2ND EDITION

UNDERSTANDING
NEW MEDIA

EUGENIA SIAPERA

SAGE

Los Angeles | London | New Delhi
Singapore | Washington DC | Melbourne

Los Angeles | London | New Delhi
Singapore | Washington DC | Melbourne

SAGE Publications Ltd
1 Oliver's Yard
55 City Road
London EC1Y 1SP

SAGE Publications Inc.
2455 Teller Road
Thousand Oaks, California 91320

SAGE Publications India Pvt Ltd
B 1/I 1 Mohan Cooperative Industrial Area
Mathura Road
New Delhi 110 044

SAGE Publications Asia-Pacific Pte Ltd
3 Church Street
#10-04 Samsung Hub
Singapore 049483

First edition published 2011
Reprinted 2012, 2013, 2014
This second edition published 2018

Editor: Michael Ainsley
Assistant editor: John Nightingale
Production editor: Imogen Roome
Marketing manager: Lucia Sweet
Cover design: Jen Crisp
Typeset by: C&M Digitals (P) Ltd, Chennai, India
Printed in the UK

Library of Congress Control Number: 2017942509

British Library Cataloguing in Publication data

A catalogue record for this book is available from the British Library

ISBN 978-1-4462-9709-4
ISBN 978-1-4462-9710-0 (pbk)

TABLE OF CONTENTS

6

SECURITY, SURVEILLANCE AND SAFETY

LEARNING OBJECTIVES

- To learn the negative aspects of the articulation between technology, society, economics and politics
- To understand the significance of the expansion of surveillance
- To develop an understanding of issues relating to security
- To learn about online safety and protection against fraud
- To understand the relationship between new media, extreme porn and sexual aggression
- To critically understand the underlying dynamics of surveillance, security and safety

Introduction

For most people, the internet and the new media are associated with a host of positive developments, as they represent technological progress. Technological progress, one of the most central characteristics of modernity, signals improvements of almost all aspects of life, and entails the promise of the more just and equitable distribution of wealth and power. This view, which we can term techno-optimistic, is very widespread in society, with public money going into technological innovation and the spread of technologies among people. But in fact we know that technology – its 'essence' as Heidegger (Heidegger and Lovitt, 1977) would have it, or at least its uses, as other thinkers would insist – is much more ambiguous. This chapter will focus not only on this inherent ambiguity of technology, and hence of the new media, but also on some of its negative sides.

We will assume a social constructivist approach, holding that technology and its uses and outcomes must be thought of as an articulation between certain 'local' factors, such as the political, socio-cultural and economic conditions within specific historical contexts, and the specific 'affordances' or dimensions of the technology at hand. We will then look at the 'dark' side of the new media. In sections that will cover society, politics, economics and culture,

we will follow a case study approach which will examine surveillance, cyber-conflict, fraud and porn pathologies, respectively. Our goal here is not only to describe some of the 'darker' aspects of the new media, but also to find out the specific articulation of the technological elements of the new media with the specific socio-historical circumstances in the contexts in which they are located. Throughout this discussion, we must keep in mind that the economic, political and social domains are intermingled, and that the economic has a political and social dimension, and vice versa. The current division is only undertaken for analytical purposes.

Society: Surveillance and Control

If by the term 'society' we mean primarily the ways in which people associate and interact with each other, then there is no doubt that the internet and the new media have had a profound effect on these. While the specific changes in sociality – the ways in which we interact – are discussed in other chapters, the goal here is to find the 'dark' side of society online: the problematic aspects which are the outcome of the application of technology in certain ways that in turn reflect the current socio-historical circumstances. There is no doubt that these may be numerous, depending on how one chooses to define 'problematic'. In the present context, we may understand 'problematic' as those aspects that oppose the very understanding of society in Tönnies' (2001 [1887]) *Gesellschaft* form, that is, as an agreed, self-conscious and quasi-contractual association with others. While Tönnies was to an extent critical of this kind of association, we want to highlight here the reflexive and liberal elements in this understanding. In other words, if societies in an ideal-typical form are voluntary associations based on conscious choice, which preserve people's autonomy and independence, and which allow them to act freely as independent agents, then anything opposing these conditions may be deemed problematic in the current context. While many things can be considered problematic in this manner, in the context of the new media, the focus here will be on surveillance, which, as we will see, has a long history but is now taking new forms and has become more intense in and through the new media.

The rise of the continuous monitoring of people and the collection of massive quantities of personal data on all of us have led theorists such as David Lyon (2001) to propose that we are witnessing the rise of a surveillance society. This kind of society refers to the increasing amount of surveillance that is taking place, alongside an explosion in the variety of methods and means for observing and monitoring people's behaviours. While to an extent surveillance must be thought of as one of the defining characteristics of modernity, new media and technologies have helped make surveillance a central aspect of late (or post-) modernity as well. Surveillance, and significantly also self-surveillance and what Mark Andrejevic (2005) calls lateral surveillance, have now become an inextricable part of modern governance. Without surveillance, the work of governing bodies and bureaucracies would be extremely difficult, if not impossible. But surveillance introduces new divisions, new ways of classifying people and dealing with their behaviour. In so doing, new symbolic meanings are generated alongside new modes of control and often punishment: in short, new forms of power are made

possible, and this power is concentrated in the hands of those who collect and control surveillance data. All these may be seen as infringements of personal freedom and as detrimental to the democratic principles according to which our societies are said to function.

Panopticon and Synopticon

Surveillance has a relatively long history as it pre-existed new media technologies. However, as we shall see, it now takes new forms, which are commensurable with current socio-political developments. Specifically, in one of the better-known formulations of his relevant work, Michel Foucault has spoken of the Panopticon, an imaginary machine designed in 1791 by Jeremy Bentham, a British architect and legal reformer. This contraption allowed for the total and complete surveillance of prison inmates who, quite literally, inhabited a transparent world with no place to hide. The logic behind this machine, as Foucault (1995 [1975]) tells us, is that prisoners (aware of their complete and total visibility) would regulate their behaviour, knowing that any wrongdoing would be caught. For Foucault, this ensures the automatic functioning of power, since it would be internalized by prisoners without the need for any external enforcer to be present at all times. For power to work in this manner, it must be visible, seen by everyone, and unverifiable – it must operate independently of whether there is an enforcer or inspector present at all times.

While the Panopticon was designed for prisoners, today's surveillance society has extended its function to society as a whole: for how else can we describe the preponderance of the all-seeing CCTV cameras across not only public buildings and banks, but also in shops, squares, open spaces, train platforms, airports? Knowing that we are watched, we must behave ourselves: the visibility of power is evidenced in the ubiquity of cameras, whereas we almost never see the enforcers, the inspectors behind the cameras, those whose job it is to watch us all the time. The very idea of the Panopticon, argues Foucault, is an ideal form of power, and as such it was destined to spread in society, as it makes power more efficient. Its main principle is that people internalize the surveillance and behave in ways that conform to the requirements of power, and the result is not so much a repressed and conformist society, but rather a society whose individuals have been constituted as subjects/objects of surveillance. This means that they are constructed as subjects/objects for whom information can be, and is, collected on a constant basis, analysed, collated, processed, and even sold. In this manner, individuals are constantly (re)classified and assessed according to the requirements of power. But it is crucial to see the changes in the mechanisms of power involved in the shift from the Panopticon, which was essentially an architectural device or implement of power, to late modern ways of surveillance that primarily use the media.

