31

The governance of cyberspace

Lennon YC Chang and Peter Grabosky

1. Introduction

The challenge of discouraging undesirable conduct in cyberspace is, in many respects, similar to the management of misconduct 'on the ground'. In terrestrial space, most social control is informal. Cultures—whether they are cultures of indigenous peoples or of the modern university—have their social norms, to which most of their members adhere. Minor transgressions tend to elicit expressions of disapproval, while more serious misconduct may be met with ridicule, ostracism, some form of 'payback' or expulsion from the group or organisation.

With the rise of the modern state, formal institutions of social control have evolved to provide rules of behaviour, forums for the resolution of disputes between citizens and institutions for policing, prosecution, adjudication and punishment of the most serious transgressions. However, it is now generally accepted that governmental agencies of social control are neither omnipresent nor omnipotent, thus creating a demand for supplementary policing and security services. These state institutions are accompanied by a variety of non-state bodies that 'coproduce' security. Such entities vary widely in size and role, from large private security agencies and the manufacturers and distributors of technologies such as closed-circuit television (CCTV), to the good friend who keeps an eye on her neighbour's house at vacation time.

This wider notion of policing terrestrial space has been nicely articulated by scholars such as Bayley and Shearing (1996) and Dupont (2006) (see also Brewer, Chapter 26, this volume).

Cyberspace differs only slightly from terrestrial space in its response to antisocial behaviour. Most of us who use digital technology do the right thing not because we fear the long arm of the law in response to misconduct, but, rather, because we have internalised the norms that prevail in our culture (on compliance generally, see Parker and Nielsen, Chapter 13, this volume). Most of us take reasonable precautions to safeguard things of value that might exist in digital form. Nevertheless, because there are deviant subcultures whose members do not comply with wider social norms, and nonchalant citizens who are careless with their digital possessions, there is a need for formal institutions of social control in cyberspace. So, too, is there a need for the coproduction of cybersecurity.

One characteristic of cyber-deviance that differs significantly from terrestrial misconduct is that cross-national activity is much more common. Very early on in the digital age it was said that 'cyberspace knows no borders'. The nature of digital technology is such that one may target a device or system physically located on the other side of the world just as easily as one in one's own hometown. A successful response to transnational cybercrime thus requires a degree of cooperation between states—cooperation that may not be automatically forthcoming.

The governance of cyberspace is no less a pluralistic endeavour than is the governance of physical territory. This chapter will provide an overview of regulatory and quasi-regulatory institutions that currently exist to help secure cyberspace. In addition to state agencies, we will discuss a constellation of other actors and institutions, some of which cooperate closely with state authorities and others that function quite independently. These range from large commercial multinationals such as Microsoft, Google and Symantec; other non-governmental entities such as computer emergency response teams (CERTs); groups like Spamhaus and the Anti-Phishing Working Group; and hybrid entities such as the Virtual Global Task Force and End Child Prostitution, Child Pornography and Trafficking of Children for Sexual Purposes (ECPAT), both of which target online child sexual abuse. In addition, there are independent, 'freelance' groups such as Cyber Angels, which exist to promote cybersafety, and ad hoc, transitory collectives that engage in independent patrolling and investigation of cyberspace.

Other groups, such as Anonymous, and whistleblowers such as Edward Snowden, challenge apparent cyberspace illegality with sometimes questionable methods of their own. Anonymous attacked sites related to child pornography in 2011 (Operation Darknet) and Edward Snowden's disclosures revealed questionable practices by the US National Security Agency.

The next section of this chapter will briefly review some of the more important published works on the social regulation of digital technology. We will then discuss, in order, state, private and hybrid regulatory orderings. The chapter will conclude with some observations on regulatory orderings in cyberspace, through the lens of regulatory pluralism.

2. Literature on the regulation of cyberspace

Current literature on the regulation of cyberspace is no longer focused on whether cyberspace can be regulated. Instead, discussion focuses on how cyberspace *is* regulated and who are the regulators. It is generally conceded that the state cannot adequately control cyberspace via laws and regulations. Even when laws and regulations are kept up to date with developments in technology, the functions and effectiveness of laws and regulations will be limited; the transnational dimensions of much cyber illegality and the architectures of digital technology all but guarantee this (Grabosky et al. 2001; Katyal 2003). Other regulatory methods such as code and system design, self-regulation by the private sector and co-regulation via public and private cooperation have been proposed as alternatives with which to govern cyberspace.

