (*NBC News*, 11 April 2014). *Forbes* (11 April 2014) reported that: ‘A billion smartphone users may be affected by the Heartbleed security flaw’, whilst *The New York Times*, *CNBC* and *The Financial Times* (10 April 2014) were amongst a host of news agencies suggesting that ‘criminals could be impersonating bank services or stealing users’ online banking passwords’.

By emphasising how the Heartbleed bug may effect a host of products and services integrated into citizens' daily lives, reporting draws upon a Barlovian vision of cyberspace

wherein ‘the virtual is not a space of *transcendence* but one of *extension*: it is yet another mode or means through which fundamental organising features of social life are articulated and inextricably entwined with the ‘offline’ environment’ (Yar, 2012: 197, emphasis in original). A ‘precautionary logic’ (Ericson, 2007) characterises this discourse, with reports highlighting that: 'While it's conceivable that the flaw was never discovered by hackers, it's nearly impossible to tell.' (*Fox News*, 10 April 2014). More worryingly, the Heartbleed bug is likely to represent just one of many other unidentified security flaws that leave Internet services ‘utterly vulnerable’ to exploitation by criminal entrepreneurs:

> The whole situation is chilling — not just because we don’t know who might have known about the bug and leveraged it to steal data, but also because it’s such a sobering reminder of how little we know about the software we depend on every day. There are other Heartbleeds out there; it’s just that nobody’s told us about them yet. (*Time*, 11 April 2014)

Under the rubric of risk, such coverage reinforces the idea that all Internet users are potential victims in an environment in which crimes can be anonymous, instantaneous and automated (Brenner, 2007): ‘The worst case scenario is that someone found the flaw [two] years ago and has spent all that time scraping sites for personal details.’ (*Daily Mail*, 10 April 2014). The discursive construction of the Heartbleed bug is emblematic of news reporting that routinely presents the computer user as being exposed to a host of online threats, predations and risks. However, the Heartbleed bug represents a new stage in the evolution of the way in which threats are communicated to media organisations and the general public. By branding the insecurity, Codenomicon was successful in presenting itself as the authoritative voice on the vulnerability, orchestrating both the tone and content of media coverage. Consequently, speculative notions of what could happen to citizens’ data frame media coverage, with emphasis placed on the ease with which cyber criminals could acquire

individuals' personal details, bank information and medical records if appropriate action is not taken to avert this threat. With Heartbleed's name, logo and web domain playing a central role in media reporting, the bug was constructed as an eminent threat to computer users. Thus citizens were provided with the opportunity to consume fear, regarding the insecurity of both their personal data and the online environment in which it is held, through media coverage of a new, 'dangerous' (*NBC*, 8 April 2014) and 'scary' (*The Wall Street Journal*, 8 April 2014) vulnerability that 'is nothing to mess with' (*The Wire*, 8 April 2014) .

A discourse of self-protection

The governance of cybercrime is marked, in part, by a 'stepping back' of the state, with responsibility for crime prevention dispersed amongst a variety of non-state agencies, as well as consumer citizens. This stepping back is mirrored in public discourse, as government officials and criminal justice personnel's voices are largely absent from debates on cybercrime and cybersecurity. Filling this vacuum is the private security expert, readily available to impart a precautionary logic which serves to responsibilise citizens and encourage them to take the necessary action to reduce their likelihood of victimisation.

Computer security experts appeared as the principal (and often only) source of information throughout media reporting of the Heartbleed bug. For example, Mikko Hypponen of security firm F-Secure advised citizens to: 'Take care of the passwords that are very important to you. Maybe change them now, maybe change them in a week. And if you are worried about your credit cards, check your credit card bills very closely.' (*Yahoo! News*, 9 April 2014). Such sage advice is echoed across news headlines, with the: 'Public urged to change ALL passwords over major computer security flaw' (*Daily Mirror*, 10 April 2010)

and if ‘you haven’t changed your passwords, do it now’ (*The Washington Post*, 10 April 2010).