The social theorist Zigmunt Bauman (1999) argues that while the Panopticon created docile people to populate the factories of the industrial era and created an information asymmetry between the owners and controllers of production systems and labourers, current conditions have different requirements. In globalized informational capitalism it is no longer efficient to discipline labour from 'above'. Producing a docile labour force through discipline is no longer necessary as this labour force can be found everywhere in a globalized world.

Rather than discipline, Bauman argues, the mechanism is seduction: introduce the stakes through televised broadcasts of celebrities and create new fantasies and new desires. The Panopticon is thus turned into a Synopticon which seduces people into watching. Specifically, Synopticon, a term coined by Thomas Mathiesen (1997), is taken to refer to a new technique of power, exemplified by the mass media, in which people are themselves turned into watchers: the many watch the few, but these few tend to be the global elites, movie stars and celebrities, politicians and star academics, in short, those in power and those whose statements are carefully repeated and all together convey a total way of life that is subsequently admired as the only or the most worthy way of life. Bauman's argument is that this technique of power, which is implemented by the mass media, legitimizes the current state of inequality through giving the impression of transparency and equivalence between the watched elites and the watchers. At the same time, it stifles any dissenting voices by propagating a certain lifestyle to be emulated and endorsed, in a bid to ensure conformity.

But while Bauman argues that the techniques of power have fundamentally changed under globalization, Mathiesen's (1997) original argument was that panoptical methods, in which the few watch the many, coexist with synoptical methods, in which the many watch the few. Similarly, David Lyon (2001) argues that these two work in tandem, complementing each other as mechanisms of control: for Lyon, the fact that the many watch the few legitimizes and justifies that the few can watch the many. But for Mathiesen, and Bauman, the rise of synoptical techniques takes place through the mass media, and especially television, which allows the many to watch the few. The question, however, that emerges here concerns the role played by the new media, which may introduce a new dynamic. Indeed, the new media offer renewed possibilities for surveillance, intensifying the processes of watching. At the same time, the new media impose a new model of watching, which entails constant surveillance of one another – it's as if the Panopticon was outsourced to everyday people, who now act as constant watchers of one another. Mark Andrejevic (2004, 2005, 2007) has extensively discussed surveillance and its mode in late modernity, holding that recent developments have intensified and amplified disciplinary surveillance. He refers to a new kind of lateral surveillance, in which peers watch one another. Although this kind of monitoring existed in villages and other, older forms of social organization, new media technologies have introduced new modes of watching, and have made these available to many people. For Andrejevic (2005), this democratization of access to investigatory techniques is linked to the rise of risk and uncertainty: anything can happen at any time by anyone. This creates a general culture of insecurity and suspicion which in turn feeds into and sustains the techniques of surveillance. Andrejevic further argues that the spread of surveillance techniques among the general populace reflects broader shifts in governance, shifts that relate to the rise of neoliberalism. On the other hand, this constant watching of one another follows or has contributed to the tendency to dissolve the boundaries between the public and the private: in a world of 24/7 surveillance, there is nothing left hidden, no area protected from the Big Brother gaze. Indeed, the metaphor of the Big Brother, based on George Orwell's novel *1984* , has now become a reality; in television shows, on our computer screens, and in public spaces, we are subjected to others' gaze and scrutiny, while we too subject others to the same scrutiny.

Surveillance, the State and the Expropriation of Information

Summarizing these theoretical elements, we can see that surveillance can be direct and top-down (Panopticon), used to coerce people into conformity; or indirect (Synopticon), in which the many watch the few, implemented through the mass media, using seduction to ensure conformity and the legitimization of existing inequalities. While the former, argues Lyon (2003), results in a system of control through classifying and categorizing people, the latter contributes to what may be called 'soul training'. Based on Andrejevic's work, we can argue that the new media have introduced a new dynamic in which the many watch the many: through the popularization of the new media and associated techniques of surveillance (including digital web-cameras, but also Google Earth, following people's accounts on Twitter, Facebook and the like, and through search engines and mobile phones) we can collect information on others, and they can collect information on us. This lateral surveillance supports and amplifies the previous two forms while intensifying further the functions of control, classification and wilful subjection to power. But apart from the clear socio-political implications here, which include loss of privacy, constant suspicion and a generalized sense of insecurity, surveillance has another dimension as well. This concerns the commercial exploitation of the information that is collected. Information is not only used for purposes of classification and social control, but also bought, sold and otherwise capitalized upon.

As we use supermarket fidelity cards, as we shop on e-shops such as Amazon, as we download music from iTunes or vote on talent shows using our mobile phones, we generate more and more information. These data are subsequently collected and used to create massive databases, which are then bought and sold. These databases are used to inform marketers of our choices, tastes and preferences, enabling them to sell or market products and services in more efficient ways. Often unbeknownst to us, the data trail we leave behind is used to classify us, to include us in certain categories, which are then used to inform production, marketing and the distribution of products and services. This commercial use of such data means that information that previously had no owners is now someone else's property. Already Facebook and Twitter are making money by selling 'analytics' – demographic information combined with user online behaviours – which they collect on the basis of what their users disclose and how they move within these applications. This is raising serious questions regarding information ownership, privacy and exploitation. More broadly, it questions the rhetoric on the rising power of the user, a rhetoric that has dominated the debate since the introduction of Web 2.0. In taking control over the information that we, the users, produce through our media use, new cleavages and new power structures emerge, while more and more domains of life become commodities to be bought and sold. Information is collected by a few private companies, resulting in what Andrejevic (2007) has called a 'recentralization' of information. While those controlling the massive databases that have been created are private companies, they make information freely available to national security agencies, compromising activism as well. What is worrying here is that, until recently, surveillance techniques were controlled by governments, which, whatever their failings, at least represent the broader public and act

on its behalf. Now, surveillance techniques have become the property of private companies, who operate for profit: more and more control and power is ceded to them, leaving less space for the public, the non-commercial and the common to operate freely.

But it is not that corporate surveillance has replaced state surveillance: far from it. In June 2013, whistleblower Edward Snowden revealed the extent of the surveillance being undertaken by the US National Security Agency (NSA), through its PRISM programme, providing details of the extensive and illegal surveillance of internet communications and that the NSA has direct access to the servers of Facebook, Google and Apple (Greenwald, 2013). According to Snowden, the NSA and other security agencies collected metadata on all communications by default – that is, they collected information on the who, what and when of all communications (Poitras and Greenwald, 2013). The agencies subsequently filter, measure and store this information for as long as it fits their purpose. The revelations sparked a debate over the US government's actions, and the legal aspects of accessing and storing this information without warrants, probable cause and the knowledge and consent of users. The fallout had an impact that was both domestic, in the US context, and global, as the PRISM programme targeted non-US citizens and spied on US allies. For example, it spied on the German Chancellor Angela Merkel, the Mexican leader Enrique Pena Nieto, and Brazilian President Dilma Rousseff, and it also spied on Chinese computers. The main points of the debate regarding the NSA revelations include: (1) the extent to which any government should be allowed to have access to private communications, (2) the data trail that people leave as they communicate online, and (3) who stores, owns and has access to this trail.