Code and architecture

As pointed out by Professor Lawrence Lessig (1999), the internet was built for research and not commerce. Its founding protocols are inherently unsecure and are designed for the sharing, rather than the concealment, of data. The subsequent devolution of access to the computer network from government and research bodies to individual private users has provided a gateway for cybercriminals and cyber-deviant entrepreneurs.

Lessig (2006) argued that cyberspace is substantially regulated by *code*—computer programming and system architecture. In this book, *Code: Version 2.0*, he notes that the internet is built on simple protocols based on the Transmission Control Protocol and Internet Protocol (TCP/IP) suite. Cyberspace is simply a product of architecture, not of 'God's will'. Lessig argued that the internet is the most regulable space that we know, since, through its architecture, it can reveal who someone is, where they are and what they are doing. When the machine is connected to the internet, all interactions can be monitored and identified. Thus, anonymous speech is extremely difficult to achieve.

Lessig (2006) described the code embedded in the software or hardware as 'West Coast Code', as it is usually 'enacted' by code writers on the West Coast of the United States such as in Silicon Valley and Redmond, Washington, the headquarters of Microsoft. It is different from the 'East Coast Code'—the laws enacted by the US Congress in Washington, DC, complemented by state legislation. Although each code can work well alone, Lessig pointed out that the power of East Coast Code over West Coast Code has increased, especially when the West Coast Code becomes commercial. A classic example was seen in 1994 when the US Government enacted the *Communications Assistance for Law Enforcement Act* (*CALEA*). Under this Act, telephone companies are required to create a network architecture that serves well the interests of government, making wire-tapping and data retrieval easier.

Similarly, Katyal (2003) speaks of digital architecture and its relationship to cybercrime. He suggests that the architectural methods employed to solve crime problems offline could provide a template to help control cybercrime. This will become even more obvious as digital technology pervades modern society, and as the divide between the real-space and cyberspace diminishes. Katyal proposes four principles of real-space crime prevention through architecture: 1) creating opportunities for natural surveillance; 2) instilling a sense of territory; 3) building communities; and 4) protecting targets of crime (2003: 2262).[1]

To elaborate, Katyal maintains that current proliferating claims in cyber law are too grand and should not be seen in a binary formula, such as 'open sources are more/less secure' and 'digital anonymity should be encouraged/discouraged' (2003: 2261–2). Based on the architecture

1 As the building of communities and protecting targets of crime focus on collaboration with other institutions, these will be introduced in a later section.

of 'natural surveillance', he argues that open source platforms such as Linux might not necessarily be more secure than closed source software such as Microsoft Windows. Although the open source platform might attract more people to view the code to improve security for reward or to enhance their reputation, only those with a technological background can achieve these objectives. The number of such people is much smaller than the pool of people available for natural surveillance offline. Therefore, Katyal (2003) suggests that a closed platform can be a better security model than an open source platform when natural surveillance is low.

Katyal (2003) also emphasises the importance of territoriality. Territoriality can be easy to define in the real world, however, it is usually hampered by the anonymity of users in cyberspace. He suggests that a 'verified pseudonymity' using Internet Protocol logging (IP logging) would be helpful for law enforcement agencies to identify criminals. IP logging attaches a designated address number to each computer connected to the internet. It can facilitate crime investigation or even deter crime from happening. As some skilled criminals might 'mask' their IP logging, Katyal (2003) suggests that a verified digital identity involving biometric information such as a fingerprint scan might eliminate this concern. He called this 'pseudonymity' as it will not disclose the user's identity online. However, when it comes to crime investigation or prosecution, the government would be able to link the IP logging to a person by matching the biometric information. One notes that this capacity may be directed against human rights activists as well as cybercriminals.

Although both Lessig and Katyal focus on the architecture of code, they have different opinions on the involvement of state power. Katyal (2003) disagrees with Lessig's (1999) fear that if code is to be regulated by government, it will lose its transparency and become an architecture of control. Katyal (2003) argues that freedom of information laws might play an important role in maintaining the transparency of regulation (at least in those jurisdictions where such laws exist). Direct government regulation will also generate effective architecture that provides security and builds both trust and commitment.

