Since January 2020 Elsevier has created a COVID-19 resource centre with free information in English and Mandarin on the novel coronavirus COVID-19. The COVID-19 resource centre is hosted on Elsevier Connect, the company's public news and information website.

Elsevier hereby grants permission to make all its COVID-19-related research that is available on the COVID-19 resource centre - including this research content - immediately available in PubMed Central and other publicly funded repositories, such as the WHO COVID database with rights for unrestricted research re-use and analyses in any form or by any means with acknowledgement of the original source. These permissions are granted for free by Elsevier for as long as the COVID-19 resource centre remains active.
In this chapter, we propose a framework for identifying clear contexts and attendant mechanisms associated with authoritarian regimes’ internet control measures. We build on the concept of the ‘field’ formed around internet control in authoritarian regimes. Viewing cyber-control as an ‘institutional field’ allows us to examine the evolution of regulative, normative and cognitive institutions. We have advanced a model that explains how an institutional field evolves. The findings are broadly consistent with existing theories on field formation. Nonetheless, this chapter has revealed unique processes and mechanisms associated with cyber-control-led field construction and reconstruction in authoritarian regimes.

Introduction

Although more than three dozen governments in the world control their online environment (Mackinnon and Palfrey, 2006), few have done so more skilfully than China. China’s state strategies toward information and communications technology (ICT) have been to balance economic modernisation and political control (Kalathil, 2003). According to Reporters Without Borders, ‘China was one of the first countries to realize it couldn’t do without the internet and so it had to be brought under control’ (McLaughlin, 2005). Arguably, Beijing thus focused its attention on the internet before other developing countries because it spotted a need to maintain control (Yang, 2001; Zhang, 2001). Estimates suggest that tens of thousands of government agents are engaged in various cyber-control activities (Stevenson-Yang, 2006). In 2007, the Chinese government forced the closure of 44,000 websites; some 868 people were arrested on internet pornography charges and
about 2,000 people engaged in activities relating to internet pornography were penalised (e-commercetimes, 2008). According to Reporters Without Borders, 50 Chinese ‘cyberdissidents’ were in prison in January 2008 (Jesdanun, 2008). New regulations, effective from 31 January 2008, require China’s online video providers to censor all video clips with ‘anti-Beijing content’ (Einhorn, 2008). These are labelled by Reporters Without Borders as ‘unprecedented censorship measures’.

In recent years, Chinese authorities have also won agreements from foreign technology companies including Yahoo, Google and Microsoft for filtering and screening out sensitive words (McLaughlin, 2005; French, 2006). In addition to social and political effects, government control of the internet has also been a major concern for the growth of e-business in China (Kshetri, 2007).

Issues related to control of the online environment in authoritarian regimes are important to the interests and objectives of a diverse set of players such as Western governments, human rights groups (e.g. Amnesty International), Chinese dissident groups, Falun Gong, anti-Falun Gong groups and businesses involved in the internet value chain. Perhaps more important is that among these players, who tend to have competing interests and disparate purposes (Brint and Karabel, 1991; Greenwood and Hinings, 1996; Hoffman, 1999), the balance of power and the patterns of interaction are rapidly altering over time. New organisations or populations are entering in the dialogues related to cyber-control and some of the existing organisations are exiting (Brint and Karabel, 1991; Hoffman, 1999: 355). This means that the ‘content, rhetoric, and dialogue’ (Hoffman, 1999: 355) among constituencies that have interests in internet control in China are shifting over time.

A clearer understanding of internet control measures in authoritarian regimes is important from theoretical, managerial and policy standpoints. First, the relation between internet diffusion and the growth of democracy is unclear (Wilson and Segal, 2005). In the USA, for instance, critics are concerned about the internet-led polarisation of the country and argue that the internet’s effect on democracy is unclear (Benkler, 2006). The internet diffusion-democracy nexus, especially in authoritarian regimes, seems to be less clear than it might at first appear. One upshot of such a tendency is that there are some well-founded rationales for and against Western companies’ involvement in internet-related activities in authoritarian regimes, as well as a number of misinformed and ill-guided viewpoints. To take one example, when the French telecom company, Alcatel, began merger talks with Lucent in
2006, some US lawmakers criticised Alcatel's ties with Iran. Alcatel had upgraded Iran's telecom network and provided the country with its first high-speed DSL internet connections (Bremmer, 2006). One view thus held that Alcatel had helped the Iranian regime. Nonetheless, one might argue the contrary, insomuch as wiring the country has allowed Iranians to communicate with one another and the outside world more easily, thus helping to promote democracy in the country (Bremmer, 2006). Why is the relationship between internet diffusion and democracy in authoritarian regimes so unclear? Much depends on the precise circumstances. In particular, whether the internet forces authoritarian regimes to promote democracy or whether it will be controlled like other mass media (Hachigian, 2001; Stevenson-Yang, 2006) has been a pressing theoretical and policy issue that adjoins the larger social and political concerns of democratic society.