Briefly unpacking these points, the increased securitization, itself an outcome of the War on Terror but also connected to the rise of a risk society (Beck, 1992), has led to a confused ethical landscape where personal freedoms and rights can be compromised in the name of security. Thus, internally and later in the relevant hearings, the NSA justified its actions on the basis of protecting from and pre-empting future terrorist hits. The case remains, however, that such actions can be seen as unconstitutional, at least when US citizens were concerned, and unethical, when citizens of other countries were involved. The legal justification for the surveillance hinged on the notion of metadata: while the content of personal communications clearly falls within the remit of the Fourth Amendment, requiring probable cause and a warrant, this is not so clearly the case with metadata, as these concern information about the communication but not the contents of the communication *per se*. On the other hand, metadata reveal so much information that they render the actual content redundant. At the very least, these revelations alerted users to the digital trails their communications leave behind, and how both governments and corporations make use of this trail and the data it generates for their own purposes.

In parallel, the revelations that the NSA had access to the servers of corporations such as Google, Facebook and Apple implied that these organizations either worked with the NSA or that their security systems had been compromised. All the corporations refuted claims of collaboration with the security agencies, and following some high-profile hacking incidents – most notably of Apple's iCloud – they moved towards stronger encryption systems that would not allow for any kind of backdoor access, either by governments or by the

corporations themselves. Nevertheless, the move towards strong encryption is resisted by the security agencies, which consider that they must have a way into private communications in order to save lives. The debate has acquired a new momentum following the terrorist attacks in Paris in November 2015, although there is no evidence that encryption played any part in organizing these attacks. Yet security experts warn that any 'backdoor' access to people's communications can be exploited by hackers and other malicious agents (Sneed, 2015).

The main issue underlying these revelations and the question of surveillance is the right to privacy. Given that the technology allows our data to be accessed and stored by third parties, what remains of the right to privacy? And, as the security agency discourses argue, why should we worry if we have nothing to hide? Most countries have adopted complex data protection legislation, which has to balance the right to privacy with the ability of corporations to monetize data and governments to intercept malicious communications; in most cases this balancing act is imperfect and often the right to privacy ends up being compromised. As for the 'nothing to hide' argument, Edward Snowden's retort in a Reddit Ask Me Anything session in May 2015 addresses this very effectively: 'Arguing that you don't care about the right to privacy because you have nothing to hide is no different than saying you don't care about free speech because you have nothing to say' (Snowden, 2015). There is clearly a political component involved here and some of the threads of this discussion will be picked up in the next section.

To conclude, it is worth noting that in some ways, submitting to this constant monitoring in all its forms is seen as participation – we are doing it willingly, because we want to be part of the online networks and to take advantage of what they offer. But this kind of participation under conditions such as those described above, argues Andrejevic (2007), is a kind of unpaid immaterial labour (see also Chapter 3; Fuchs, 2013), as we produce even as we surf the internet, use our phones, update our social networking account, or download music. Both aspects of new media surveillance, which include the loss of privacy and generalized suspicion as well as the expropriation of information by private companies (Schiller, 2007), are commensurable with neoliberalism. This ideology revolves around ideas of deregulation and privatization (Murdock and Golding, 2001) and is also associated with an emphasis on individual self-regulation and assumption of responsibility for everything – ultimately, this heightened individualism ends up eroding the connections and bonds between people that make up society. From this point of view, surveillance of the many by the many (the lateral kind), which is precisely a reflection of this kind of neoliberalism in that it represents surveillance that has passed on to individuals themselves, ends up undermining the societies in which we live. If in general we can argue that the flip side of online participation is surveillance and control, then for as long as we – not as individuals but as the public – refuse to take control of the information we generate, this dark side will remain.

Politics: Cyber-conflict, Terrorism and Security

In our discussion of politics and the new media, we argued that the new media entail important political promises for more democracy, and a more just and equitable distribution of

wealth and power. Such a promise for more democracy also entails improvements in the lives of all people across the world. While being critical of utopian approaches that considered that new technologies will cure all political evils, we must not overlook the positive potential of more engagement by more people, which may result in important democratic gains. From this point of view, it is surprising that two profoundly problematic political phenomena are encountered in online and other new media environments. These include cyber-conflict and -terrorism. The former may be defined as real-world conflicts that spill over to cyberspace (Karatzogianni, 2004), while cyber-terrorism is understood as politically motivated attacks against information systems that result in violence against non-combatant targets, and which are undertaken by sub-national groups or clandestine agents (Curran, Concannon and McKeever, 2008). Extending this definition, we can also include here the ways in which terrorist groups have used new and social media to their advantage. Both cyber-conflict and cyber-terrorism may be considered problematic, if not inherently undemocratic, because they involve violence and the imposition of the will of the few against that of the many. From this point of view, they do not include cyber-activism, which is primarily aiming to change and influence public opinion. Rather, as Karatzogianni (2004) argues, in cyber-conflict, antagonists use the internet as a weapon, which is hurled against others. In this section we will discuss some of the methods and effectiveness of the internet when used as a weapon.

Karatzogianni (2004, 2006, 2009) situates cyber-terrorism primarily within the frame of ethno-religious (cyber-)conflict, and holds that its main methods include hacking enemy sites and creating/managing sites for propaganda and mobilization. To these we can add the use of the internet to distribute terrorist know-how on using bombs, explosive devices and so on, while another use includes soliciting financial support. More recently, a lot has been made of the use of social media for 'radicalization' (i.e., for the recruitment of followers) by terrorist groups such as the so-called Islamic State or Daesh. In what follows we will attempt to unpack the relationship between war, terrorism and new media.

Hacking and/in War and Conflict

Hacking, also referred to as information warfare, uses information technology tools to attack enemy websites. It uses the standard methods employed by hacktivists, but to different ends. These include distributed denial-of-service (DDoS) attacks, as well as Domain Name Service (DNS) attacks (see Karatzogianni, 2004). In the case of DDoS attacks, websites are prevented from working because they are flooded by a very high number of page requests, usually by 'zombie' machines. In DNS attacks, the domain name is severed from its numerical address, preventing users from accessing the site. While these are methods used by hacktivists for purposes that are considered to be more acceptable because they are primarily symbolic, in cyber-conflict and cyber-terrorism in particular, two more malicious methods are used as well: the spread of worms and unauthorized intrusions (Karatzogianni, 2004). Worms may enable hackers to gain control of computer accounts, turning them into 'zombies', which operate without the owners' knowledge and approval. Unauthorized intrusions into computer systems are perhaps the most widespread form of hacking in the popular

imagination, spread through films in which hacker-geniuses break into top-secret supercomputer systems such as that of the US military, NASA, etc. Through their illicit actions, such hackers can get access to top-secret information or otherwise sabotage the system.

These methods can work together as well as separately, and are quite effective weapons in cyber-war. In some cases, they can even herald hostility and forthcoming war. In the summer of 2008, some weeks before the conflict between Georgia and Russia escalated into an armed one, there were extensive reports of DDoS attacks against Georgia (Markoff, 2008). Observers noticed a stream of data directed at Georgian government sites with the message 'win+love+in+Russia'. These attacks effectively shut down Georgian servers, while the Georgian President, Mikheil Saakashvili, saw his website being attacked and rendered inoperable for 24 hours. In response, the presidential site was moved to Atlanta, in the US state of Georgia, to be hosted by Tulip Systems, a company run by a Georgian ex-patriate. In other hacking attacks, just as Russian troops entered South Ossetia, DDoS attacks crippled media, communications and transportation sites, as well as the National Bank of Georgia site (Markoff, 2008). The result, argues Markoff, was that throughout the attack, Georgia effectively had no internet connection and could not communicate with possible sympathizers abroad. Although those responsible for the attack were never identified, sources cited by Markoff point the finger at Russian nationalists. A group under the name of South Ossetia Hack Crew has claimed responsibility for defacing the Georgian Parliament website with image collages comparing Georgian President Saakashvili to Adolf Hitler (Leyden, 2008). In the meantime, the website of the South Ossetian government was attacked in August 2008, hours before being attacked by the Georgian artillery, while the Russian news agency RIA Novosti was also hit by a DDoS attack. In a combined DDoS and DNS attack in January 2009, the Central Asian Republic of Kyrgyzstan was knocked offline for more than a week, reportedly by Russian cybermilitia (Googin, 2009). In many ways, this kind of cyber-war represents the escalation and/or spillover of conflicts into cyberspace.