The altering of online behaviour was also encouraged, with the inability of citizens to implement safe computing habits presented as exacerbating an already dangerous situation. For example, Gerry Egan, senior director of product management at Symantec, suggested that the failure of computer users to implement proper password etiquette, such as not using one password for multiple services, could lead to the leakage of vital information:

> "We believe a lot of users take shortcuts in their usernames and passwords," he says. "While the big sites might have fixed this issue, if the smaller sites haven't and one of those gets attacked, that credential is potentially in their hands." (*USA Today*, 9 April 2014)

The inability of citizens to act responsibly online – by demonstrating user awareness and safe computing habits – is thus constructed as a key causal factor in the creation of security vulnerabilities and the spread of viruses and worms. Technology forecaster’ Paul Saffo noted how: ‘Good security practices get in the way of our click-and-go culture’ and, consequently, the ‘biggest risk to the consumer is the consumer himself’ (*International Business Times*, 10 April 2014). By expediting the distribution of malicious software and presenting entry points for hackers, individual and organisation users are depicted as computer illiterate and less than adept. Failure 'to secure one's system and oneself from harm' (Brenner, 2005: 679) is by association a failure to act as a good netizen.

Some news reports, including those by *BBC News* (8 April 2014) and *The Christian Science Monitor* (10 April 2014), directed citizens to digital innovation news site *Mashable*, which had compiled a ‘hit list’ of ‘the passwords you need to change right now’. *Mashable* (10 April 2014) detailed a range of governmental organisations, social networking sites,

email providers, financial institutions, as well as a range of stores and entertainment providers, affected by the bug and implored it readers to ‘change your passwords immediately.’ This discourse validates a model of crime control governance wherein good cybercitizens are expected to purchase and use particular software and educate themselves about the various dangers that surface online.

As a ‘link based phenomenon’ (Steinmetz 2012: 29), the Internet is inherently multi-sited, with information often disseminated through hyperlinks that redirect individuals to different web pages. Embedded throughout some of the media coverage of the Heartbleed bug are links to various cybersecurity companies’ expert blogs and consumer facing websites. For Codenomicon, Heartbleed's name and logo serve as conduits through which responsible citizens can access its dedicated web presence and consume the necessary crime control information. Whilst much of this information is free, some hyperlinked sites provide opportunities for individuals to purchase additional information.

A number of security companies responded to the dangers posed by the Heartbleed bug by releasing free tools to help consumers determine if a website that they visit is safe or not. Some of these tools were promoted in media coverage with embedded links guiding readers to security companies’ consumer facing websites. For example, both *BBC News* (10 April, 2014) and *ITV News* (10 April 2014) were amongst a host of media organisations that directed citizens to the LastPass website where they could utilise a free program, which identifies whether or not a site is vulnerable to the Heartbleed Bug: 'LastPass will not only alert you to which sites are vulnerable, but also tell you the last time you updated your password for the site, when that site last updated their certificates and what action we recommend taking at this time.' (LastPass, 2014). However, the LastPass site also presents the opportunity for citizens to 'Go Premium' and upgrade to the 'Complete LastPass Experience'. Similarly, *The Huffington Post* (12 April 2014) encouraged readers to visit

McAfee's website, where they could enter any website name to find out if the website is 'currently vulnerable' and, therefore, arm themselves with the requisite knowledge to 'stay safe'. Highlighting that 'in this day and age, we all need to be vigilant about protecting ourselves online', responsibilised citizens were provided with links not just to McAfee's free Heartbleed checker tool, but also to its 'LiveSafe' products and online blog, which offers further information and security software that may be purchased in order: 'To secure your digital life'.

Cybersecurity companies have been particularly successful in developing freemium business models (Anderson, 2009) that attract individuals through free software and shareware programs and then upsells some of them to premium services. In the field of cybersecurity, the success of such a model is predicated on the ability of private companies to present their premium products and services as being able to offer consumers liberation from specific cyber threats and fears. That consumer-citizens seek to 'buy off' fear is, therefore, an essential element of a functioning capitalist computer culture (Parikka, 2008).

