China & Cyber Sovereignty: The Growing Gap between Political Freedom and Economic Affluence

Karl Althaus, MS, MA
University of South Florida
School of Interdisciplinary Global Studies
4202 E. Fowler Ave.SOC 107
Tampa, FL 33620
USA

Abstract

China balances its cyber interests between political goals – minimal freedom – and economic benefits – maximal freedom.This analysis contrasts China's economic affluence with its political freedom within cyberspace. In particular, its objectives are threefold: (1) discuss China's worldview and its cyberview, (2) examine its policies that limit the use of the internet as opposed to free access to it, and (3) analyze the political implications as it relates to China's restrictions of internet use and its economic freedom. How has China's economic affluence surpassed political freedom and how much will it impact its economic performance? I agree that restricting access to the free Internet harms ideas exchanges and economic development, alike.China's notion of cyber sovereignty – absolute state control of communication – becomes a surveillance blueprint for the first digital totalitarian state.

Keywords: China, cyber sovereignty, political freedom, economic affluence, Internet policies

1. Introduction

The Internet is a pervasive global force that connects every other person in the world. It is contemporaneous in every country in the world and exceeds 3 billion online users (Internet Society, 2015). Its tentacles reach deeply into political, and economical spheres. It has augmented human progress by building societies that drive innovation and bring political progress. Rising data breaches are eroding trust in the Internet and simultaneously are affecting the way governments view cyberspace. Policies are being enacted that are shaping commercial and personal freedoms.The Internet has created a global village of our international system. In general, there are many positive uses of bringing the world together in cyberspace, but there are also negative aspects to it. On the positive side, the Internet enables free speech on a global scale, while on the negative side it can be a mechanism of censorship and surveillance.It heralded the process of globalization in the wake of revolutions in information technology. Over the last decade, the Internet has shaped the ways in which economic interaction has an effect on political outcomes.

The focus of this paper is to contrast China's economic affluence with its political freedom within cyberspace. In particular, its objectives are threefold: (1) discuss China's worldview and its cyberview, (2) examine its policies that limit the use of the internet as opposed to free access to it, and (3) analyze the political implications as it relates to China's restrictions of internet use and its economic freedom.How has China's economic affluence surpassed political freedom and how much will it impact its economic performance?

The Internet is designed to disregard national borders by enabling freely exchanged opinions that are open to everybody. Thus, it has enhanced the interactions between individuals and groups. Nobody needs passport and visa when accessing foreign websites. On the political side, China's government grants very little political freedom to its citizens fearing Western democratic and cultural ideas will undermine its national identity. China introduced the concept of "cyber sovereignty"(Schneier, 2015) that seeks absolute jurisdiction over communication within its borders, and beyond. Furthermore, it adheres to a policy of noninterference in domestic affairs, emphasizes cyber security, and, more recently, expands it program of facial recognition at enormous cost to citizens' privacy.

On the economic side, following its outstanding commercial accomplishments in global trade and manufacturing, China bestows enormous economic cyber freedom to its citizens; provided there is the desire to access it. The main beneficiary of economic growth is the middle class that uses cyberspace as a marketplace. Additionally, China's cyber giants, Taobao, Alibaba, Baidu, benefits from its enormous domestic market, which restricts foreign competition.Therefore, the Chinese government acts unfairly as it restricts access to its "lucrative sectors, while financing assaults on those same industries abroad."(The Economist, 2017)

2. China's Worldview and Cyber view

"China's emphasis is definitely not on civil liberties and political rights as understood in the West. The foremost inalienable right for China is the right to development, defined as promoting economic and social progress or meeting basic human needs."(Conteh-Morgan, 2015) This is a remarkable view as it opposes the United Nation's Universal Declaration of Human Rights, which grants individuals fundamental rights such as freedom of association, liberty, equality, freedom of movement. China values collective rights more than individual rights thereby giving more emphasis to economic and social rights.

Historically, China has no democratic tradition but only dictatorial rule from absolute emperors to its current model of authoritarian capitalism. It institutionalized the teachings of Confucius, which emphasized the value of social hierarchy and personal morality, as the basis for government. Therefore, China adheres to the belief that collectives supersede individuals and no country should impose its own human rights views on China. Curiously, the Chinese constitution guarantees freedoms of speech, assembly, and association, but such rights are subordinated to the state.

Criminalizing digital activity reveals China's cyberview. A law on cyber security, which became effective on June 1, 2017, criminalizes any online information that is viewed as damaging "national honor", "disturbing economic and social order", and contributing to the "overthrow of the socialist system". (Financial Times, 2017) These catchall rules give the state the total right to pry on anyone who is online and force companies to abide by this law. China is proclaiming its vision of "Internet sovereignty" as a model for the world and is making it a legal reality at home. Fascists and communists do not like free speech either, especially when individuals disagree with them. China's Internet czar, Lu Wei uttered this: "This path is the choice of history, and the choice of the people, and we walk the path ever more firmly and full of confidence."(Denyer, 2016)According to Wei,China had struck the correct balance between "freedom and order" and between "openness and autonomy." It is traveling, he said, on a path of "cyber-governance with Chinese characteristics."

3. Political Freedom in Cyberspace

In principle, the Internet is free but it can also be understood as a mosaic of national internets (intranets) that are connected with each other through controlled gateways to the free Internet. Communication within the intranet is, of course, under the jurisdiction of national governments. Communication within the free Internet is under the purview of the United Nations — with some influence by the United States, its founder. As expected, China perceives the United States exercises too much power on Internet governance.