Two further examples show the ways in which new media have been put to the service of war. First, the high-profile hacking by the Syrian Electronic Army and, second, the development of Stuxnet. According to Al-Rawi (2014), the Syrian Electronic Army (SEA) is better understood not as a hacking group but as a cyber-warrior group. Its members describe themselves as non-aligned politically, but all their attacks and the rhetoric they use in their website and social media accounts support Bashar al-Assad. Al-Rawi (2014) holds that the SEA was initially hosted by the Syrian Computer Society, which was headed by Assad. He further argues that such activities could not take place in government-controlled areas in Syria without the government knowing and approving of them. The SEA has two objectives: to counter the impact of Syrian oppositional groups and to draw attention to the official Syrian version of events (Al-Rawi, 2014). Their method is simple: they hack into the sites of well-known and high-profile targets and then post the defaced sites on social media. Their targets have included universities (UCLA and Harvard), news media (Reuters, the *New York Times*, The Onion, ITN News, Associated Press and others), high-profile social media accounts (e.g., hacking into the Facebook and Twitter accounts of President Obama and redirecting them to a propaganda video) and military sites. In the summer of 2015 they

hacked into the US Army's public website, leaving a message that read: 'Your commanders admit they are training the people they have sent you to die fighting' (Vinton, 2015). In another high-profile hack in 2013, they hacked into the Twitter account of Associated Press and posted the following tweet: 'Breaking: Two Explosions in the White House and Barack Obama is injured.' Fisher (2013) claims that this hack led to a $136 million dip in the US stock market, making the case that this was not merely an act of vandalism but an act of cyber-terrorism since it led to real-world damage. The Syrian Electronic Army is also significant because of its attacks against media and against social media sites; their methods, which are not limited to DDoS through zombie computers, also include 'phishing' and other espionage methods, point to a thorough knowledge and understanding of coding and information infrastructures. Symbolically, this electronic army is a very useful branch of the Syrian army, and it is clear that no modern army or military group can operate without such an electronic counterpart. This is even more clearly illustrated in the case of Stuxnet.

Stuxnet has been discussed as a pivotal moment in the development of cyber-warfare, a cyber-weapon purposely built in order to destroy enemy infrastructure (Langner, 2011). In brief, Stuxnet is a computer program that was developed in order to infiltrate and disable the Iranian nuclear facility in Natanz. It works by entering a computer and reprogramming it. Effectively, in 2010 Stuxnet managed to enter the programs that controlled the Natanz nuclear plant and sabotaged their centrifuges. The key issue with Stuxnet, argue Farwell and Rohozinski (2011), is not its technological sophistication – Stuxnet was not particularly innovative and was easily disabled – but the movement to a new form of war which is conducted entirely online. While it is not clear where Stuxnet originated, its code suggests some involvement of Russian hackers, who have used similar instruments in the past for the purposes of industrial espionage (Farwell and Rohozinksi, 2011). Farwell and Rohozinski (2011) claim that this kind of cyber-attack represents the first of its kind: using off-the-shelf and deniable resources from the global cyber-crime community, the actual source of the attack can remain hidden and avoid retribution. If Iran felt it was attacked by an enemy, it cannot prove its case and cannot retaliate. In 2012, however, Iran found a computer virus, which they called 'Flame', that was collecting intelligence on their nuclear plants (Nakashima, 2012). It later transpired that Flame shared its basic 'DNA' with Stuxnet, leading to speculation that the US and Israel had colluded in developing and planting Stuxnet (Nakashima, Miller and Tate, 2012). Whatever the case, Stuxnet indeed represents a new phase, wherein states are themselves involved in the production of malware that is being used as a weapon to attack significant infrastructures.

New Media as Communication Tools in War and Conflict

The use of the new media in propaganda has often had disturbing consequences. In 2007 a video of a girl being stoned to death by a mob surfaced on the internet. The girl was 17-year-old Du'a Khalil Aswad, of Kurdish ethnic origin and Yazidi religion, who was stoned to death in

an honour killing in the Iraqi-Kurdish town of Bashiqa because she had eloped with a Kurdish Muslim boy. This video was replayed in various Islamic and jihadist forums, which reframed it as a crime against Islam, on the basis that the girl was killed because she had converted to Islam, subsequently calling for some sort of retaliation and revenge. This came in April 2007, a few weeks following Du'a's death: several cars full of gunmen stopped a bus of factory workers returning to Bashika, abducting all the men of Yazidi faith and executing them (Cockburn, 2007). Although there is no possible way in which to link the video with the calls for retaliation with the actual executions, we may place it in a context in which offline conflicts continue seamlessly in an online environment. Similarly the many videos of, for instance, Palestinian children in Gaza or images in war-torn Iraq and Afghanistan, may not contribute directly to the radicalization of young Muslims and others, but must be seen as part of the wider conflict and, as such, as tools in the effort to recruit more supporters (Hoskins, Awan and O'Loughlin, 2011). The processes of radicalization through social media are complex and have not yet been fully unravelled. This is discussed in more detail in the case study below.

Finally, this is the broader context in which we must place other techniques, such as use of the internet to distribute know-how and other kinds of practical knowledge. Manuals, how-to lessons, as well as detailed instructions are available online to guide prospective terrorists, while terrorists use the internet to make financial transactions, either through money laundering (Castells, 2004) or through seeking donations. Levitt (2002) reports that in 2001 a British internet site called the Global Jihad Fund (GJF), which openly associated itself with Osama Bin Laden, provided bank account information for various Islamic fundamentalist fronts and groups to 'facilitate the growth of various Jihad movements around the world by supplying them with funds to purchase their weapons' (posted on GJF's site). Ariely (2008: 9) reports that terrorist organizations must be seen as 'learning organizations' involved in knowledge transfers, including communication and economic, scientific and practical information and knowledge. The Islamic State or Daesh has also been known to solicit donations through Twitter and Facebook, but the US Treasury has taken steps to disrupt and stop such activities (Sink, 2014).

We can see, therefore, that the use of the internet in cyber-conflict can be very effective: it can be used to initiate events and control their outcome, as in the case of DDoS and DNS attacks; it can be used to regulate the flow of information, as in the propagandistic uses discussed above; and it can be used to mobilize support, both in the form of new recruits and in seeking donations. From this point of view, the internet is indispensable in modern cyber-conflict. More broadly, the use of the internet in cyber-conflict and cyber-terrorism provides, it seems, a good example of the mutual shaping of technology and society-politics. In a world which is riddled with conflict, technology can neither be seen as neutral nor as imposing its own logic of efficiency. Rather, it seems that new technologies are shaping some of the forms this conflict takes, which are now organized around distributed networks, using sophisticated technological tools, and mobilizing support from across the world. At the same time, the spillover of conflict in technological domains gives rise to antagonistic, aggressive and destructive technological practices. New technologies must therefore be seen as part and parcel of the current world order, actively shaping it while also being shaped by it.

