This paper is the original manuscript and has not been revised or edited.
For the final version, see the French translation.

CYBER-CONTROL AND CYBER-ESPIONAGE ACTIVITIES IN THE AGE OF CLOUD COMPUTING: EVIDENCE FROM CHINA

Par **Nir Kshetri**, Associate Professor, University of North Carolina-Greensboro, United State, kshetri1@hotmail.com

For the final version, see the French translation.
"Les activités d'espionnage électronique et de contrôle d'internet à l'ère de l'infonuagique : le cas de la Chine", *Télescope*, Vol. 18, No. 1-2, 2012, pp. 169-187.
www.telescope.enap.ca/Telescope/docs/Index/Vol_18_no_1-2/Telv18n1-2_kshetri.pdf

Abstract: Although about forty governments control their online environments, few have done so more skilfully than by China. This concern is especially pronounced in recent years due to a rapid diffusion and development of cloud competing, which is described as the ultimate spying machine. In this paper, we propose a framework for identifying clear contexts and attendant mechanisms associated with authoritarian regimes' internet control measures. We build on the concept of an institutional 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.

■ INTRODUCTION

Although about forty governments in the world control their online environments China's approach probably representsthe most sophisticated and carefully constructed control of the cyber-space. 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 realise 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). 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 require China's online video providers to censor all video clips with 'anti-Beijing content' (Einhorn, 2008). . In December 2011, China tightened its regulations requiring microbloggers to register for such services using real names. Measures like these are labelled by Reporters Without Borders as 'unprecedented censorship measures'.

Since 2009 the Chinese government also tightened the registration requirements and processes for getting .cn domain names. The new rules do not allow individuals to register .cn domains. To register for businesses,

it is required to submit a copy of the business license. 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).

Cyber-control issues associated with the Chinese government have become more interesting and complex in recent years with a rapid development and diffusion of cloud computing in the country. In this regard, it is important to note that some of the Chinese companies are among the most influential players in the global cloud computing industry (Kshetri, 2011). According to CCID Consulting, China's cloud market was over US$1.5 billion in 2009, which will reach US$10 billion by 2012. It is also important to emphasize that the cloud is described as the ultimate spying machine (Kshetri, 2010a). An obvious danger in an authoritarian regime concerns the possibility that the government may intensify further controls on citizens using this technology (Zittrain, 2009). According to a Foreign Policy survey, 38% of the world's top Internet experts viewed the governments as the biggest threat to the open Internet. 34% of the experts considered corporations as the biggest threat and 15% considered cybercriminals (Foreign Policy, 2011).

To understand a cloud's security risks, consider Google's 2009 report that it had discovered attacks on its infrastructures that originated in China. The company further noted that the attack was part of a larger operation that infiltrated the infrastructures of at least 20 other large companies. Other reports had indicated that the hackers had attacked networks of more than 100 companies (McMillan, 2010). In April 2010, U.S.- and Canada-based researchers published a report that tracked a sophisticated cyberespionage network, which they referred as the Shadow network (Information Warfare Monitor/Shadowserver Foundation, 2010). The targets included the Indian Ministry of Defense, the United Nations, and the Office of the Dalai Lama. The report noted, "Clouds provide criminals and espionage networks with convenient cover, tiered defenses, redundancy, cheap hosting, and conveniently distributed command and control architectures.". Likewise, a China-originated cyberspying operation in 2009, known as GhostNet, reportedly infected 1,295 computers in 103 countries (Hvistendahl, 2010).

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), 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 (Hoffman, 1999).

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). 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. 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. Before proceeding, we offer some definitions. Cloud computing involves hosting applications on servers and delivering software and services

via the internet. In the cloud model companies can access computing power and resources on the 'cloud' and pay for services-based on usage (Kshetri 2011).

In the remainder of the paper, 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

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.

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). 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). Institutional evolution thus takes place by an alteration of the interaction patterns and power balances among organisations (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). Oliver (1991: 151)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 shut down when a user looked for sensitive words (McLaughlin, 2005). Google thus re-entered the Chinese cyber-control field. China's unfavourable environment from the security standpoint, however, again led to Google's withdrawal from China in 2010.

■ CYBER-CONTROL IN CHINA

The nature of regulative institutions

A focus on maintaining powerful grip on the public life and consciousness

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 (2006) 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].

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,b; Weaver, 2002). Pointing out problems faced by organisations because of a lack of specificity, a business group asked the Chinese government to issue clearer regulations (Kalathil, 2003). Stevenson-Yang (2006) 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.