Self-regulation/private regulation

Apart from code and architecture, markets themselves can serve as regulatory institutions. Compared with laws enacted by government, 'self-regulation offers greater speed, flexibility, sensitivity to market circumstances, efficiency, and less government intervention' (Gunningham et al. 1998: 52). It has also been regarded as a form of responsive regulation—regulation that responds to the particular circumstances of the industry in question. Commercial activities within the private sector, and the influence they exert on and through markets, are having a significant effect on regulation (Grabosky 2013).

Feick and Werle (2010) observe that voluntary, private self-regulation coordinated the early architecture of the internet. Debate relating to the regulatory arrangement of the internet is divided into two main camps. On one side, some argue there is too much regulation of the internet. They believe that network neutrality rules are unnecessary and dispensable. Others, however, argue for more regulation, particularly of technical infrastructure. Some scholars have even regarded responsible self-regulation as the only legitimate form with which to govern cyberspace (Johnson and Post 1996; Murray 2012).

Three forms of self-regulation are commonly identified (Gunningham et al. 1998: 51): voluntary or total self-regulation (without government involvement), mandated self-regulation (involving direct government involvement) and mandated partial self-regulation (partial government involvement) (Braithwaite 1982). It is quite rare to see pure self-regulation. Most self-regulation has some government involvement in directing, shaping or endorsing the regulation (Tusikov 2016). The Internet Corporation for Assigned Names and Numbers (ICANN) is an example of self-regulation with government involvement. ICANN is a non-profit organisation that operates the internet's Domain Name System (DNS). However, it is contracted by the US Department of Commerce and overseen by the US Government (Murray 2012). Similar situations can also exist at the nation-state level, especially in critical infrastructure industries such as banks, telecommunications and electricity. For example, in 2006, the Internet Society of China, a Chinese Government–endorsed industry association, announced the 'Self-Regulation against Malicious Software' to regulate abuse from malicious software and prevent its spread. Members who signed the self-regulation protocol are required to protect the cyberspace environment and do their best to control malicious software. They also have a duty

to report any malicious software found and to share that information with other companies. Most of the large telecommunication companies and internet service providers (ISPs), such as China Telecom, CNNIC, Yahoo!, Baidu and Sina, signed up to this self-regulation agreement (Chang 2012).

Nonetheless, one can still find examples of regulation of online behaviour without intervention from the state. To tackle online infringement of copyright, the Recording Industry Association of America (RIAA), an association formed by music companies in the United States, conducts its own investigations to locate the IP addresses of those who are illegally sharing music. It then contacts the ISPs to identify the perpetrators and may sue them directly and/or enlist the support of ISPs in controlling offending behaviour (Tusikov 2016). Nonetheless, the RIAA's might is always successful in identifying the user, even though they have no coercive power to force the ISPs to give the information to them (Shiffman and Gupta 2013). This also illustrates the weakness of private regulation.

Distributed security/Wikified crime prevention

For offline crime, police play an important role in investigation and prevention. However, a higher level of cooperation with states, the private sector and even individual users is required to tackle online crime. Governing risk through a national approach is no longer sufficient (Ericson 2007). New approaches need to be taken to secure cyberspace. Brenner (2005) proposed a 'distributed security' scheme to emphasise that government, users (individual and organisational) and computer architects should all share responsibility for cybersecurity. Similarly, Chang (2012) proposes the idea of 'wiki cybercrime prevention' to address the necessity of mass collaboration between the government and the private sector when sharing information on security incidents and establishing early warning schemes.

Brenner (2005) argues that, unlike crime in the real world, cybercrime is not typical one-to-one victimisation. Because of the automation of such crime, cybercriminals can commit a huge amount of crime with very little effort. Due to limited resources and a reactive strategy, law enforcement agencies may not be able to deal with this problem. Brenner proposes four measures to improve law enforcement's reactive strategy: 1) the Convention on Cybercrime; 2) law enforcement strikeback

techniques; 3) civilian strikeback techniques; and 4) more officers. However, she argues that these are not only insufficient to deal with cybercrime, they might also add to the problem, as strikeback techniques might produce collateral damage to legitimate systems in a hospital or a telecommunications company.

Supporting the idea that 'the monopolization of policing by government is an aberration' (Bayley and Shearing 2001: 1), Brenner (2005) contends that it is essential to involve the private sector in responding to cybercrime and in cybercrime prevention. She proposes a new concept—a 'distributed policing strategy'—that relies mainly on active citizens rather than active police. The distributed policing strategy is different from the idea of community policing, as it shifts the focus of law enforcement from reaction and punishment to deterrence and prevention. Normally, community policing focuses on cooperation between police and the public to create a secure place where crime is not tolerated. It is established on the basis that participants want to live in a secure neighbourhood. However, as Brenner argues, this strategy cannot easily be applied to cybercrime prevention, as cybercrime is a distributed crime that has no central and binding focus such as a physical neighbourhood.