CASE STUDY | Online Radicalization

In 2011, Arid Uka, an Albanian Muslim living in Germany, shot and killed two US servicemen on a bus in Frankfurt. Uka had no connection to terrorist groups and no past or present that could indicate any terrorist involvement. When the police studied his internet history, they put together a picture which showed a gradual progression from an initial interest in jihadi content to a growing fascination and eventual engrossment. A few hours before the shooting he had watched a video showing a purported rape of a Muslim woman by US soldiers, leading Weimann (2014) to argue that there is a direct connection between material on social media and radicalization. In February 2015, three teenagers from Bethnal Green in London ran away in order to go to Syria and marry ISIS fighters. The issue of 'jihadi brides' caused considerable anxiety and foregrounded once again the role of social media. These young girls were groomed online through Facebook, Tumblr, Twitter and peer-to-peer social media such as Skype and WhatsApp. In a nuanced account, Nacos (2015) argues that the relationship between social media and radicalization is a complex one, and that especially for 'jihadi brides' one has to take into account the role of gender. For Nacos, research into this topic should examine the role of social media through the lens of parasocial interaction (Horton and Wohl, 1956) and understand young women as a kind of fan community. Furthermore, Sage (2015) draws attention to clear parallels between moral panics on other forms of media, such as television, and panics regarding social media: in the 1980s the UK government banned the voice of Gerry Adams, the leader of Irish Sinn Fein – the political arm of the IRA – from being broadcast on British media for fear of 'radicalizing' or encouraging terrorism. However, if the links between terrorism and media were so clear, then why is it that radicalized persons remain a very small minority of those exposed to them? Do we in fact have any evidence for a correlation between terrorism and social media?

Gill, Corner, Thornton and Conway (2015) argue that existing research on online radicalization suffers, first, from a lack of empirical evidence (which tends to be anecdotal) and, second, from conceptual confusion, as radicalization includes a wide range of online behaviours, from accessing jihadi material to detailing attack plans online. Moreover, Gill et al. (2015) point to the surprising lack of criminological inquiries into this area, although there are established and useful paradigms. Lastly, the literature makes no distinction between different ideological groups, for example Islamic extremists and right-wing extremists. In their own work, Gill et al. (2015) examined the online behaviours of convicted terrorists in the UK and found that in fact the internet did not increase terrorism but mostly played a role as a facilitating tool. They call for a disaggregation of terrorist-related activities and groups. For example, they found that extreme

right-wing terrorists were 3.39 times more likely to learn online than those who had committed al-Qaeda-related crimes. Moreover, right-wing extremists were four times more likely to use online materials in preparation of a violent attack. However, Gill et al. point out that online learning for violent attackers was much more likely to be accompanied by face-to-face interactions with non-violent co-ideologues. In other findings, they report that those targeting property were twice more likely to communicate online, while those targeting the military were less likely to communicate online. In short, these authors conclude that disaggregation, in terms of ideology and actual behaviours, offers a more nuanced understanding of the relationship between new media and terrorism. They also refute the existence of a dichotomy between offline and online behaviour, arguing instead in favour of a continuum along which offenders move on the basis of the kind of activity they are plotting. This kind of empirical research shows that any kind of blunt policy instrument (e.g., mass surveillance) is unlikely to prove helpful. More nuanced and targeted intervention is necessary in a variety of domains – schools, neighbourhoods and online environments.

Recently, social media corporations, alongside several authors and policy makers, have focused on the production of counter-narratives, aimed at taking apart terrorist and hate messages. Bartlett and Krasodomski-Jones (2015) studied the creation and effectiveness of bottom-up attempts to counter hate speech and extremist ideology, concluding that community-based counter-speech may constitute an important tool in the fight against extremism. Archetti (2015), however, is quick to note that just as no single narrative can trigger a terrorist act, no single communication can counter hate and terrorism. Rather, she argues that the whole communicative environment needs to be taken into account, looking at specific communities and individuals, their identities, their significant and relevant others, opinion leaders, and so on. In the end, she argues, 'a community-based approach and close attention to the consistency between our narrative (words) and our policies (deeds) are in the end the most effective tools against extremism' (Archetti, 2015: 56).

Economics: Fraud and Deception

While in cyber-conflict we discussed attacks aimed at political targets, the economic dimension reveals a wide arsenal of cyber-tools aimed at defrauding and deceiving people for monetary gains. The relationship between new media technologies and economics was discussed in Chapter 3, in which we placed developments in the context of informational capitalism. In this section, however, we will focus on the underbelly of online economics, which shows its vulnerability to attacks motivated by financial gains. Ranging in sophistication from email scams

to trojans and other high-tech tools to defraud, one thing is for sure: online fraud is here to stay and it proliferates even as we speak. To understand the range of this kind of crime and the role of new technologies, this section relies on a crucial distinction between cyber-enabled and cyber-dependent crime. In theoretical terms, the main argument here is that although fraud has always been a part of capitalism, its online counterpart is linked to developments concerning the erosion of trust and the rise of risk, thereby feeding into other 'dark' developments, such as surveillance and conflict.

Cyber-enabled and cyber-dependent crime

In their work reviewing evidence for cyber-crime, McGuire and Dowling (2013) make a distinction between cyber-dependent and cyber-enabled crime. Cyber-dependent crime refers to new forms of crime that can only be committed through a computer and/or through access into networks. The main types of cyber-dependent crime are hacking, DDoS attacks and the spread of viruses. In contrast, cyber-enabled crime refers to traditional crime that can increase in scale or reach – mainly including fraud and theft. This section will outline some of the varieties and instances of these two broad categories of crime and will seek to discuss some of their consequences.

As we saw earlier, hacking and DDoS attacks, as well as the construction of viruses, can be used politically; they can play an important political role symbolically and materially. However, we will focus on the criminal use of these, which are mobilized in the service of personal gain for the instigators. Hacking into computer networks to release information can have important political consequences, even if it is an illegal act, but hacking into personal or corporate accounts in order to access people's bank accounts is motivated by financial gain.

Several high-profile hacks have been documented in the last few years, resulting in significant losses for banks and companies, which are then likely to be passed onto customers. While such attacks are not uncommon, companies that have fallen victim are reluctant to make the attacks public because of the loss of customer confidence. There is therefore a tendency to downplay the intrusions and their impact. Examples of high-profile hacks include the Target hack of 2014, which saw hackers obtain details of 70 million Target customers and in which 40 million credit and debit card details were compromised (Perez, 2014). In the UK, an estimated 157,000 customers of the telecoms company TalkTalk had their credit and bank details stolen when the company was hacked in 2015, resulting in a massive loss of profit and customers (BBC, 2016).

The spread of malware is the main form of cyber-dependent crime. The three main types of malware include viruses, worms and trojans. Viruses are self-replicating programs that spread between computers but which require human action to trigger them – users have to open a file that is infected by a virus. Viruses can lead to significant destruction in computer systems and loss of files and data. In contrast, worms do not need a host and can spread through accessing websites or networks, peer-to-peer file exchange systems, and so on. Worms can then cause disruption or they can control computers remotely, stealing personal

information or turning computers into 'zombies', which can subsequently be used for DDoS attacks or to send spam. Unlike viruses and worms, trojans are not self-replicating but look like legitimate files that users are tricked into downloading and executing. Trojans are used for similar purposes as viruses and worms, to gain access to personal data, including online banking passwords and other information in users' computers.