The state's entrenchment in the economy facilitating controls

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 to 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).

In the mobile telecommunications industry, 70% of the operators are state-owned (Zhang & Prybutok, 2005). Compared to the West, Chinese technology companies are more government-centric and less consumer-centric. There are persuasive arguments to support the notion that state priorities come ahead of shareholders' profits for Chinese Telecommunications companies (Kshetri, Palvia and Dai, 2011).

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 short messaging system (SMS); in some cases, these are replacing more traditional media (Kshetri, Dholakia and Awasthi, 2003).

There are reports that 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 (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 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).

The nature of normative institutions

Professions and trade associations are important forms of normative institutions. A profession is 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).

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 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). Prior research indicates that to increase their influence, organisations such as 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, 2002). Likewise, in 2009, China's dominant search engine, Baidu, and 19 other Internet companies received the "China Internet Self-Discipline Award". ISC Officials praised them for their roles in fostering, and supporting "harmonious and healthy Internet development" (MacKinnon, 2012). Note that the Chinese

government has emphasized the importance of a healthy and harmonious cyberspace. In the Chinese context, a healthy cyberspace is one that is "porn-free" and "crime-free" and "harmonious" means that it does not challenge or threaten to destabilize the existing social and political order of the CCP-controlled state.

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 (Precision Marketing, 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).

One result of the weak civil society and strong state is that trade and professional associations are likely to engaging in activities that are likely to promote the CCP's authoritarian agenda. For instance, the ISC announced that it would help strengthen cyber-security orientation of users and Internet companies. If the past actions of the ISC are any indicator, however, its activities are more likely to be prompted by the CCP'S need to maintain the dominance

The U.S. government seems to be concerned that the state and the private sector in China have been working together to develop cyber-attack capabilities. According to a U.S. diplomatic cable released by Wikileaks, from June 2002 to March 2003, China's largest infosec vendor, Topsec reportedly employed Lin Yong, the founder of Honker Union of China (also known as the Red Hackers), as a senior security service engineer to manage training (Espiner, 2010). Topsec was partially funded by the Chinese government and reported to provide training and support service for the PLA (Keizer, 2010).

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 policymaking (Su and Yang, 2000) and transforming the structure and practices of local companies (Shen, 2005). It is also important to distinguish China's private sector's cyber-security measures from those in other countries. In India, the trade association National Association of Software and Service Companies (NASSCOM) has played a critical role in strengthening institutions related to cyber security (Kshetri, 2010b). Private sector actors such as trade associations in China have been notably absent in enhancing cyber-security. This distinctive pattern can be explained with the strong state and weak civil society in China.

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 grass-root voluntarism (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; 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 (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.

The nature of cognitive institutions

It is important to understand the attitudes and mental maps of Chinese citizens and corporate decision-makers. 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 to justify their internet control measures.

A related point is that the Chinese society is conditionally tolerant of the domination of civil society by a strong state. Analysts argue that the fact that China's "post-Tiananmen generation" has experienced little or no hardship has made this generation indifferent to democracy (Hvistendahl, 2009).

The level of taken-for-grantedness, however, is not highly established for cyber-control and associated activities. As discussed earlier, there are views 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 Yahoo chief Jerry Yang and chair of the ISC, Hu Qiheng's statements 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

As noted above, organisations and populations that inhabit China's cyber-control field are also affected by other sets of formal and informal rules of the game. 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 institutions in the USA, which need to be analysed to have a clearer understanding of the field. 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 Chinese government to censor internet use in China (US Fed News Service, 2006). In the USA, the enactment of the Global Online Freedom Act 2006 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

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'.

In this regard, it is important to note that China has shown a willingness to form an astonishing alliance with its traditional rival, Taiwan. It is also relaxing restrictions on its approach to Internet control. In June 2011, China announced an investment of US$154 million to develop a cloud center for high-tech and start-up firms in Chongqing. The cloud computing Special Administrative Region (SAR) will be free of the country's strict internet censorship filters (Russell, 2011). China is also seeking cooperative ventures with Taiwanese manufacturers in various areas of cloud computing (Wang, 2011)

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 is an illustrative of such an approach.

It is also important to note that authoritarian regimes' measures to control the internet are less likely to catch up with advancements in technologies. On other words, once 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 extensively use 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, many foreign multinationals are co-opting with the Chinese government in exchange for access to China's huge e-business market.