Brenner (2005) suggests that, to let civilians be active and responsible for the prevention of cybercrime, obligatory conduct might be more effective than voluntary conduct. An individual user or organisation might be required by law to install security software or to report illegal activity. The alternative is a lengthy hiatus, as it takes a long time to form and internalise a norm that it is everyone's responsibility to prevent cybercrime. Brenner considers that 'do not' laws might be better than 'do' laws, which impose an obligation to take certain preventive measures. 'Do laws' will 'not only impose an unprecedented obligation to prevent cybercrime; they produce criminal activities *even though no crime was committed*' (Brenner 2005: 15, emphasis in original).[2] She also stresses that, as software plays an important role in cyberspace, it should be seen as national infrastructure, rather than as a 'civil product'.

2 For example, internet users are required to set up a password to secure a wireless connection. They will be fined if they fail to do so and unauthorised people take advantage of this open connection to conduct criminal behaviour such as illegally downloading data (see also Grieshaber 2010).

Malicious computer activities are the 'infectious diseases' of the virtual world. They are pandemics and can be hard to control. Therefore, for cybercrime prevention, risk management measures become particularly important in the prevention of malicious activities from spreading and in reducing harm to society. Chang (2012) also emphasises the importance of civilian participation in cybercrime prevention. Learning from infectious disease prevention models, he advocates 'wiki cybercrime prevention'. Chang (2012) argues that cybercrime can easily become a 'chain reaction', as most public and private sectors are sharing the same closed-code software. Therefore, it is important to discover the breach or vulnerability used for the attack and to share this information with other users immediately to reduce damage to society. That is, it is important to develop 'early warning' and 'information sharing' systems.

This is not a completely new idea as there have been attempts to establish models of 'wikified' cybercrime prevention. For example, in 2002, the US *Federal Information Security Management Act* (*FISMA*)[3] established a reporting system to protect both national security and non–national security related computer systems in government agencies (including government agency contractors). In most countries, there are CERTs to deal with reporting and information sharing. However, as the recent experiences of Sony Pictures, Target and Home Depot suggest, when institutions such as banks, large retailers and telecommunications companies share their adverse experiences, they risk reputational damage, administrative punishment, law suits, audits, public shaming and further onerous reporting requirements. These risks might inhibit the willingness to report (Chang 2012). For example, banks might suffer from unexpected audits and be penalised for administrative system or prudential failure, even if the reporting was voluntary. Moreover, existing hydra-headed reporting systems might also discourage reporting. According to Chang (2012), some industries are required to report computer incidents to as many as five competent authorities within a defined time. They would prefer not to disclose the incident to avoid additional work at the very time they are busy fixing the problem.[4] To minimise those concerns, Chang (2012) suggests the reporting should be voluntary, confidential and non-punitive, as is the practice in the Aviation Safety Reporting System (ASRS 2008). If a company's voluntary reporting has successfully prevented malicious cyber activities

3 *Federal Information Security Management Act*, 44 USC § 3541, et seq.

4 For an overview of data breach notification laws in the United States, see NCSL (2015).

from spreading and causing more serious damage, the government should even consider praising or rewarding the reporting company or agency to acknowledge its contribution. Information security companies could be used for intermediation or as a gateway in the reporting system. By reporting through an information security company, victims can have their identity well protected. Furthermore, an incident might be caused by human error or a conflict between software and hardware within the organisation; these can all be resolved before disclosure to avoid alarmist public reaction.

3. Regulatory institutions in cyberspace

The previous section introduced different regulatory methods involving different agents, including state regulatory institutions, private sector bodies and even individuals. This section introduces some important regulatory institutions in cyberspace.

State regulatory institutions

Among regulatory institutions, the most significant are state agencies. No matter which regulatory method is used, there is intervention or involvement from state regulatory institutions. Despite the revolutionary idea that 'code is law', Lessig (2006) demonstrated the importance of law made by state regulatory institutions. Even with self-regulation, one can see the influence of government in the form of constructing, shaping, promoting and/or facilitating self-regulation (Tusikov 2016).