Buying off digital fear

By appearing in media reportage of the Heartbleed bug, commercial computer crime control businesses were able to position themselves as recognised and legitimate providers of online security. As Coaffe and van Ham (2008: 191) note, 'being recognised as a provider of security offers concomitant authority and credibility. In this sense, what we might refer to as 'security branding' adds value to, or at least reconfigures, existing brand images, and creates Unique Selling Points (USP's).' Through such recognition, Codenomicon and a host of other security companies and experts were able to promote their wares and present opportunities

for consumer citizens to purchase products and services that are constructed as being able to relieve their fears and anxieties.

Codenomicon's heartbleed.com domain was identified as the authoritative source of information concerning the vulnerability by the vast majority of media agencies reporting on the vulnerability, with a link to its site embedded in most articles:

> Fortunately, Finnish security firm Codenomicon has already set up a dedicated website to help users and companies protect themselves against the new threat. (*ITV News*, 10 April 2014).

> There's a Heartbleed Bug website that has the technical details. It's not light reading, by any means, but it's interesting and important if you're into this kind of stuff. (*Time*, 9 April 2014).

The heartbleed.com domain is, in turn, linked to Codenomicon's commercial site, which offers consumers a suite of different services, including security testing, abuse situation awareness solutions and unknown vulnerability management. A scrolling banner at the top of Codenomicon's homepage expounds a pre-crime prudentialism that encourages consumer citizens to act immediately: 'In cyber security, the opposite of proactive is too late'. By reiterating that: 'It's what you don't know that makes you vulnerable', Codenomicon is able to present a host of products that are responsive to a wide array of computer and consumer insecurities. As Yar (2008: 189-190) recognises:

> [I]n decidedly neo-liberal times, the capitalist market now mediates a bewildering range and variety of tools and technologies, expert knowledge and 'best practice' strategies, precautionary codes and threat assessments. Security has, in other

words, now become inextricably entwined with the circuits of accumulation in contemporary capitalism.

Other private security providers also sought to benefit from this ‘capitalism of fear’ (Duclos 2005), by presenting and promoting 'novel' consumer products. For example, Russian security software maker Kaspersky Lab is quoted in an article by *BBC News* (10 April 2014), with embedded links directing citizens to their blog and on to their consumer facing website. Here, consumer citizens are encouraged to 'Check your passwords now' and review 'The cyberworld survival guide', whilst opportunities to purchase 'Internet security' are also presented. Others, including security company CloudFlare, whose commercial webpage is embedded in an article in *The Guardian* (10 April 2014), claimed to have addressed the vulnerability prior to it becoming public knowledge: ‘We fixed this vulnerability last week before it was made public. All sites that use CloudFlare for SSL have received this fix and are automatically protected’. This announcement highlights that despite the Internet presenting ‘a range of online threats from spammers to SQL injection to DDOS…CloudFlare is on top of things and making sure your sites stay as safe as possible.’ Similarly, private security company F-Secure (see *Yahoo! News*, 9 April 2014) offers citizens 'award winning technology' that not only claims to secure 'you, all your devices and your whole family' when shopping and banking online but, more extravagantly, to 'protect your life on every device'. Explicit in this imagination is the inherent danger cyberworlds present not just to individual's data double but, by extension, individuals themselves. Moreover, it is only by purchasing the requisite computer crime control security and software that the potential for victimisation can be reduced.

Undoubtedly, the discovery of the Heartbleed bug provided the computer crime control industry with a significant opportunity to advance their corporate interests. By emphasising the long exposure of the vulnerability, the ease with which it may be exploited

and that attacks will leave no trace, a scenario in which citizens' personal and financial data is in imminent danger is constructed. For the responsibilised netizen, it is only through the consumption of the necessary computer crime control knowledge, products and services that such a threat can be averted. The Heartbleed 'event' is indicative of the success with which computer capitalists have been able to benefit from the coding errors and vulnerabilities inherent in their own products and services:

> Digital capitalist culture…seems to be the first system that has really succeeded in converting its own accidents to its own profit. The noise of the network machine is folded back (reterritorialized) into its circuits in a manner that suits the logic of the risk society and second-order cybernetics. (Parikka, 2007: 100)

Under such conditions, insecurities are recycled, repackaged, rebranded and resold, in order to sustain a computer capitalism that instils in the public a 'want' for consumer products that are depicted as being able to offer citizens readymade remedies for the fears and anxieties that infiltrate their online activities.