Technology companies' responses

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. Many Chinese entrepreneurs returning from the West comply with the government requests to provide filtering technology to the cyber-police. Western technology companies, however, are required to appease a diverse set of competing institutions. These companies thus are required to decouple their responses. The exact nature of decoupling is a function of the perception of relative powers of competing organisational and institutional interests (March and Olsen, 1989). 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, according to China e-Business Research Center and CNZZ Data Center, China's e-commerce market reached $703 billion in 2010, which was 22% higher than in 2009 (Lan, 2011). 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.

Chinese government built 'The Great Firewall of China' with the help of foreign companies such as Cisco Systems (Gutmann, 2002). Cisco also provided China with hardware 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 with the Chinese government.

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, 199), 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.

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). Alternatively, the strategy could also be 'escape', which entails exiting 'the domain within which pressure is exerted' (Oliver, 1991: 155).

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). 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).

■ CONCLUDING COMMENTS

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 paper has revealed unique processes and mechanisms associated with internet control measures in China.

If the recent major cyberespionage activities teach a lesson, it's that countries with strong cyberspying and cyberwarfare capabilities such as China will be in a good position to exploit the cloud's weaknesses for such activities. In the Shadow case, for instance, the cyberespionage network combined social-networking and cloud computing platforms, including those of Google, Baidu, Yahoo, Twitter, Blogspot, and blog.com, with traditional command and control servers (Information Warfare Monitor/Shadowserver Foundation, 2010).

Various aspects of the institutional environment can weaken the cloud's value proposition and discourage investors. In 2008, Google's CEO said that his company would work with Chinese universities, starting with

Tsinghua University, on cloud-related academic programs. The country's unfavorable environment from the security standpoint, however, led to Google's withdrawal from China. A related point is that cloud providers from China might face barriers to internationalization activities, particularly because security is among the most important concerns for cloud adoption. One concern is that the institutional environment in China can't guarantee the security and privacy of client data. The Chinese government's reputation suggests that data stored in a cloud hosted in China might not be safe. These concerns further increase when we take into consideration the possibility of government control of China-based clouds providers.

■ REFERENCES

Aldrich, M. (1999). E-com Legal Guide: China, Baker and McKenzie, Hong Kong, www.bakerinfo.com/apec/chinaapec.htm (page consultée le 11 décembre 2006).

Asia Pulse (2006). China's Online Transactions Seen to Reach US$125, www.bushwatch.com/archive2006/e-mail-20060719.htm (page consultée le 30 avril 2007).

Backoff, J. F. et C. L. Martin Jr. (1991). « Historical perspectives: development of the codes of ethics in the legal, medical and accounting professions », Journal of Business Ethics 10: p. 99-110.

Basu, O., M. Dirsmith et P. Gupta (1999). « The Coupling of the Symbolic and the Technical in an Institutionalized Context: The Negotiated Order of the GAO's Audit Reporting Process », American Sociological Review, 64, p. 506-526.

BBC News (2002a). China Blocking Google, http://news.bbc.co.uk/1/hi/technology/2231101.stm (page consultée le 28 janvier 2008).

BBC News (2002b). Google Fights Chinese Ban, http://news.bbc.co.uk/1/hi/technology/2233229.stm (page consultée le 28 janvier 2008).

Bremmer, I. (2006). « The World is J-curved », Washington Post, 1er octobre, p. B.3.

Brint, S. et J. Karabel (1991). « Institutional Origins and Transformations: The Case of American Community Colleges », dans W. Powell et P. DiMaggio (dir.), The New Institutionalism in Organizational Analysis, Chicago, University of Chicago Press, p. 337-360.

Burt, R. S. (1983). Corporate Profits and Cooptation: Networks of Market Constraints and Directorate Ties in the American Economy, New York, Academic Press.

Camenisch, P. E. (1983). Grounding Professional Ethics in a Pluralistic Society, New York, Haven Publications.

Campbell, J. L. (2004). Institutional Change and Globalization, Princeton, Princeton University Press.

Christensen, T. (1996). « Chinese Realpolitik », Foreign Affairs, vol. 75, no 5, p. 37-52.

Claypool, G. A., D. F. Fetyko et M. A. Pearson (1990). « Reactions to Ethical Dilemmas: A Study Pertaining to Certified Public Accountants », Journal of Business Ethics, 9, p. 699-706.