Legislation still plays an important role in combating cybercrime despite some libertarians strongly opposing government use of law and regulation to intervene in the development of cyberspace (Barlow 1996; Goldsmith and Wu 2006; Grabosky et al. 2001; Katyal 2003). However, as mentioned earlier, state regulatory institutions have limitations when it comes to regulating cyberspace due to the decentralisation and de-territorial character of cyberspace. The cross-border character of cybercrime restricts the effectiveness of laws and regulations. Issues such as legal consistency among states and collaboration in investigating cybercrime have been raised (Chang 2012).

International agreements and conventions encourage harmonisation of cyber laws and regulations, and seek to build cooperation among nations in responding to cybercrime. For example, three decades ago, the Organisation for Economic Co-operation and Development (OECD) published *Computer-related Crime: Analysis of Legal Policy*, which emphasised the importance of establishing common criminal law and criminal procedural law to protect international data networks (OECD 1986). From 2001 onwards, the United Nations (UN) has adopted resolutions encouraging its member states to take proper actions against cybercrime. It called on its members to note the Convention on Cybercrime (Budapest Convention) drafted by the Council of Europe. The Budapest Convention is the first and only international convention to encourage harmonisation of cyber laws and regulations, and to build cooperation among nations in controlling cybercrime. It is open to Council of Europe member states and non-member states. It is currently the most accepted convention on cybercrime, with 51 states ratified/acceded as of December 2016 (Council of Europe 2001). Key members include European nations and the United States.

Nevertheless, most countries in Latin America, the Middle East and Asia-Pacific, including Brazil, Russia, China and India, are not signatories to the Budapest Convention because they were not involved in the drafting or, as is the case with less-affluent countries, they lag behind in developing domestic cybercrime laws to the requisite standards (Broadhurst and Chang 2013). This reduces the effectiveness of the convention as it applies to less than half of the world's internet users and, as Archick (2006) argued, most of the 'problem countries' are not actively involved in the convention. In 2012, a new global cybercrime treaty was proposed by China, India, South Korea and a number of other regional countries at the twelfth UN Congress on Crime Prevention and Criminal Justice in Salvador, Brazil. Although the proposal did not gain much support from Western countries, it might provide a good basis for a new, more inclusive convention.

Bilateral and multilateral state–state cooperation

To control cross-border cybercrime, states need to sign agreements with other states covering areas such as substantive criminal law, as well as procedural laws covering such matters as arrest, search and seizure, evidence collection and extradition. These can be bilateral agreements negotiated directly by the respective authorities in two countries or

multilateral agreements or treaties negotiated through international or regional organisations (on the difficulties of multilateral negotiation, see Downie, Chapter 19, this volume). The Budapest Convention was envisaged as being *the* multilateral agreement against cybercrime; however, due to its limited membership, it cannot be regarded as a truly global platform for mutual assistance on cybercrime investigation. Therefore, most states still need to enter into mutual assistance agreements either bilaterally or multilaterally.

Normally, bilateral mutual assistance agreements provide more efficient and reliable bases for cooperation in crime matters than multilateral agreements, as they are negotiated by the two parties based on their mutual trust and confidence in successful pre-existing relationships (Chang 2013). The disadvantage of bilateral agreements is that it can be rather time-consuming to reach agreement with many partner countries. Also, due to political concerns, it may be difficult for jurisdictions such as Taiwan and China or South Korea and North Korea to reach agreement. That said, some collaboration can be seen between Taiwan and China against telecommunications crimes. For example, in an action called 'Operation 0310', 692 suspects were arrested in a joint investigation against telecommunications fraud syndicates in June 2011 (Mainland Affairs Council 2012).

4. Non-state actors

Non-state actors also play important roles in the governance of cyberspace. As in the discussion of code and architecture, self-regulation and wikified cybercrime prevention, here, we can see evidence of non-state actors (see Tusikov, Chapter 20, this volume). Here, we will discuss three crucial non-state actors as regulatory institutions in cyberspace: commercial companies, non-profit organisations and grassroots bodies or individuals.