In the remainder of the chapter, we first provide a brief review of the theoretical foundation. We then translate the theories within the context and limits of cyber-control in China. Next, we discuss responses of various institutional actors from the standpoint of internet control in China. The final section provides conclusion and implications.

The theoretical framework: institutional field

At the centre of our argument is the concept of the field formed around internet control. Hoffman (1999: 352) argues that a field is ‘formed around the issues that become important to the interests and objectives of specific collectives of organizations’. To put things in context, these organisations include authoritarian governments attempting to control the internet, human rights groups such as Amnesty International, Western governments, professional associations and businesses involved in the internet value chain. Accordingly, the ‘content, rhetoric, and dialogue’ (Hoffman, 1999: 355) among these constituencies influence the nature of internet control measures.

An important point to bear in mind is the ‘evolving’ rather than ‘static’ nature of fields (Hoffman, 1999: 352). Institutional theorists make an intriguing argument as to how a field evolves. It is important to note that an organisational field is a dynamic system characterised by the entry and exit of organisations or populations and/or interaction patterns.
among them (Brint and Karabel, 1991; Hoffman, 1999: 355). Like other ‘issue-based’ fields, internet control can also be viewed as ‘arenas of power relations’ (Brint and Karabel, 1991: 355) in which various players and constituencies with competing interests and disparate purposes negotiate over issue interpretation and engage in institutional war (White, 1992; Hoffman, 1999: 351–2). Institutional evolution thus takes place by an alteration of the interaction patterns and power balances among organisations (Brint and Karabel, 1991; Greenwood and Hinings, 1996; Hoffman, 1999).

As observed above, internet control in authoritarian regimes is not yet fully institutionalised as it is not ‘uncritically accepted’ and is not considered to be a ‘natural and appropriate arrangement’ (Tolbert and Zucker, 1996; Greenwood, Suddaby and Hinings, 2002). Tolbert and Zucker (1996) refer to this as semi-institutionalisation. An important question then is how an idea (e.g. cyber-control) moves from preinstitutionalisation towards full institutionalisation. A valuable lead into this question is provided by Oliver (1991: 151), who suggests that organisational actors’ strategic responses to institutional processes vary from ‘passivity to increasing active resistance: acquiescence, compromise, avoidance, defiance and manipulation’. To put things in context, in China, internet companies’ responses to the government’s pressure to create a controlled cyber environment vary widely. Moreover, some organisations have changed their strategies to deal with government pressures. Among foreign affiliates, Yahoo followed the strategy of ‘acquiescence’ from the beginning, obeying rules and norms, and cooperating with the government. Some portals and search engines such as Google and Altavista, on the other hand, ’defied’ or actively resisted the institutional processes and were blocked in the country in 2002 (Singer, 2002). Put differently, they exited the Chinese cyber-control field in 2002. Subsequently, however, Chinese authorities have won agreements from Google for filtering and screening out sensitive words (French, 2006). For instance, Google in China shuts down when a user looks for sensitive words (McLaughlin, 2005). Google has thus reentered the Chinese cyber-control field.