Clemens, E. S. et J. M. Cook (1999). « Politics and Institutionalism: Explaining Durability and Change », Annual Review of Sociology, 25, p. 441-466.

Crampton, T. (2006). « Innovation may Lower Net Users' Privacy. Embraced by China, New Standard Helps to Trace People Online », International Herald Tribune, 20 mars, p. 1.

DiMaggio, P. J. (1988). « Interest and Agency in Institutional Theory », dans L. Zucker (dir.), Institutional Patterns and Organizations, Cambridge, Ballinger, p. 3-22.

e-commercetimes (2008). China dismantles 44,000 sites in anti-porn offensive, www.ecommercetimes.com/story/China-Dismantles-44000-Sites-in-Anti-Porn-Offensive-61336.html?welcome=1201374030 (page consultée le 28 janvier 2008).

Economist (2002). « Asia: Stop your Searching. The Internet in China », Economist, 7 septembre, p. 68.

Einhorn, B. (2008). 'New regulations for China's YouTube wannabes', available at: http://www.macnewsworld.com/story/web20/61268.html (accessed 26 January 2008).

Einhorn, B., A. Webb et P. Engardio (2000). « China's Tangled Web », Business Week, 17 juillet, p. 56-58.

Elsbach, K. D. and Sutton, R. I. (1992). 'Acquiring organizational legitimacy through illegitimate actions: A marriage of institutional and impression management theories', Academy of Management Journal 35: 699–738.

Espiner, T., (2010). Cable reveals US concerns over Chinese cyber-warfare, ZDNet UK, December 6,http://www.zdnet.co.uk/news/security-threats/ 2010/12/06/cable-reveals-us-concerns-over-chinese-cyber-warfare-40091072/

Fackler, M. (2000). The Great Fire Wall of China?, www.abcnews.go.com/secions/tech/DailyNews/chinanet001108.html (page consultée le

Foreign Policy, (2011). The FP Survey: The Internet, September/October 188, 1-9.

Foushee, H. (2006). « Gray Area: The Future of Chinese Internet », Harvard International Review, vol. 8, no 2, p. 8-9.

Fowler, G. A. (2006). « Great Firewall: Chinese Censors of Internet Face "Hacktivists" in US; Programs Like Freegate, Built by Expatriate Bill Xia, Keep the Web World-wide; Teenager Gets His Wikipedia », Wall Street Journal, 13 février, p. A.1.

French, H. W. (2006). « Chinese Discuss Plan to Tighten Restrictions on Cyberspace », New York Times, 4 juillet, p. A.3.

George, E. et autres (2006). « Cognitive Underpinnings of Institutional Persistence and Change: A Framing Perspective », Academy of Management Review, vol. 31, no 2, p. 347-385.

Guillén, M. F. et S. L. Suárez (2005). « Explaining the Global Digital Divide: Economic, Political and Sociological Drivers of Cross-national Internet Use », Social Forces, vol. 84, no 2, p. 681-708.

Guoguang, W. (2006). « The Peaceful Emergence of a Great Power? », Social Research, vol. 73, no 1, p. 317-345.

Gutmann, E. (2002). « Who lost China's internet? », The Weekly Standard, vol. 7, no 23, 15 février, p. 24-29.

Hachigian, N. (2001). « China's Cyber-strategy », Foreign Affairs, vol. 80, no 2, p. 118-133.

Hirsch, P. (1997). « Sociology without Social Structure: Neo-institutional Theory Meets Brave New World », American Journal of Sociology, vol. 102, no 6, p. 1702-1723.

Hoffman, A. J. (1999). 'Institutional Evolution and Change: Environmentalism and the US Chemical Industry', Academy of Management Journal, vol. 42, no 4, p. 351-371.

Hvistendahl, M. (2009) "The China Syndrome," Popular Science, May, 274, 5, pp.60-65.

Hvistendahl,M.(2010)"China's Hacker Army,"3 March, http://www.foreignpolicy.com/articles/2010/03/03/china_s_hacker_army?page=full

Information Warfare Monitor/Shadowserver Foundation,(2010). Shadows in the Cloud: Investigating Cyber Espionage 2.0, Joint Report: Information Warfare Monitor Shadowserver

Jasper, W. F. (2006). 'Terror in America, Made in China', New American 22(6): 19–21.

Jesdanun, A. (2008). 'China catching up to US in number of web surfers', available at: http://www.technewsworld.com/story/China-Catching-Up-to-US-in-Number-of-Web-Surfers-61292.html?welcome=1201370753 (accessed 26 January 2008).