a) Commercial organisations

Commercial companies, especially information technology companies, are playing critical roles in the governance of cyberspace. Some of them take up the role voluntarily while others are forced to participate under government laws and regulations. As mentioned earlier, Lessig (2006) argued that government can control cyberspace by regulating the code. Similarly, Goldsmith and Wu (2006: 68) remind us not to 'overlook how

often governments control behaviour not individually, but collectively, through intermediaries'. In the real world, doctors and pharmacists are used as gatekeepers to prevent drug abuse and bartenders are given responsibility to prevent their alcohol-affected customers from driving. Internet content providers are asked to take down copyright-infringed music and films, as well as indecent content that may come to their attention. Quite independently of government, the multibillion-dollar information security industry exists to protect the digital assets of its customers.

b) Non-profit organisations

There are also many non-profit organisations that act as regulatory institutions in the cyber world. ICANN, mentioned earlier, is a non-profit organisation that regulates the distribution of domain names. The World Wide Web Consortium (W3C) is a non-commercial collective of volunteer organisations. The work of the W3C has political and regulatory consequences since internet standards are not purely technical, having underlying commercial interests, political preferences and moral evaluations (Feick and Werle 2010).

In the domain of third-party cooperation against cybercrime, CERTs are prominent non-governmental organisations that share information on malicious cyber activities. CERTs are organisations that provide incident response to victims. It not only helps to safeguard information security within one country, but also collaborates with other CERTs at international and regional levels.

There are also other non-profit organisations that deal with different types of issues in cyberspace—for example, Spamhaus, the Anti-Phishing Working Group and ECPAT. In addition, independent groups such as Cyber Angels promote cyber safety and engage in independent investigation of cyberspace.

c) Grassroots bodies

Other groups, such as Anonymous, and individuals such as Edward Snowden, challenge cyberspace illegality with questionable methods of their own. Cyber crowdsourcing—the power of netizens conducting crime investigation by using social networking tools—has been shown to be a formidable form of private regulation. This is especially the case in Asia (Chang and Poon 2016; Grabosky 2013). Cyber crowdsourcing has been

successfully used to identify viruses and malware. The US Government has also been harnessing the power of cyber crowdsourcing to combat cybercrime. It has recently established the 'Neighborhood Network Watch' program, which educates internet users on cybersecurity and encourages them to report suspicious behaviour related to terrorism (Shiffman and Gupta 2013). This can also be seen as 'wiki cybercrime prevention'.

Hybrid regulatory orderings

There are three basic ways by which commercial companies collaborate formally with government as regulators of cyberspace: such cooperation can be commanded by law, it may flow from commercial public–private partnerships or it can be entered into on a pro bono basis by the commercial actor (Ayling et al. 2009). An example of coercive collaboration is the requirement that telecommunications carriers design systems in such a way as to facilitate surveillance by state law enforcement agencies. The *CALEA* legislation noted above is but one example.

Commercial joint ventures have been established between law enforcement agencies and private commercial entities. The New York Police Department (NYPD) and Microsoft jointly developed the 'Domain Awareness System' to track surveillance targets using databases and surveillance cameras around New York City. The system is designed to be licensed for use by other law enforcement agencies, with profits to be shared by the NYPD and Microsoft (City of New York 2012).

The private sector may also provide goods and services to law enforcement agencies free of charge. In 2014, a memorandum of understanding was signed between Microsoft and the Jakarta Police Department to educate the public on the danger of using pirated software. Through the training, they wished to increase awareness and cybersecurity protection for customers and businesses (Cosseboom 2014). Similarly, Intel's McAfee security branch has signed an agreement with European law enforcement to establish joint operations to control cybercrime (Kirk 2014). Such acts of corporate largesse are obviously in the donors' interests. Whether they are entirely consistent with the policy priorities of the recipient is another matter (see Tusikov, Chapter 20, this volume).

Big companies are not the only ones to play a role in governing cyberspace; small and medium-sized companies also contribute via information sharing. InfraGard, an information sharing and analysis effort established by the US Government with business, academic institutions, state and local law enforcement agencies and other participants, is a good example

of how commercial companies can contribute as regulatory institutions to protect cybersecurity. Another example is the Virtual Global Task Force, which provides information, training and investigation in furtherance of child protection. Commercial partners include Blackberry, PayPal and Microsoft.

5. Conclusion

There is no 'one-size-fits-all' prescription for securing cyberspace. Governments differ in their willingness and capacity to contribute to the solution. In situations where states, alone or in concert, are not in a position to ensure cybersecurity, a variety of private and hybrid actors may be able to assist. We refer to these, because of their influence, as *quasi-regulatory* institutions. We have noted how the information security, telecommunications, software and entertainment industries each contribute their own solutions for cybersecurity. Ideally, these will serve the public's interest as well as that of the institution. Individual users also bear some responsibility for managing their own resources and information. Ad hoc collectives also provide quasi-regulatory services at the grassroots.