Cyber-enabled crime can be more low-tech, though there are increasingly sophisticated variants. Early scams, such as the 419 scam, named after Section 419 of the Nigerian Criminal Code (Capp 777 of 1990) that prohibits advance fee fraud (Longe et al., 2009), still exist, alongside more sophisticated attempts to entice users to part with their passwords or other sensitive data. Phishing, spoofing or pharming are all different kinds of scams used to get passwords, card or other details. In most cases, this type of fraud relies on social engineering methods, which take advantage of people's trust or belief in authority, use urgent calls for help or winning notifications to exploit people's curiosity, and so on. One of the most common forms of cyber-enabled crime affects e-commerce, where customers use their credit cards without being present in person. Such fraud may use fake websites to get credit card numbers, sometimes mimicking well-known sites or offering bargain prices for luxury goods. These types of fraud proliferate despite the increase in awareness and the widespread use of verification systems and other means of fraud detection.

While these two categories of crime are analytically distinct in practice, they can be combined. For example, fraudsters can use the telephone to get computer users to download a virus, and then hold them to ransom, asking them for money to return their files and data. The proliferation of all kinds of cyber fraud has an enormous cost. A recent study by Juniper Research estimates that the cost of these crimes will rise to $2.1 trillion by 2019, as e-commerce grows and as new forms of payments, for example through mobiles, are introduced (Juniper Research, 2015). Fraud and the threat of fraud have also given rise to new ways of managing these, so that, for example, the cyber insurance industry is expected to grow from $2.5 billion in 2015 to $7.5 billion by 2020, while projections for the growth of cyber-security products and services estimate a rise from $75 billion in 2015 to $175 billion by 2020 (Morgan, 2016).

Risk, Trust and Security: More Surveillance?

On a more abstract level, this kind of economic fraud and deception seems to link directly with other 'dark' aspects, such as that of surveillance and control. In proliferating the methods of deception, the new media have fed into the erosion of trust, one of the key characteristics of the risk society. Ulrich Beck, who coined the term 'risk society', summarized neatly the relationship between risk and trust: 'The discourse of risk begins where trust in our security and belief in progress end' (Adam, Beck and van Loon, 2000: 213). In these terms, hearing and learning about such fraud and scams damage our trust in the system and raise the risk associated with online environments. The upshot is that we more than welcome attempts to police such environments, and are prepared to submit to methods of surveillance 'for our own protection'.

The other side of the same coin is that eventually such fraudulent behaviour may actually lead to open conflict. We must keep in mind that although the above discussion was focused on individual victims of fraud, there is another more dangerous world of online corporate fraud, which includes industrial espionage and corporate identity theft. Indeed, by spoofing authentic websites, and by scamming individuals who then pass on the costs of fraud to their insurance or to their banks, firms are already involved in online fraud. But there are cases of firms becoming involved in fraud not as victims but as perpetrators, using online means to spy on their competitors. By far the largest and most interesting case is the Google versus China affair that took place in late 2009–early 2010. When Google decided to enter China in 2006, it promised to abide by the Chinese rules of the game, which included censorship of certain politically sensitive keywords and sites – a practice known as the Great Firewall of China. This led to Google receiving a lot of flak from people who thought that Google was selling out for profit the internet cyber-libertarian principles of freedom of information. Given Google's compliance with the Chinese government, we can only imagine their surprise when in December 2009, Google fell victim to a cyber-attack that was subsequently linked to China. The attack, which contained code linked to China, is said to be of the Aurora or Hydraq trojan kind, which gives hackers the possibility to run commands on the hacked computers, allowing them to download files and other information stored therein (McMillan, 2010). While the hack attacked other US corporations as well, Google took the attacks personally. It responded immediately by making the attacks public and when, in January 2010, the attacks were openly linked to China, the US government via its Secretary of State, Hillary Clinton, called for a thorough investigation into the matter. On 22 March 2010, Google decided to effectively leave China by relocating to Hong Kong and exiting the Great Firewall. The decision, which involves economic and strategic losses for Google given the size of China's market, also reflects an internal dilemma for Google, as Sergey Brin, one of its founders, is a vocal advocate for freedom of speech (Johnson, 2010). On the other hand, more recent evidence suggests that Google has never in fact left China: Google Analytics, which obtains data on websites' traffic and visitors, was found to operate beyond the Great Firewall, collecting and transmitting analytics on Chinese websites (Repnikova and Libert, 2015).

Another side of this conflict reveals the tensions involved: in April 2015, Google decided to refuse to recognize security certificates issued by the China Internet Network Information Center (CNNIC), China's internet authority, which means that users of Chinese sites will be given a security warning message (Kharpal, 2015). This shows that while Google may be prevented from accessing the Chinese market, it can retaliate by preventing or obstructing access to Chinese websites from elsewhere in the world. This case represents an increasingly complex situation unfolding in cyberspace: an intermingling between strategic and political interests, technological know-how, and high economic stakes. In this sense, it is not strictly speaking a case of fraud or deception, but it involves the mobilization of technological know-how for economic and political purposes. While China seeks to control the access of its citizens to cyberspace, the US is seeking to consolidate its position as a global leader in human rights advocacy and protection, and Google to protect its reputation and 'Don't be evil' mantra as well as its commercial interests. At the same time, some see China as being

involved in industrial espionage in a move to ascend into a higher position in industrial design and production (see, for instance, Homeland Security Newswire, 2010a). All these cases show the inevitable cross-overs between economics and politics but also directly feed into other practices, such as increased surveillance and control. For example, as soon as Google realized it was being hacked it contacted the US National Security Agency (NSA) in order to draft an agreement which includes data sharing between the two organizations (Homeland Security Newswire, 2010b). This may involve Google handing over data upon NSA requests, and these data may include personal emails and other personal information. From this point of view, political cyber-conflict and economic cyber-fraud and espionage feed directly into practices of surveillance and control over cyberspace. Is this the case for 'dark' cultural practices? We will examine this question in the next section.

Culture: Online Porn

This discussion must begin with a short justification of the rise of online pornography as one of the negative outcomes of the new media. Pornography has had a long history of being debated within feminist circles as well as more broadly in society: Might not porn just represent a human tendency towards appreciation of the erotic? Must we always view women as victims, when some sex workers themselves feel they are in control of their sexuality? What about issues of freedom of speech? These are debates that have not been resolved, and are not likely to be in the near future, but the internet and the new media have in some ways exacerbated these dilemmas by making porn freely available in online environments.

Paasonen (2010) found that estimates of the prevalence of online porn vary considerably, ranging from 3.8% to 80% of all internet traffic – the variation is attributed to the different times as well as the different agencies involved in the measurement. Thus, in the early–mid-1990s, online porn was more prevalent, while in later years, with a wider demographic using the internet, the numbers fell. Similarly, filtering software sites or conservative family organizations tend to exaggerate the incidence of online porn, often making no distinction between erotic poems, hardcore porn and sex education (Paasonen, 2010). Moreover, online porn-related content may range from extreme sadomasochist (SM) and violent porn to alternative erotica, referred to as altporn (Attwood, 2007; Paasonen, 2010), and porn catering to diverse sexualities, queer, alternative body types, and so on, referred to as netporn (Jacobs, Janssen and Pasquinelli, 2007, in Paasonen, 2010). Finally, the production of online porn may range from professional and commercialized to artistic and writerly, and may include user-generated amateurish porn content, as found in YouPorn, the pornographic version of YouTube. The extent of this variety in prevalence, content and production makes any generalized conclusions regarding porn difficult.