Conclusion:

This paper presents the first criminological analysis of how computer threats and vulnerabilities are textually and visually communicated to citizenry, through an analysis of the Heartbleed bug. Three consumption cues are embedded in media reporting of the vulnerability and serve to help sustain a neoliberal regime of computer crime control wherein citizens are charged with protecting themselves from the various risks, dangers and predations that are seen to permeate virtual environments. The Heartbleed bug was constructed as a severe threat to the safety of individuals' personal and financial data

throughout global media reporting. Acting as a signal event that retrained the public's focus on the insecurities of digital databases, media coverage served as a conduit through which the public could consume fear. Fear is undoubtedly a primary motivator among humans and was harnessed by Codenomicon in its construction of the Heartbleed bug. Through its name, logo and dedicated web presence, fear and insecurity was socially constructed, amplified by the mass media, and consumed by citizenry. This 'branding of insecurity' enabled Codenomicon to position itself as the principal source of information and authoritative voice regarding the vulnerability, shaping both the content and tone of news coverage.

The construction of online vulnerabilities such as Heartbleed as imminently threatening could serve a number of different purposes. It may well be the case that the hyperbolic news reporting that follows the discovery of a new digital danger acts to drive public awareness and increase the speed with which online populations identify and deploy preventative measures and remedies for the myriad of bugs, worms and viruses that threaten virtual environments. Alternatively, the 'marketing' of the Heartbleed bug could well be read as 'a deliberately calculated attempt to peddle fear, uncertainty and doubt by the media and cyber-security industry to further its interests' (Wall, 2008a: 46). As some have argued (Parikka 2007; Monaghan, 2008), the contemporary computer capitalist condition is marked by a synergetic relationship between those forces that produce fear and those forces that produce consumer products. By maintaining a reassurance gap between the public's expectations and the state's ability to provide safety and security online, citizens are encouraged to look to the marketplace for solutions to their fears and anxieties. The consumption of cybercrime control information, products and services enable citizens to feel safer. Thus: 'The desire to consume as a way to fight fear and anxiety is at the very heart of digital culture and, in our case, the discourse' of such threats and vulnerabilities (Parikka, 2007: 169).

Irrespective of the motivations behind the presentation of the Heartbleed bug, Codenomicon has undoubtedly been successful in forging an everlasting association between itself and one of the most significant security oversights in the history of the Internet. That Google's security team also discovered the vulnerability is likely to be consigned to a mere footnote in history, demonstrating the commercial value in the effective communication of cyber risks and insecurities. With industry profits driving the logic of computer crime control, the branding of insecurities, threats and vulnerabilities is likely to become standard practice. If this is the case, the next virus, worm or bug could well have many names and many logos, as private security companies compete to promote themselves, their products and their services.

Acknowledgements

The author would like to thank the anonymous reviewers for their invaluable suggestions.

Notes

1 OpenSSL is an open source implementation of Transport Layer Security and its predecessor, Secure Sockets Layer, which are security protocols designed to provide communication security over the Internet.

2 A recent Court of Justice of the European Union ruling that Internet search engines must remove individual's information upon their request may well serve to limit the availability of 'undesirable' personal material online. The 'right to be forgotten principle' does, however, only require the deletion of information if the individual's privacy is deemed to outweigh the public's right to find it. Moreover, Internet intermediaries, such as Google, are merely obliged

to remove content from the index of search engines and not completely from the online environment. With personal data still accessible through a dedicated search of page history, this information never dies it just fades away.

3 The Heartbleed bug was incorrectly described as a virus by a number of media outlets, which is indicative of a more general lack of awareness of the distinguishing features of different types of computer threat amongst the public at large. A bug is a defect in a computer program or system that causes it to behave in unexpected ways. By contrast, viruses are typically self-replicating programs that undertake a task in the manner they were designed to do. However, viruses and bugs can be interrelated with either viruses causing bugs in programs or bugs providing the security vulnerabilities through which viruses may spread.

4 The 1991 New Virus Naming Convention represents the first attempt to construct a standard virus naming scheme by a group of security experts known as the Computer AntiVirus Researcher Organization (CARO) (Riau, 2002).