To the extent that these various regulatory and quasi-regulatory institutions function in an efficient and effective manner, so much the better. Those who continue to look to the state for leadership in cybersecurity are likely to favour a degree of coordination under state auspices. One should, however, be cautious about expecting the state to deliver beyond its capacity. In all but the most draconian jurisdictions, a degree of spontaneity on the part of non-state actors is both inevitable and desirable. This spontaneity may be beneficial when it results in constructive, creative outcomes. But such success is by no means guaranteed. Regulatory space is contested, and resulting relational interactions between institutions are often complex. One must be alert for initiatives that are part of the problem, rather than part of the solution. Institutions and initiatives should be accountable, whether they exist under commercial or private auspices.

The appropriate institutional configuration for cybersecurity will vary over time and place, depending on the security setting in question and the prevailing capacities of individual participants. Efforts by the private sector may in some situations compensate for shortcomings on the part of government. Some states may be in a position to raise the security

consciousness of their citizens, while others are not. But there is little doubt that cooperation across sectors is the general direction in which we should be heading.

Further reading

Coleman, G 2014. *Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous*. New York: Verso.

Gasser, U, Zittrain, J, Faris, R and Heacock Jones, R 2014. *Internet monitor 2014: Reflections on the digital world*, Research Publication No. 2014-17, Berkman Center for Internet & Society, Harvard University, Cambridge, Mass. Available at: thenetmonitor.org/research/2014/.

Lerner, Z 2014. 'Microsoft the botnet hunter: The role of public–private partnerships in mitigating botnets', *Harvard Journal of Law & Technology* 28(1): 237–61.

Zetter, K 2014. *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*. New York: Crown Publishers.

References

Archick, K 2006. *Cybercrime: The Council of Europe Convention*. Washington, DC: The Library of Congress.

Aviation Safety Reporting System (ASRS) 2008. *ASRS Program Briefing*. Moffett Field, CA: ASRS. Available at: asrs.arc.nasa.gov/overview/summary.html.

Ayling, J, Grabosky, P and Shearing, C 2009. *Lengthening the Arm of the Law: Enhancing Police Resources in the 21st Century*. Cambridge: Cambridge University Press.

Ayres, I and Braithwaite, J 1992. *Responsive Regulation: Transcending the Deregulation Debate*. New York: Oxford University Press.

Barlow, JP 1996. *A Declaration of the Independence of Cyberspace*. Davos, Switzerland: Electronic Frontier Foundation. Available at: homes.eff.org/~barlow/Declaration-Final.html.

Bayley, D and Shearing, C 1996. 'The future of policing', *Law and Society Review* 30(3): 585–606. doi.org/10.2307/3054129.

Bayley, D and Shearing, CD 2001. *The New Structure of Policing: Description, Conceptualization, and Research Agenda*. Washington, DC: National Institute of Justice.

Braithwaite, J 1982. 'Enforced self-regulation: A new strategy for corporate crime control', *Michigan Law Review* 80(7): 1466–507. doi.org/10.2307/1288556.

Brenner, SW 2005. 'Distributed security: Moving away from reactive law enforcement', *International Journal of Communication Law & Policy* 9(Spring): 1–42.

Broadhurst, R and Chang, LYC 2013. 'Cybercrime in Asia: Trends and challenges', in B Hebenton, S Jou and J Liu (eds), *Asian Handbook of Criminology*. New York: Springer, pp. 49–64. doi.org/10.1007/978-1-4614-5218-8_4.

Chang, LYC 2012. *Cybercrime in the Greater China Region: Regulatory Responses and Crime Prevention across the Taiwan Strait*. Cheltenham, UK: Edward Elgar. doi.org/10.4337/9780857936684.

Chang, LYC 2013. 'Formal and informal modalities for policing cybercrime across the Taiwan Strait', *Policing and Society* 22(4): 540–55. doi.org/10.1080/10439463.2013.780221.

Chang, LYC and Poon, R 2016. 'Internet vigilantism: Attitudes and experiences of university students in Hong Kong', *International Journal of Offender Therapy and Comparative Criminology*. doi.org/10.1177/0306624X16639037.