But it should be clear that not all of these categories may be seen in negative terms. This section is concerned with online/new media-related practices that introduce a negative, exploitative dynamic that may disrupt and otherwise dislocate flows of culture and cultural expression. In this instance, this translates to a disruption of broadly accepted cultural

conventions on sexuality, and/or the cases in which people are seriously harmed in both a physical and an emotional and psychological manner. Thus, while porn is often linked to moral panics (Kuipers, 2006), the exaggerated view that it always leads to sexism or violence against women or that it undermines the morality of the family is not warranted by all porn content. On the other hand, there are instances of extremely violent and disturbing pornography in which people are clearly exploited. It is this kind of exploitation that places online porn in the 'dark' side of cyberspace. In a sense, this is a modified form of Catharine MacKinnon's *mala in se* (evil in itself) argument that pornography is violence against women, and that women are coerced into this exploitative industry. From this point of view, we will discuss violent and paedophile porn as two instances of problematic porn, and examine its articulations with the new media.

In April 2003, police in West Sussex, UK, discovered the body of a 31-year-old music teacher, Jane Longhurst, who was strangled with a pair of tights. Her body was hidden for weeks before it was found. In March 2004, Graham Coutts was convicted of her murder and sentenced to 26 years in prison. Coutts, a 35-year-old musician, admitted he had a neck fetish and that he had used internet porn sites involving asphyxial sex and strangulation for about eight years (BBC News, 2004). During his trial it emerged that 86% of the pornographic images found in Coutts' computer were violent, often showing naked women with ligatures around their necks. The prosecution in the trial showed evidence that Coutts had visited websites advertising violent 'snuff movies' the day before the murder. Although there is no proof that violent porn led to this murder, the victim's mother, Liz Longhurst, campaigned against this kind of internet porn. She argued that the government must 'take action against these horrific internet sites, which can have such a corrupting influence and glorify extreme sexual violence' (BBC News, 2006a). Furthermore, Liz Longhurst argued that most women appearing in these images are not consenting adults, but trafficked and exploited women (in Murray, 2009). From this point of view, the production of such images is a violent crime. Although in the UK it is considered a crime to produce and distribute violent porn, new laws have made it illegal to possess images that are or appear to be violent or life-threatening and which may lead to severe injury. Section 63 of the Criminal Justice and Immigration Act 2008 criminalizes the possession of images depicting violent sex, bestiality and necrophilia. While the extent to which this law is justified may be questionable, many see it as a necessary first step towards controlling and punishing violence against women (see Murray, 2009, for the legal arguments).

Another extremely disturbing case concerned Vanessa George, a 39-year-old from Plymouth, UK. George worked at a nursery, looking after children up to the age of four years old. In June 2009, George admitted 13 charges which included sexual abuse of children and making and distributing indecent images of children (BBC News, 2009). George had befriended an IT consultant and known sex offender, Colin Blanchard, and another individual, Angela Allen. She then began abusing children in her care, taking pictures of the abuse on her phone, which she would then send to her Facebook friends, Blanchard and Allen, who would do the same for George. There is no doubt that the new media have created new opportunities for child abusers, who can produce, distribute and download abusive images in

mere minutes. Although the legal framework for this kind of activity exists, the internet's vast size and geographical spread make it difficult to control either the production or distribution of such images.

In yet another disturbing case, Ashleigh Hall, a 17-year-old British girl, was groomed by a Facebook 'friend' who pretended to be a teenage boy calling himself Peter Cartwright. 'Cartwright' published a photo of a handsome, bare-chested teenage boy, and befriended Ashleigh on Facebook, eventually exchanging text messages and making arrangements to meet in October 2009. In fact, 'Peter Cartwright' was Peter Chapman, a 33-year-old sex offender who lured Ashleigh into his car by pretending to be 'Peter's' father. He then raped and killed her, dumping her body in a gully by a fence. Chapman confessed the murder to police the next day and was eventually jailed for life. The murder prompted Facebook to issue a statement urging people not to meet anyone who has contacted them online unless they know them well, 'as there are unscrupulous people in the world with malevolent agendas' (BBC News, 2010). In this instance, a new medium allowed a predatory sex offender to contact and lure an innocent girl to her death.

A more recent practice that has emerged is that of revenge porn, where disgruntled former lovers send compromising pictures of their former partners to designated revenge porn sites or even to their family and friends. The impact on the victims is clearly immense, but more broadly, as Filipovic (2013) argues, revenge porn is a form of misogyny aimed at humiliating and degrading women, who are the main victims of this crime. Courts tended to agree with this view, finding that posting pictures without consent constitutes an illegal act. High-profile cases such as that of Kevin Bollaert in the US are seeking to turn the tide against such practices. Bollaert operated a site called ugotposted.com, which allowed anonymous postings of nude photographs without the consent of those depicted. He also operated another site, changemyreputation.com, where he charged victims in order to remove their photos. Bollaert was found guilty and sentenced to 18 years' imprisonment in 2015. Revenge porn is now outlawed in the UK and in some US states, but there are still ways that perpetrators can post revenge porn. In a variation of the crime, some people superimpose a victim's picture on pornographic scenes and then post this in social media. In a case that sparked anger in the UK, the police decided not to bring a criminal case against a 36-year-old man who had taken photographs of a 15-year-old girl from her Facebook account, superimposed them on explicit porn pictures, and posted them on a porn site where users can comment and rate them (Laville, 2016).

New Media and Sexual Aggression

In general, there is little doubt that new media technologies have created a new environment of opportunities for predators of all kinds. Donna Hughes (2002) argues that the articulation of new technologies with a broader ideology of sexism and violence against women create an explosive combination that leads to violence and other forms of sexual exploitation. This is happening either directly, in cases where women and other vulnerable groups such as children are coerced into having sex, are raped and assaulted, and then videos of these acts are

sold or posted online for the gratification of others; or indirectly, through the mainstreaming of pornography, which in turn fuels more violence and exploitation. Hughes further attributes this to the proliferation of internet porn, which, she argues, intensifies competition leading to the production of even more extreme and degrading sex scenes. Equally, the new media have given rise to a massive growth of child pornography: older media, such as cameras and analogue videos, were expensive and difficult to use and reproduce, while the main distribution medium was 'snail mail'. The new media have revolutionized both production (digital cameras, scanners, phone cameras and other digital recording media being used to capture pornographic images of children) and distribution (the internet can reach an unprecedented number of people). Moreover, the new media have offered new opportunities to paedophiles to contact and groom children, who are sometimes accosted in chat rooms and asked to pose and send photographs, or they even try to meet them. Finally, pimps and traffickers use the internet to advertise their 'wares' and find customers.

The relationship between the new media and sexual aggression is therefore fourfold. First, it involves the actual physical and emotional harm of people who are filmed in extreme scenes. Second, it offers an unprecedented ease of production, distribution and access to extreme and violent porn. Hughes cites a consultant who says that before the advent of the new media, sexual predators had to remove themselves from their community by three levels: they had to physically go somewhere, then they had to know where to go, and then they had to know where to find the extreme images to meet the sensations they sought (Hughes, 2002: 139). Third, the proliferation of extremely violent pornographic images may contribute to the rise in violent crimes against people, such as the kinds of rapes and murders we discussed above. Finally, the new media offer the opportunity to sexual predators to contact and groom vulnerable people in online environments such as chat rooms and social networking sites.