Johnson, K. (2006). « Voices of Dissent », Time International, 25 septembre, p. 50.

Kahn, J. (2006). 'China says web controls follow the west's lead', New York Times, 15 February, p. A.6.

Kalathil, S. (2003). « China's New Media Sector: Keeping the State in », Pacific Review, vol. 16, no 4, p. 489-501.

Keizer, G. (2010). "Chinese Firm Hired Blaster Hacking Group, Says U.S. Cable," 6 December, http://www.computerworld.com/s/article/9199898/Chinese_firm_hired_Blaster_hacking_group_says_U.S._cable

Kshetri, N. (2007). 'The adoption of e-business by organizations in China: an institutional perspective', Electronic Markets 17(2): 113–25.

Kshetri, N (2010a). "Cloud Computing in Developing Economies", IEEE Computer, 43(10): 47-55.

Kshetri, N. (2010b). The Global Cyber-crime Industry: Economic, Institutional and Strategic Perspectives, May, Springer-Verlag: New York,Berlin and Heidelberg.

Kshetri, N. (2011). "Cloud Computing in the Global South: Drivers, Effects and Policy Measures," Third World Quarterly, 32(6) 995-1012.

Kshetri, N. and Cheung, M. K. (2002). 'What factors are driving China's mobile diffusion?' Electronic Markets 12(1): 22–6.

Kshetri, N. and Dholakia, N. (2001). 'Impact of cultural and political factors on the adoption of digital signatures in Asia', paper presented at the Americas' Conference on Information Systems, Boston, MA, 3–5 August.

Kshetri, N., Dholakia, N. and Awasthi, A. (2003). 'Determinants of e-government readiness: evidence from China and India', paper presented at the First International Conference on E-governance, New Delhi, 18–20 December.

Kshetri, N., Palvia, P., et Dai, H., (2011). "Chinese Institutions and Standardization: The Case of Government Support to Domestic Third Generation Cellular Standard", Telecommunications Policy, 35(5), 399-412

Lan, T. (2011) 'Real Rules for Virtual Space,', Beijing Review,24 November, 54(47):12-13

Li, M., Lin, Z. and Xia, M. (2004). 'Leveraging the open source software movement for development of China's software industry, Information Technologies and International Development, 2(2): 45–63.

Los Angeles Times (1997). 'The cutting edge; testing the boundaries; countries face cyber control in their own ways', Los Angeles Times, 30 June, p. 1.

MacKinnon, R. (2012) 'Inside China's Censorship Machine,' 29 January, http://fullcomment.nationalpost.com/2012/01/29/rebecca-mackinnon-inside-chinas-censorship-machine/

Mallaby. S. (2006). 'Google and my red flag', The Washington Post, 30 January, p. A.17.

March, J. G. and Olsen, J. P. (1989). Rediscovering Institutions. The Organizational Basis of Politics, New York: Free Press.

March, J. G. and Simon, H. (1958). Organizations, New York: Wiley.

Marsh, C. and Dreyer, J. T. (2003). US-China Relations in the Twenty-First Century: Policies, Prospects, and Possibilities, Lanham, MD: Lexington Books.

McLaughlin, K. E. (2005). 'China's model for a censored internet', Christian Science Monitor, 97(210): 1–10.

McMillan, R. (2010). 'More Than 100 Companies Targeted by Google Hackers,'27 February, Retrieved from http://www.computerworld.com/s/article/9163158/More_than_100_companies_targeted_by_Google_hackersMeyer, J. and Rowan, B. (1977). 'Institutionalized organizations: formal structure as myth and ceremony', American Journal of Sociology 83: 333–363.

Meyer, J. W., Scott, W. R. and Deal, T. E. (1983). 'Institutional and technical sources of organizational structure: explaining the structure of educational organizations', in J. W. Meyer and W. R. Scott (eds) Organizational environments, Beverly Hills, CA: Sage, pp. 45–67.

Myers, W. H. (1996). 'The emerging threat of transnational organized crime from the east', Crime, Law and Social Change 24: 181–222.

Oliver, C. (1991). 'Strategic responses to institutional processes', Academy of Management Review 16: 145–79.

Palmer, K. (2005). 'Contrabandwidth', Foreign Policy, 147 (March/April), p. 93.

Pei, M. (2003). 'The paradoxes of American nationalism', Foreign Policy 136 (May/June): 30–7.