According to Hoffman’s (1999) model, institutional evolution entails transitions among Scott’s (1995, 2001) three institutional pillars – regulative, normative and cognitive. Building a regulative/law pillar system is the first stage of field formation. It is followed by a formation of normative institutions and then cognitive institutions (Hoffman, 1999).
Cyber-control in China as an institutional field

Formation of regulative institutions

A focus on monitoring and sanctioning rather than rule setting activities

With regard to regulative institutions, the Chinese cyber-control field seems to be concentrated on ‘monitoring, and sanctioning’ rather than ‘rule setting’ activities (Scott, 1995: 35). For Chinese authorities there are a wide range of reasons for prosecuting and punishing individuals for online ‘crimes’ (e.g. protecting the value of Chinese assets exposed to global capital markets, preventing unauthorised political organisation, etc.) (Stevenson-Yang, 2006). Chinese cyber police have intensified their prosecution of internet content violations. A number of democracy organisers, human rights activists, Falun Gong members, scholars and other dissidents have been arrested for their alleged involvement in online crimes (Hachigian, 2001).

Indeed, in China, ‘the law is marginalised and the legal system relegated to a lowly position in a spectrum of meditative mechanisms, while at the same time available for manipulation by powerful sectors within the state and the society at large’ (Myers, 1996: 188). This is even more so for laws related to control on the internet. Most of China’s internet regulations are guidelines only and do not represent formal laws (Shie, 2004). Stevenson-Yang notes:

Published regulations are convenient as a means of expressing policy, but in the end, political policy, not statute, is the true law of the land in China. The case against editors from Southern Metropolis News in 2004 provides an example: the three were convicted of bribery and embezzlement, but their real offenses, it was universally believed, were reporting on Severe Acute Respiratory Syndrome, or SARS [on the internet]. (Stevenson-Yang, 2006)

Compared with other developing countries, China was slow to enact laws to recognise digital and electronic signatures (DES) (Aldrich, 1999). Encryption software, which is an essential component of DES, allows confidential messages to be sent, thus making it difficult, even
impossible, for the government to detect politically and culturally objectionable content transmitted through the internet (Kshetri and Dholakia, 2001).

Cyber-control in China is thus characterised by a lack of clear rules and policies. In early 2002, several foreign search engines, most notably Google and AltaVista were blocked for several days without explanation (BBC News, 2002a, 2002b; Weaver, 2002). Pointing out problems faced by organisations because of a lack of specificity, one business group asked the Chinese government to issue clearer regulations (Kalathil, 2003). Stevenson-Yang notes:

International companies may or may not agree with this set of prohibitions, but they do not generally object to them. Rules, as long as they are knowable and actionable, are easily accepted as a sovereign nation’s prerogative. But the heart of China’s information control system lies in the prescriptive regime – the one designed to manage the process of creating public speech and, above all, designed to ensure that public speech does not have damaging effects. (Stevenson-Yang, 2006)

The state’s entrenchment in the economy

In China, the state’s entrenchment in the economy (Pei, 2006) makes it easier to monitor internet control measures. As of 2001, 70 per cent of large and medium-sized ‘corporatised’ enterprises had Communist Party members on their boards of directors (Pei, 2006). The country’s ISPs are controlled by state-run companies (McLaughlin, 2005). China is thus mediating ownership to capitalise on the internet’s economic benefits and at the same time combat its risks (Hachigian, 2001). A group at the Ministry of Information Industry (MII) coordinates relevant ministries’ efforts in detecting objectionable content and then implements a block. To do this, the group passes the information to the nine state-owned internet access providers that control China’s internet traffic (Stevenson-Yang, 2005).

Development of government ICT capability

To increase the effectiveness of monitoring activities, the Chinese government has also increased its ICT capability. As China is harnessing the network for government use (Hachigian, 2001), its e-government performance is rated ahead of industrial countries such as Switzerland,
the UK, Singapore and Germany (West, 2002). In its e-government activities, the Chinese government employs a variety of ICT tools, such as the short messaging system (SMS); in some cases, these are replacing more traditional media (Kshetri, Dholakia and Awasthi, 2003).

Tens of thousands of government agents pretend to be dissidents and participate in chat rooms, speaking out against the government, thus many internet users are afraid to engage in online conversations on subjects such as democracy, Japan, religion and other sensitive topics (Mallaby, 2006; Stevenson-Yang, 2006). Indeed, China has the largest cyberpolice force in the world (Mallaby, 2006).

Until the late, 1990s, blocking was mostly in the form of access prevention to certain sites. Later, those sites were made accessible but keyword searches on ‘sensitive issues’ were made unavailable. According to the Berkeley China Internet Project, the government hides websites containing phrases such as freedom, democracy, China-liberal, and falun (Foushee, 2006).