5 The MITRE Corporation is a not-for-profit corporation working in the public interest. As part of a wider range of research and outreach activities, MITRE manages and maintains a list of information security vulnerabilities and exposures.

6 SQL injection is a way to extract information from the databases behind web sites and services using specially crafted queries.

References

Aas, K. F. (2004) *Globalisation and Crime*. London: Sage.

Anderson, C. (2009) *Free: The Future of a Radical Price.* London: Random House.

Ayres, T and Y. Jewkes (2012) ‘The haunting spectacle of crystal meth: A media-created mythology’, *Crime, Media Culture*, 8(3): 315-332.

Banks, J. (2012) 'Unmasking deviance: The visual construction of asylum seekers and refugees', *Critical Criminology*, 20(3): 293-310.

BBC News. (2007) ‘Data lost by Revenue and Customs’, *BBC News* [online]. Available at: http://news.bbc.co.uk/1/hi/uk/7103911.stm (accessed 16 June 2014).

BBC News. (2013) ‘Adobe in source code and data security breach’, *BBC News* [online]. Available at: http://www.bbc.co.uk/news/business-24392819 (accessed 16 June 2014).

Brenner, S. W. (2005) 'Distributed security: Preventing cybercrime', *The John Marshall Journal of Information Technology and Privacy Law*, 23(4): 659-710.

Brenner, S. W. (2007) Cybercrime: Re-thinking crime control strategies. In Y. Jewkes (ed.) *Crime Online*, pp. 12–28. Cullumpton: Willan.

Briggs, J. (2014) ‘Heartbleed, the first security bug with a cool logo’, *TechCrunch* [online]. Available at: http://techcrunch.com/2014/04/09/Heartbleed-the-first-consumer-grade-exploit/ (accessed 2 July 2014).

Buchanan, B. (2014) ‘Heartbleed bug: Insider trading may have taken place as shares slid ahead of breaking story’, *The Conversation* [online]. Available at: http://theconversation.com/Heartbleed-bug-insider-trading-may-have-taken-place-as-shares-slid-ahead-of-breaking-story-26026 (accessed 26 June 2014).

Castells, M. (1996) *The Rise of the Network Society.* Oxford: Blackwell.

Castells, M. (2001) *The Internet Galaxy.* Oxford: Oxford University Press.

Christie, N. (2000) *Crime Control as Industry: Towards Gulags, Western Style.* London: Routledge.

Coaffe, J. and van Ham, P. (2008) "Security branding': The role of security in marketing the city, region or state', *Place Branding and Public Diplomacy*, 4(3): 191-195.

Cohen, S. (2002) *Folk Devils and Moral Panics*. 3rd ed. London: Paladin

Crosby, J. (2008) *Challenges and Opportunities in Identity Insurance*. London: HM Treasury.

Curtis, S. (2014) ‘‘Heartbleed’ bug in web technology threatens user data’, *The Independent* [online] 09 April. Available at: http://www.telegraph.co.uk/technology/internet-security/10754169/Heartbleed-bug-in-web-technology-threatens-user-data.html (accessed 1 July 2014).

Deverell, J. (2014) ‘Lock down cybersecurity or face another Heartbleed – or worse’, *The Conversation* [online]. Available at: http://theconversation.com/lock-down-cybersecurity-or-face-another-Heartbleed-or-worse-26237 (accessed 26 June 2014).

Douglas, M. (2002) Purity and danger: An analysis of the concepts of pollution and taboo. London: Routledge.

Duclos, D. (2005) 'Everyone under control: On the cultivation of fear' Available at: http://www.eurozine.com/articles/2005-08-23-duclos-de.html (accessed 03 October 2014).

Dunn Cavelty, M. (2013) ‘From cyber-bombs to political fallout: Threat representations with an impact in the cyber-security discourse’, *International Studies Review*, 15(1): 105-122.

Ericson, R. V. (2007) *Crime in an Insecure World*. Cambridge: Polity Press.

Ericson, R. V. McMahon, M. and Evans, D. (1987) ‘Punishing for profit: Reflections on the revival of privatisation in corrections’, *Canadian Journal of Criminology*, 28(4): 355-387.