Pei, M. (2006). 'The dark side of China's Rise', Foreign Policy, 153 (March/April): 32–40.

Popov, V. (2006). 'Foreign direct investment in Russia: why doesn't it come? Should there be more of it?' Canadian Foreign Policy 13(2): 51–64.

Precision Marketing (2003). 'Mobile industry to clamp down on youth marketing', 12 December, p. 3.

Rodan, G. (1998). 'The internet and political control in Singapore', Political Science Quarterly 113(1): 63–99.

Russell, J. (2011, June 25)., China to develop $154m tech centre free of web restrictions, Retrieved from ⟨http://asiancorrespondent.com/58249/china-to-develop-154m-tech-centre-free-of-web-restrictions/⟩

Sautman, B., 2001. 'Peking man and the politics of paleoanthropological nationalism in China', Journal of Asian Studies 60(1): 95–124.

Scott, W. R. (1995). Institutions and Organizations. Thousand Oaks, CA: Sage.

Scott, W. R. (2001). Institutions and Organizations. Thousand Oaks, CA: Sage.

Shen, X. (2005). 'A dilemma for developing countries in intellectual property strategy? Lessons from a case study of software piracy and Microsoft in China', Science and Public Policy 32(3): 187–98.

Shie, T. R. (2004). 'The tangled web: does the internet offer promise or peril for the Chinese Communist Party?' Journal of Contemporary China 13(40): 523–40.

Singer, M. (2002). 'Google blocked in China', available at: http://siliconvalley.internet.com/news/article.php/1455921 (accessed 11 December 2003).

Stevenson-Yang, A. (2006). 'China's online mobs: the new red guard?', Far Eastern Economic Review 169(8): 53–7.

Stoner-Weiss, K. (2006). « Russia: Authoritarianism without Authority », Journal of Democracy, vol. 17, no 1, p. 104-118.

Stout, K. L. (2002). 'China sites count cost of cyber-control', available at: http://www.cnn.com/2002/TECH/11/03/china.content/ (accessed 11 December 2006).

Su, F. and Yang, D. L. (2000). 'Political institutions, provincial interests, and resource allocation in reformist China', Journal of Contemporary China 9 (24): p. 215-230.

Terrill, R. (2005). « What does China want? », Wilson Quarterly, vol. 29, no 4, p. 50-61.

Tolbert, P. S. et L. G. Zucker (1996). « The Institutionalization of Institutional Theory », dans S. R. Clegg, C. Hardy et W. R. Nord (dir.), Handbook of Organization Studies, London, Sage, p. 175-190.

US Fed News Service, Including US State News (2006). 'Democracy and human rights: Somalia, Mauritania, Internet', 6 July, available at: http://www.europarl.europa.eu/news/expert/infopress_page/015-9503-187-07-28-902-20060629IPR09390-06-07-2006-2006-false/default_de.htm (accessed 30 April 2008).

Wang, L (2011, June 18). China seeks to work with Taiwan in smart devices and cloud computing, Retrieved from ⟨http://www.taipeitimes.com/News/biz/archives/2011/06/18/2003506036⟩

Ward, S. P., Ward, R., Deck, D. R. and Alan, B. (1993). 'Certified public accountants: ethical perceptions, skills and attitudes on ethics education', Journal of Business Ethics 12: 601–10.

Weaver, L. R. (2002). 'Report: China blocks another search engine', available at: http://edition.cnn.com/2002/TECH/internet/09/06/china.internet.block/index.html (accessed 28 January 2008).

West, D. M. (2002). 'Global e-government, 2002', available at: http://www.insidepolitics.org/egovt02int.PDF (accessed 22 June 2003).

White, H. (1992). Identity and Control: A Structural Theory of Social Interaction, Princeton, Princeton University Press.

Wilson, E. J., III and Segal, A. (2005). 'Trends in China's transition toward a knowledge economy', Asian Survey 45(6): 886-906.

Yang, D. L. (2001). 'The great net of China', Harvard International Review 22 (4): 64–9

Zhang, X.,et Prybutok, V. R. (2005). How the mobile communication markets differ in China, the U.S., and Europe. Communications of the ACM, 48(3), 111–114.

Zittrain, J, (2009, July 19) 'Lost in the cloud'. nytimes.com, Retrieved from www.nytimes.com/2009/07/20/opinion/20zittrain.html?bl&ex=1248235200&en=7d30b8c05442733a&ei=5087%0A accessed 1 December 2009.