Decoupling symbolic and substantive actions

The regulative institutions are also characterised by a decoupling of symbolic and substantive actions. One official, who supervises internet affairs for China’s State Council has said that China’s efforts to regulate web content are aimed primarily at pornography or other content harmful to teenagers and children (Kahn, 2006). In reality, however, access to pornography, despite being technically illegal, is not actually blocked (Los Angeles Times, 1997).

Beijing is also decoupling illegitimate internet control measures from formal structures. It is important to note that organisations’ responses to institutional pressures are not always legitimate. The study by Elsbach and Sutton (1992: 716), for instance, indicated that activist organisations ‘decoupled illegitimate actions from formal organizational structures by performing these actions as anonymous individuals’ or as part of a temporary group operating under different names. As authoritarian regimes tend to have fewer checks and balances to prevent misuse of power (Popov, 2006; Stoner-Weiss, 2006), such regimes are likely to be involved in illegitimate internet control measures. Moreover, because of the anonymity inherent in the internet it is easy to decouple illegitimate internet control measures from formal structures. There are even reports that Chinese authorities send viruses to attack banned sites (Guillén and Suárez, 2005).
Formation of normative institutions

Professions and trade associations are important forms of normative institutions. Savan (1989: 179) defines ‘the professions’ as groups that apply ‘special knowledge in the service of a client’. A profession is also self-regulated by a code of ethics (Claypool, Fetyko and Pearson, 1990) and is characterised by its role as a moral community (Camenisch, 1983). These codes require members to maintain higher standards of conduct than required by law (Backoff and Martin 1991), to help make professional norms visible (Frankel, 1989) and to act as a vehicle to assure the public and clients that members are competent, have integrity, and maintain and enforce high standards (Ward et al., 1993). Apart from convincing external parties of the integrity of the profession, codes play an important role in forcing members to question their values (Meyer, 1987).

Chinese professional associations that are part of the normative institutions related to the cyber-control field seem to have idiosyncratic and unusual features. The government-backed Internet Society of China (ISC), which was formed in May 2001 with more than 130 members, is a highly visible example. ISC is sponsored by network access carriers, ISPs, facility manufacturers and research institutes. The formation of the ISC can be considered as a part of Beijing’s manipulation strategy, that is, a ‘purposeful and opportunistic attempt to co-opt, influence, or control institutional pressures and evaluations’ (Oliver, 1991: 157). To increase their influence, organisations such as the ISC may ‘attempt to persuade organizational constituents to join the organization or its board of directors (Oliver, 1991: 157). The ISC, for instance, asked internet companies to sign a voluntary pledge on ‘Self-discipline for China’s Internet Industry’ that commits them to investigate and block websites with politically and culturally-sensitive content. By March 2002, the pledge had been signed by over 120 internet portals (Stout, 2002). The pledge commits signatories not to disseminate information ‘that might threaten state security or social stability’ (Economist, 2002a).

The ISC’s activities differ drastically from e-business related professional associations in the West. For instance, the UK Mobile Marketing Association issued its code of conduct in December 2003, specifying what times of day mobile marketers can target consumers (Balmond, 2003). Likewise, in the USA, in early 2001, technology-industry lobbyists and consumer and civil-liberties activists including the American Civil Library Association, Electronic Privacy Information Center and Consumer Federation of America circulated a letter to
members of Congress and the president calling for a stronger set of privacy rules (Benson and Simpson, 2001). While these activities are designed to protect consumer privacy, the ISC’s actions have promoted the government’s interest. For instance, Hu Qiheng, chair of the ISC, has defined internet crime to include ‘acts counter to the interests of the Chinese government’ (Crampton, 2006).

Prior research has found that authoritarian regimes tend to hinder the growth of ‘civic organisations’ characterised by equal, voluntary and participatory norms (Putnam, 1993; Un, 2006). Howard (2003: 11–12, 62) has noted that in the former Eastern Bloc, participation in voluntary associations in post-communist societies is significantly lower than in older democracies. In general, in Asian societies such organisations are ‘seen in familial, authoritarian terms rather than in terms of voluntary, supposedly “horizontal” associations’ (Chandler, 1996). In China, special interest groups and non-government entities are loosely organised (Li, Lin and Xia, 2004) and there is little room for these groups to influence national policy-making (Su and Yang, 2000) and transforming the structure and practices of local companies (Shen, 2005).