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

Finch, E. (2002) 'What a tangled web we weave: Identity theft and the Internet' in Y. Jewkes (ed.) *Dot.cons: Crime, Deviance and Identity on the Internet,* pp. 86-104. Cullompton: Willan.

Finch, E. (2007) 'The problem of stolen identity and the Internet', in Y. Jewkes (ed.) *Crime Online*, pp. 29-43. Cullompton: Willan.

Furedi, F. (2002) *Culture of Fear: Risk-taking and the Morality of Low Expectations*. London: Continuum.

Garland, D. (2001) *The Culture of Control: Crime and Social Order in Contemporary Society.* Oxford: Oxford University Press.

Grabosky, P., Smith, R. G. and Dempsey, G. (2001) *Electronic Theft: Unlawful Acquisition in Cyberspace.* Cambridge: Cambridge University Press.

Haggerty, K. and Ericson, R. (2000) 'The surveillant assemblage', *British Journal of Sociology*, 51(4): 605-622.

Hall, S. (1973) 'The Determinations of News Photographs', in S. Cohen and J. Young (eds) *The Manufacture of News: A Reader,* pp. 176-190. Beverly Hills: Sage.

Hall, S. and Winlow, S. (2005) 'Anti-nirvana: Crime, culture and instrumentalism in the age of insecurity', *Crime, Media Culture*, 1(1): 31-48.

Harris, E. A. and Perlroth, N. (2014) 'For Target, the Breach Numbers Grow', *The New York Times* [online] 10 Jan. Available at: http://www.nytimes.com/2014/01/11/business/target-breach-affected-70-million-customers.html (accessed 16 June 2014).

Hayward, K. (2004) *City limits: Crime, Consumer Culture and the Urban Experience.* London: Glasshouse Press.

Hayward, K. J. and Presdee, M. (2010) *Framing Crime: Cultural Criminology and the Image.* Oxford: Routledge.

Holt, T. J. (2013) 'Examining the forces shaping cybercrime markets online', *Social Science Computer Review,* 31(2): 165-177.

Holt, T. J. and Lampke, E. (2010) 'Exploring stolen data markets online: Products and market forces', *Criminal Justice Studies,* 23: 33-50.

Innes, M. (2004) 'Reinventing tradition? Reassurance, neighbourhood security and policing', *Criminal Justice,* 4(2): 151-171.

Jones, P. J. and C. Wardle (2008) 'No emotion, no sympathy': The visual construction of Maxine Carr', *Crime, Media Culture,* 4(1): 53-71.

Kress, G. and T. V. Leeuwen (1996) *Reading Images: Grammar of Visual Design.* London: Routledge.

Lyman, J. (2002) 'Name that worm – How computer viruses get their names', *Newsfactor Network.* Available at: http://www.newsfactor.com/perl/story/15662.html (accessed 30 June 2014).

McKenzie, P. (2014) 'What Heartbleed can teach the OSS community about marketing', *Kalzumeus Software.* Available at: http://www.kalzumeus.com/2014/04/09/what-Heartbleed-can-teach-the-oss-community-about-marketing/ (accessed 30 July 2014).

Merkel, R. (2014) ‘How the Heartbleed bug reveals a flaw in online security’, *The Conversation* [online]. Available at: http://theconversation.com/how-the-Heartbleed-bug-reveals-a-flaw-in-online-security-25536 (accessed 26 June 2014).

Miller, V. (2010) ‘The Internet and everyday life’, in Y. Jewkes and M. Yar (eds.) *Handbook of Internet Crime,* pp. 67-87. Cullompton: Willan.

Monahan, T. (2009) ‘Identity theft vulnerability: Neoliberal governance through crime construction’, *Theoretical Criminology,* 13(2): 155-176.

Mosendz, P. (2014) ‘How computer viruses get their names’, *The Wire* [online]. Available at: http://www.thewire.com/technology/2014/05/how-computer-viruses-get-their-names/361756/ (accessed 16 July 2014).

Motoyama, M., McCoy, D., Levchenko, K., Savage, S. and Voelker, G. M. (2011) ‘An analysis of underground forums’, *IMC’11,* 71-79.