In other studies, researchers have highlighted the kind of cultivation effect that online porn may have on culture. Dines (2010) argues that one of the effects of the online proliferation of pornography has been the mainstreaming of porn, which in turn has important implications for how women and men understand and construct their sexualities. For Dines, online porn is a multi-billion industry that relies on the exploitation of those taking part in it and which reproduces dominant masculinist tropes of sexuality. Similarly, Atkinson and Rodgers (2015) view extreme porn as a site of cultural exception, which ends up denying the humanity of those depicted and any harm caused, while at the same time reinforcing hyper-masculinist socio-cultural values. Atkinson and Rodgers further make use of the notion of drift (Matza, 1967), which refers to the ways in which porn production and consumption move to even more extreme practices of cruelty and callousness over time.

Responses: Surveillance Once Again

The response to the kind of synergy created between the new media and sexual aggression and exploitation is in turn twofold. First, it takes the form of the development of a legal framework that addresses the challenges of the new media. Here, for instance, we can place the banning of the possession of violent porn images, as discussed above. Most countries also

ban not only the production but also the possession and distribution of sexual images of children. Other developments include an amendment passed in 2006 in the UK Data Protection Act. This allows credit card companies to withdraw credit cards from customers who use them to purchase child pornography on the internet (BBC News, 2006b). The second form of response is a technological one. Special filters and tracking software have been developed with a view to protecting vulnerable people such as children from accessing porn sites, and in order to track consumers and users of online child pornography. Net Nanny, Safe Eyes, CYBERsitter and others are just some of the filtering software programs that have been developed with the specific agenda to prevent access to porn, but they may go further than this: they may allow parents to follow their child's activities on social networking sites, to prevent access to P2P (peer-to-peer) sites, to block chat rooms, and so on. In 2005, Microsoft Canada, along with the Royal Canadian Mounted Police and the Toronto Police Service, developed CETS (Child Exploitation Tracking Software), which allows police agencies to collect and process large volumes of information, and to cross-reference and use social network analysis to identify offenders. In March 2010, a US software program called the Wyoming Toolkit allowed police to cross-reference millions of illegal images being shared across the internet and create a map of users accessing and using these images (*Herald Sun*, 2010). Clearly, these responses, albeit helpful in containing to some extent the sexual abuse and exploitation of people, are part and parcel of the broader culture of surveillance and security in online environments. In these terms, safety relies once more on surveillance and monitoring.

Conclusions

This chapter explored some of the negative dimensions of the new media, revealing the disruptive or even destructive aspects of social, political, economic and cultural flows that can harm the bonds of society and/or persons. We have argued that these negative dimensions are not the result of the technology as such. Although surveillance, conflict, fraud and porn pathologies pre-existed the new media, their articulation with new technologies has given rise to new forms, opened up new avenues, and created new opportunities for disruptive and problematic relationships to operate. Some of these articulations are summarized in the box below.

We have seen the proliferation of surveillance and the appropriation of non-proprietary information; the rise of cyber-conflict and cyber-terrorism, which creates issues of security; the explosion of fraud and deception, which erodes trust and multiplies risk; and the spread of porn pathologies, which objectify and exploits human beings: all can be linked to a rising culture of control. As these forms spread and multiply, governments and people demand more protection and more control over the new media. This control more often than not takes the form of more surveillance, which in turn often takes the form of internalized self-control and the surveillance of others: friends, enemies and even our own children. This consequently feeds into feelings of insecurity and the erosion of trust, creating a kind of vicious circle from which it is difficult to escape. Moreover, all too often control translates into curbs on free speech and the invasion of privacy: is this a necessary trade-off to ensure

safety? This is a pressing question that societies will need to address. For the time being, though, our discussion ends with the observation that the dark side is an inextricable part of the new media and one that we must at some point confront head on.

SUMMARY OF MAIN POINTS

Society

Surveillance:

- Panopticon: one watches many, e.g., CCTVs
- Synopticon: many watch one, e.g., the mass media culture, watching celebrities
- Lateral surveillance: we constantly watch each other, e.g., Google Earth, following people on Twitter
- We associate with other people in a context of mistrust and insecurity
- Information that was non-proprietary, i.e., belonged to none, is now commercially and politically exploited

Politics

Cyber-conflict and -terrorism:

- Distributed denial-of-service (DDoS) attacks
- Domain Name Service (DNS) attacks
- Worms and trojans
- Unauthorized intrusions (hacks)
- Contributes to an environment of increased risk and insecurity

Economy

Cyber-fraud and deception:

- Cyber-dependent crime
- Cyber-enabled crime
- Articulation of economic with political conflict, e.g., the Google China affair
- Feeds into more surveillance and demands for policing and control

Culture

Violent and extreme porn:

- New modes of production and distribution of (extreme) porn
- New categories, such as revenge porn
- New media allow sexual predators to groom vulnerable people online

- Internet violent porn may lead to actual physical violence, rape and murder
- People are actually hurt in the production of violent porn
- Increase of reach of legal controls
- Development of filtering and tracking software
- Both feed into culture of control and surveillance

RESEARCH ACTIVITY

The goal of this research activity is to help readers understand that online security is primarily a matter of self-control and limitation. Are readers aware of how much information can be collected about themselves? In this activity, readers are asked to imagine themselves as a detective trying to find information about themselves through whatever is available publicly. What kinds of information do they find? Are readers surprised by what they find? Will this have any implications regarding their future online behaviours?

Further Reading

The aim of selecting this list of articles is to explore the various dimensions of security, surveillance and safety as they emerge through our engagement with the new media. Greg Elmer's article highlights some of the new ways in which panoptic surveillance works through the new media, with users-consumers continuously supplying information which becomes immediately integrated into an information processing system, which then feeds it back to us. The results? Eventually, loss of differentiation and diversity as well as 'punishment' of any transgressive behaviour. On a somewhat different note, Giselinde Kuipers reminds us that some cultural elements that are considered dangerous by some are in fact quite acceptable to others. This social construction of digital dangers must be kept in mind before we embark on any kind of moral crusade. Combining insights from surveillance theories as well as taking into account the constructedness of many online threats, Torin Monahan's article, which looks at identity theft, shows that the neoliberal paradigm leads to more self-monitoring, surveillance and self-discipline. In the final article, O'Callaghan et al. show how the algorithmic regulation of online platforms, and specifically systems of recommendation, may be pushing users into more extreme positions.

Elmer, G., 2003, A diagram of panoptic surveillance. *New Media & Society*, 5(2), 231–247.

Kuipers, G., 2006, The social construction of digital danger: debating, defusing and inflating the moral dangers of online humor and pornography in the Netherlands and the United States. *New Media & Society*, 8(3), 379–400.

Monahan, T., 2009, Identity theft vulnerability: neoliberal governance through crime construction. *Theoretical Criminology*, 13(2), 155–176.

O'Callaghan, D., Greene, D., Conway, M., Carthy, J. and Cunningham, P., 2015, Down the (white) rabbit hole: the Extreme Right and online recommender systems. *Social Science Computer Review*, 33(4), 459–478.