To better understand organisations’ involvement in internet control measures, we can draw a parallel with Chinese nationalism. Pei (2003) has identified several dimensions of nationalism, including source and bases. In terms of source, he argues that some nationalism is a product of grassroots voluntarism (such as US nationalism) while some is fostered by government elites and promoted by the apparatus of the state (police, military, state-run media). Chinese nationalism is viewed as state-sponsored and an attempt to fill an ‘ideological vacuum’ left by weakening socialism (Christensen, 1996; Oksenberg, 1997; Sautman, 2001). To put things in context, organisations involved in cyber-control measures do not manifest ‘self directed sets of motivations’, as was the case with the US chemical industry’s response to environmentalism (Hoffman, 1999).

Three other key factors strongly suggest that normative institutions related to cyber-control in China tend to be engaged in government-centric activities rather operating from ‘self directed sets of motivations’ (Hoffman, 1999). First, as noted above, the state’s deep entrenchment in the economy raises the interesting possibility that the government can play a critical role (Pei, 2006).

Second, to succeed in China, e-business organisations need to make room for civil servants and high-ranking government officials (Sikorski and Menkhoff, 1999; Einhorn, Webb and Engardio, 2000). It is important to note that most internet regulations are guidelines only and
do not represent formal laws (Shie, 2004). The regulatory vacuum thus makes it important to have good relationships with government officials. For organisations involved in e-business, it is thus important to consider the government’s interest.

Third, the concepts of customer service and privacy, which are the focus of most e-business related professional associations in democratic regimes, are not well developed in authoritarian regimes. Terrill (2005) goes even further, arguing that ‘because China remains an authoritarian state, we cannot know what the Chinese people want’. Organisations involved in e-business in China thus face little or no pressure related to customer service and privacy.

Formation of cognitive institutions

Note that cognitive components represent culturally supported habits that influence behaviours related to cyber-control. Cognitive feedback loops are associated with cognitive programmes that are built on the mental maps of individual decision-makers and thus function primarily at the individual level (Huff, 1990).

More recently, while regulative and normative pillars related to cyber-control as discussed above are still active, a cognitive institutional pillar appears to be forming. For instance, Yahoo defended its decision to hand over information on a journalist, Shi Tao, claiming that the company was following Chinese ‘customs’ (Stevenson-Yang, 2006). These decision-makers are thus giving culture-related arguments (Jepperson, 1991) to justify their internet control measures.

Before we proceed, it is important to note that the idea of internet control severely lacks face validity. Put differently, unlike some fields such as environmentalism in the US chemical industry (Hoffman, 1999), the face validity of internet control is highly disputed. The adoption of an idea such as internet control tends to be less problematic when its elements possess a high ‘face validity’, which results in common agreement among diverse institutional actors concerning the overall utility (Tolbert and Zucker, 1983).

Because of the low face validity, the level of taken-for-grantedness is not highly established for cyber-control and associated activities. As discussed earlier, there are arguments for as well as against Western companies’ involvement in networking authoritarian regimes. A related point is that cyber-control’s taken-for-grantedness is not homogeneous. For instance, while statements from Yahoo chief Jerry Yang and chair of
the ISC, Hu Qiheng, reflect a belief that internet control is consistent with culture, others disagree. Many foreign observers, for instance, were not convinced that Yahoo’s decision to hand over information on the journalist had any thing to do with Chinese ‘customs’ (Stevenson-Yang, 2006).

**Evolution of competing institutions**

Up to this point, we have concentrated on cyber-control-led institutional evolution in China. As noted above, organisations and populations that inhabit China’s cyber-control field are also affected by other sets of formal and informal rules. For instance, anti-censorship companies such as Freegate (Fowler, 2006) and technology multinationals such as Google, Yahoo and Microsoft, which are major participants in China’s cyber-control field, are based in the USA. China’s cyber-control field is thus influenced by competing US institutions, a situation which is worth examining further. Hoffman notes that:

> to fully appreciate the complexity of institutional dynamics, one must analyze specific institutions at the center of an issue-based field and the competing institutions that may lie within the populations (or classes of constituencies) that inhabit that field. (Hoffman 1999: 352)