City of New York 2012. 'Mayor Bloomberg, Police Commissioner Kelly and Microsoft unveil new, state-of-the-art law enforcement technology that aggregates and analyzes existing public safety data in real time to provide a comprehensive view of potential threats and criminal activity', Press release, 8 August, City of New York, New York. Available at: nyc.gov/portal/site/nycgov/menuitem.c0935b9a57bb4ef3daf2f1c701c789a0/index.jsp?pageID=mayor_press_release&catID=1194&doc_name=http%3A%2F%2Fwww.nyc.gov%2Fhtml%2Fom%2Fhtml%2F2012b%2Fpr291-12.html&cc=unused1978&rc=1194&ndi=1.

Cosseboom, L 2014. 'Microsoft and Jakarta police team up to educate public on dangers of pirated software', *TechinAsia*, 17 December. Available at: techinasia.com/microsoft-indonesia-cybercrime-cybersecurity-pirated-software/.

Council of Europe 2001. *Convention on Cybercrime*. CETS No. 185, opened for signature 23 November 2001, entered into force 1 July 2004. Strasbourg: Council of Europe. Available at: conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG.

Dupont, B 2006. 'Delivering security through networks: Surveying the relational landscape of security managers in an urban setting', *Crime Law and Social Change* 45(3): 165–84. doi.org/10.1007/s10611-006-9033-5.

Ericson, R 2007. *Crime in an Insecure World*. Cambridge: Polity.

Feick, J and Werle, R 2010. 'Regulation of cyberspace', in R Baldwin, M Cave and M Lodge (eds), *The Oxford Handbook of Regulation*. Oxford: Oxford University Press, pp. 523–47. doi.org/10.1093/oxfordhb/9780199560219.003.0021.

Goldsmith, JT and Wu, T 2006. *Who Controls the Internet?: Illusion of a Borderless World*. New York: Oxford University Press.

Grabosky, P 2013. 'Beyond responsive regulation: The expanding role of non-state actors in the regulatory process', *Regulation & Governance* 7(1): 114–23. doi.org/10.1111/j.1748-5991.2012.01147.x.

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

Grieshaber, K 2010. 'German court orders wireless passwords for all', *NBC News*, [online], 5 December. Available at: nbcnews.com/id/37107291/ns/technology_and_science-security/#.VMXMvtKUeSo.

Gunningham, N, Grabosky, P and Sinclair, D 1998. *Smart Regulation: Designing Environmental Policy*. Oxford: Clarendon Press.

Johnson, DR and Post, DG 1996. 'Law and borders: The rise of law in cyberspace', *Stanford Law Review* 48: 1367–401. doi.org/10.2307/1229390.

Katyal, NK 2003. 'Digital architecture as crime control', *Yale Law Journal* 112(8): 2261–89. doi.org/10.2307/3657476.

Kirk, J 2014. 'Intel to work with Europol on fighting cybercrime', *Networkworld*, 19 November. Available at: networkworld.com/article/2850293/intel-to-work-with-europol-on-fighting-cybercrime.html.

Lessig, L 1999. *Code and Other Laws of Cyberspace*. New York: Basic Books.

Lessig, L 2006. *Code: Version 2.0*. New York: Basic Books.

Mainland Affairs Council 2012. *Opening Up and Guarding the Country: Benefits of the 16 Cross-Strait Agreements*. Taipei City: Mainland Affairs Council. Available at: mac.gov.tw/public/Data/2101911582271.pdf.

Murray, AD 2012. 'Internet regulation', in D Levi-Faur (ed.), *Handbook on the Politics of Regulation*. Cheltenham, UK: Edward Elgar, pp. 267–82.

National Conference of State Legislatures (NCSL) 2015. *Security Breach Notification Laws*. Denver: NCSL. Available at: ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

Organisation for Economic Co-operation and Development (OECD) 1986. *Computer-related Crime: Analysis of Legal Policy*. Paris: OECD.

Shiffman, G and Gupta, R 2013. 'Crowdsourcing cyber security: A property rights view of exclusion and theft on the information commons', *International Journal of the Commons* 7(1): 92–112. doi.org/10.18352/ijc.343.

Tusikov, N 2016. *Chokepoints: Global Private Regulation on the Internet*. California: University of California Press.

This text is taken from *Regulatory Theory: Foundations and applications*, edited by Peter Drahos, published 2017 by ANU Press, The Australian National University, Canberra, Australia.