O’Harrow, R. (2005) *No Place to Hide*. New York: Free Press.

O’Malley, P. (1992) ‘Risk, power and crime prevention’, *Economy and Society,* 21(3): 252-275.

O’Malley, P. (1996) ‘Risk and responsibility’ in A. Barry, T. Osbourne, and N. Rose (eds.) *Foucault and Political Reason,* pp. 189-208. London: UCL Press.

Parikka, J. (2007) *Digital Contagions: A Media Archaeology of Computer Viruses*. Peter Lang: New York.

PwC, (2011) *Cyber security M&A: Decoding deals in the global cyber security industry*. Available at: https://www.pwc.com/en_GX/gx/aerospace-defence/pdf/cyber-security-mergers-acquisitions.pdf (accessed 19 June 2014).

Presdee, M. (2000) *Cultural Criminology and the Carnival of Crime*. London: Routledge.

Ralph, P. (2014) 'Heartbleed patched but security time bomb is ticking', *The Conversation* [online]. Available at: http://theconversation.com/Heartbleed-patched-but-security-time-bomb-is-still-ticking-25582 (accessed 26 June 2014).

Riau, C. (2002) 'A virus by any other name: Virus naming practices', *Symantec*. Available at: http://www.symantec.com/connect/articles/virus-any-other-name-virus-naming-practices (accessed 30 July 2014).

Smith, R. G. (2010) 'Identity theft and fraud', in Y. Jewkes and M. Yar (eds.) *Handbook of Internet Crime*, pp. 273-301. Cullompton: Willan.

Steinmetz, K. F. (2012) 'Message received: Virtual ethnography in online message boards', *International Journal of Qualitative Methods*, 11(1): 26-39.

Stern, V. (2006) *Creating Criminals: Prisons and People in a Market Society*. London: Zed Books.

Symantec. (2014) 'Virus naming conventions', *Security Response*. Available at: http://www.symantec.com/security_response/virusnaming.jsp (accessed 30 July 2014).

Thomas, R. and Martin J. (2006) 'The underground economy: Priceless', *login: The Usenix Magazine*, 31: 7-17.

UNODC, (2010) 'Chapter 10: Cybercrime', *The Globalization of Crime: A Transnational Organized Crime Threat Assessment.* Available at: http://www.unodc.org/documents/data-and-analysis/tocta/10.Cybercrime.pdf (accessed 16 June 2014).

Wall, D. S. (2008a) 'Cybercrime, media and insecurity: The shaping of public perceptions of cybercrime', *International Review of Law, Computers and Technology*, 22(1-2): 45-63.

Wall, D. S. (2008b) ‘Cybercrime and the culture of fear: Social science fiction(s) and the production of knowledge about cybercrime’, *Information, Communication and Society,* 11(6): 861-884.

Wall, D. S. (2012) ‘The devil drives a Lada: The social construction of hackers as cybercriminals’, in C. Gregoriou (ed.) *The Construction of Crime,* pp.4-18. Basingstoke: Palgrave Macmillan.

Wall, D. S. (2013) ‘Policing identity crimes’, *Policing and Society: An International Journal of Research and Policy*, 23(4): 437-460.

Whitson, J. R. and Haggerty, K. D. (2008) ‘Identity theft and the care of the virtual self’, Economy and Society, 37(4): 572-594.

Woodward, A. (2014) ‘Don’t panic about Heartbleed but have a spring clean anyway’, *The Conversation* [online]. Available at: http://theconversation.com/dont-panic-about-Heartbleed-but-have-a-spring-clean-anyway-25509 (accessed 26 June 2014).

Yar, M. (2008) ‘The computer crime control industry: The emerging market in information security', in K. F. Aas, H. O. Gundhus and H. M. Lomell (eds.) *Technologies of Insecurity: The Surveillance of Everyday Life*, pp.189-204. London: Routledge.

Yar, M. (2012) ‘Virtual utopias and dystopias: The cultural imaginary of the Internet’, in K. Tester an M. Hviid-Jacobsen (eds.) *Utopia: Social Theory and Future,* pp.179-196. Aldershot: Ashgate.