China’s cyber-control-led institutional evolutions have also triggered changes in competing institutions. For instance, Human Rights in China, a New York-based nonprofit group, has provided financial support to anticensorship companies such as Freegate (Fowler, 2006). Similarly, Amnesty International has accused US-based internet companies such as Google, Microsoft and Yahoo of violating the Universal Declaration of Human Rights in their agreement with the Chinese government to censor internet use in China (US Fed News Service, 2006b). In the USA, the enactment of the Global Online Freedom Act 2006 can be considered as a part of Washington’s ‘controlling tactics’ to ‘establish power and dominance over the external constituents’ (Oliver, 1991: 157). The act has increased the US government’s power over American technology companies. The evolution of formal and informal institutions in Western countries has thus reconstructed the institutional field of cyber-control in China.
Discussion

The nature of the Chinese government’s internet control measures

Economic performance is the single most important basis on which many authoritarian regimes seek legitimacy (Naughton, 1993). The Chinese Communist Party’s (CCP) resilience can arguably be attributed to a combination of political reforms and economic development (Marsh and Dreyer, 2003; Guoguang, 2006). More to the point, the CCP is counting on the information economy to enhance its image. The CCP expects that a richer and more technology-oriented economy might help increase respect for it (Kshetri and Cheung, 2002). In short, China is interested in fostering a network economy to capitalise on the internet’s economic benefits. Hachigian (2001) quotes a senior government official: ‘we in the government think we missed a lot of the industrial revolution. And we don’t want to miss this revolution’.

Even by the late 1990s, internet control techniques in China were ‘blunt’. Internet subscribers were required to register with local security bureaus, enabling government officials to ascertain who was visiting which websites (Rodan, 1998). In an attempt to foster a network economy, this strategy changed subsequently. According to a report from Reporters Without Borders, internet control in China is conducted through ‘a clever mix of investment, technology and diplomacy’ (McLaughlin, 2005). The government-backed ISC is an example of such diplomacy.

It is also important to note that authoritarian regimes’ measures to control the internet are unlikely to catch up with advancements in technologies. On other words, as authoritarian regimes build a better mousetrap, technology companies and savvy internet users come up with better mice. Several examples illustrate this point. For instance, inside many authoritarian regimes, black marketers in cybercafés, universities and private homes are providing access to blocked websites. They typically exploit ‘technological loopholes to circumvent government filters and charge fees for access’ (Palmer, 2005). To take another example, in Vietnam, activists make extensive use of voice-over internet protocol (VoIP) to contact each other, take part in conference calls and live debates, and post recorded voice messages via online forums available on the websites of VoIP providers such as PalTalk, Yahoo! Messenger and Skype (Johnson, 2006). Importantly, the manner in
which VoIP converts conversation to digital bits makes it harder to search for offensive words, compared, for example, with e-mail.

As is the case of China, authoritarian regimes thus need to seek the help of multinationals from the developed world. In China’s case, foreign multinationals are co-opting with the Chinese government in exchange for access to the US$125 billion e-business market.

**Technology companies’ response to the government**

Various institutional actors differ in terms of their powers to affect an organisation’s outcome. The Chinese government, for instance, can exert a higher level of control on China-based technology companies. Their responses can be described as a habit – ‘unconscious or blind adherence to preconscious or taken for granted rules or values’ (Oliver, 1991: 152).

Western technology companies, however, are required to appease a diverse set of competing institutions. These companies thus are required to decouple their responses.

Different theoretical contributions and various empirical studies have led to the accepted view that the exact nature of decoupling is a function of the perception of relative powers of competing organisational and institutional interests (Pfeffer, 1981a, 1981b; March and Olsen, 1989; Oliver, 1991; Zajac and Westphal, 1995; Westphal and Zajac, 1998, 2001). These studies also provide support for the notion that substantial responses cannot be made to appease actors that diametrically oppose one another. More to the point, the substantive response relates to the threat or opportunity associated with the actor that is perceived to be more powerful and the symbolic response relates to the threat or opportunity associated with the actor perceived to possess less power (George et al., 2006).

In this regard, it is important to note that China’s online transactions were estimated at US$125 billion in 2006 (Asia Pulse, 2006). The Chinese government thus possesses enormous power over these multinationals. To gain access to the huge Chinese e-commerce market, Western organisations appear willing to take actions that are non-isomorphic with respect to their home country institutions.

To substantiate this claim, we began by arguing that the Chinese government has built ‘The Great Firewall of China’ with the help of foreign companies such as Cisco Systems (Gutmann, 2002; Shie, 2004).
Cisco also provided China with hardware specifically designed to assist China's cyber police to conduct surveillance of electronic communications (Jasper, 2006). About a quarter of the vendors at the Security China 2000 trade show, many of them foreign firms, were marketing products aimed at enhancing China’s ‘Golden Shield’ (Fackler, 2000). In short, many Western technology companies have chosen ‘to co-opt the source of the pressure’ related to cyber-control (Pfeffer and Salancik, 1978; Burt, 1983; Oliver, 1991: 157).

An important point to bear in mind is that organisational decision-makers may differ in terms of their perception of the relative powers of different organisational and institutional interests. Accordingly, their responses to institutional pressures vary. Among foreign technology companies, Yahoo’s strategy can be described as compliance – ‘conscious obedience to or incorporation of values, norms, or institutional requirements’ (Oliver, 1991: 152). Yahoo chief, Jerry Yang, said that he had to make the decision to help Chinese authorities arrest a journalist in order to do business in China (McLaughlin, 2005). It can, however, be argued that unlike many Chinese technology companies, which may have unconsciously adhered to local rules (Oliver, 1991: 152), the strategy of compliance of foreign technology companies such as Yahoo is consciously and strategically chosen to comply with institutional pressure in anticipation of self-serving benefits or access to resources (Pfeffer and Salancik, 1978; Meyer and Rowan, 1983; DiMaggio, 1988; Oliver, 1991: 153).

In the early 2000s, other foreign companies such as Google and AltaVista responded differently. These companies’ response to institutional pressure related to Chinese cyber-control can be described as ‘avoidance’ (Meyer and Rowan, 1977; Pfeffer and Salancik, 1978; Meyer, Scott and Deal, 1983; Powell, 1988). This can be defined as an ‘attempt to preclude the necessity of conformity’ (Oliver, 1991: 154). Alternatively, the strategy could also be ‘escape’, which entails exiting ‘the domain within which pressure is exerted’ (Oliver, 1991: 155).

It should also be noted that the responses of Yahoo, Google and AltaVista are not socially acceptable in their home country. Threats to resources motivate organisational leaders to conduct broader searches for alternatives that may exist beyond the bounds of social acceptability (March and Simon, 1958; George et al., 2006: 354). Theorists argue that these organisations are likely to lose resources if they adhere to current practices. For this reason, they may undervalue the risks associated with departing from established ways of doing things and with challenging the legitimacy of established ways, and, as a result, attempt to create the
framework for new legitimate forms through non-isomorphic change (George et al., 2006: 354).

Conclusions and implications

The foregoing discussion provides a framework for understanding institutional processes associated with internet control measures in authoritarian regimes. The findings are broadly consistent with existing theories on field formation. Nonetheless, this chapter has revealed unique processes and mechanisms associated with internet control measures in China. The theory presented here has thus filled in some of the gaps in macromarketing literature and other related areas of scholarship.

At this point, we should emphasise that there are some problems associated with the reliance on cognitive and normative institutions. Some institutionalists argue that the distinction between normative and cognitive institutions tends to be 'blurred' (Campbell, 2004) and it is unclear when taken-for-grantedness of social norms becomes high enough to become part of cognitive institutions (Clemens and Cook, 1999). Other have pointed out that there is a poor specification of mechanisms by which normative and cognitive structures affect behaviours of various actors (Hirsch, 1997).

The image that a company presents to external parties is a function of the power those parties have over the organisation (Basu, Dirsmith and Gupta, 1999). With new regulative institutions such as the Global Online Freedom Act 2006, the power that the US government has over US-based technology companies has strengthened. This means that these companies have to work to change their images.

Notes

1. At present, there are more than 150 members, most of which are organisations (see http://www.isc.org.cn/English/).
2. Authorities in Vietnam have blocked access to pro-democracy blogs and websites, and it is believed that e-mails are scanned.