Cyber sovereignty has been a top priority of China's President Xi Jinping. According to Freedom House (2016): "The National People's Congress drafted a cyber security law which could strengthen requirements for internet companies to censor content, shut down their services, register their users' real names, and provide security agencies with user data stored in mainland China."(Freedom House, 2016) It could be argued that cyber sovereignty is the final solution of Internet censorship.

Many websites are blocked from within China,including 12 out of the Top 100 Global Websites. The Chinese-sponsored news agency, Xinhua, stated that censorship targets only "superstitious, pornographic, violence-related, gambling, and other harmful information."(China and the Internet, 2010) However, other websites focusing on political topics are often censored, such as: police brutality, freedom of speech, democracy, and Taiwan and Tibet independence. As of 2014, the New York Times, the BBC, and Bloomberg News websites are indefinitely blocked, but those censorship targets, as stated by Xinhua, cannot possibly justify banning these websites on those grounds. Fines and short arrest are the favored punishments and websites mysteriously disappear. Perpetrators can be subjected to "education through labor" camps for "inciting a disturbance". (Human Rights Watch, 2014)

The Chinese government's crackdown on free expression under President Xi Jinping's "information security" policy is taking its toll on digital activists who have fought back against censorship and surveillance. Introduced in 2015, dozens of prosecutions related to online expression are subject to legal restrictions and have fostered self-censorship. (MacKinnon, 2015) A criminal law amendment added seven-year prison terms for spreading rumors on social media (Human Rights Watch, 2015). Rumor charges are often used against those who criticize the authorities. Some users belonging to minority religious groups were imprisoned simply for watching religious videos on their mobile phones. The London-based magazine Economist and the Hong Kong–based South China Morning Post were newly blocked in mainland China, as were articles and commentaries about sensitive events including a deadly chemical blast in Tianjin in 2015.

As a member of the United Nations Security Council, China is using its global influence to undermine the UN rights system by sharply limiting visits by UN experts to China. Furthermore, it curbs access to the UN for critics of the Chinese government, including the Dalai Lama, Tibet's exiled spiritual leader. "The UN system offers one of the few remaining channels for activists from China to share their views and press for improvements in Beijing's abysmal rights record," said Kenneth Roth, executive director of Human Rights Watch. "Unless the UN and concerned governments put a stop to China's efforts to manipulate or weaken UN human rights mechanisms, the UN's credibility, and indeed its ability to defend rights in China and around the globe, are at risk."(HRW, 2017)

Effective August 25, 2017, the Cyberspace Administration of China (CAC) released new rules that forces users to use their real identity when posting messages online. Therefore, real-name registration eradicates anonymity on the Chinese Internet. Users may not be allowed postings online without giving identifying information and details of online communities. Furthermore, no contents may appear that is prohibited by national regulations. (Sonnad, 2017) These regulations– albeit vague – apply to websites, smartphone applications, and any other communication platform. Supposedly stemming the spread of rumors, the cyber watchdog enforces the requirement that people use real names when registering accounts online.

In 2008, China became the largest population on the Internet. As of 2016, approximately 50 percent of China's population had Internet connectivity (ChinaPowerCSIS, 2008). An important characteristic of the Chinese Internet is that China'sgovernment owns all online access and network routers.Private enterprises and individuals cannot own but only rent bandwidth from the state.

In January 2015, China added seven new access points to the global free Internet backbone, adding to the three points that connect through Beijing, Shanghai, and Guangzhou. Hence, all access points to the global Internet backbone are entirely under governmental control. Furthermore, the majority of Internet users restrict their use of the Internet to Chinese websites, as most of the population lacks foreign language skills. Nevertheless, the large size of its 40 million diaspora (Poston & Wong, 2014) is a great source for information and commentary.

Internet is nonetheless thriving in China, with nearly 700 million users, putting almost 1 in 4 of the world's online population behind the so called Great Firewall, a phrase coined by the Wired magazine. All websites that operate in China with their own domain name must have a license from the Ministry of Industry and Information Technology. Baidu is the leading search engine in China; Bing China has also entered the Chinese market. It also operates Yahoo's China search functions. As of 2015, Google has no presence in China. However, the blocking of websites can be circumvented and is generally ineffective at preventing the flow of information to determined individuals. Limitations of access are, nevertheless, effective for the majority of users who are not technologically knowledgeable. It is more effective at providing a chilling effect rather than actually blocking content. One common tactic in publishing sensitive topics is to post an article on a newspaper's website, and then comply with government orders to take it down. By the time the article is removed, a large number of people have already have read it, thus negating the point of the censorship order. (Infogalactic, 2016)

Enforcement of regulations is the remit of Cyber Administration of China (CAC) that wants to "bring the online news industry into closer alignment with the domestic print and broadcast sectors, in which all outlets are owned by the state or party."(Cook, 2017) Amnesty International notes that China "has the largest recorded number of imprisoned journalists and cyber-dissidents in the world." The "offences" these prisoners are accused of, include "communicating with groups abroad", "opposing the persecution of the Falun Gong", "signing online petitions" and "calling for an end to corruption". (GIFC, 2008)

China's government is making the Great Firewall deliberately porous by allowing businesses and its English-speaking elite VPN access to the free Internet. Virtual private networks enable users to attach their computers to an out-of-country network, which assigns an external IP address, and they experience the Internet exactly as if they were in the United States, for example. The authorities have accepted that a small portion of its population circumvents the Firewall via VPNs. It allows its elite a small window on the world, however they can take that privilege away at any time. Other circumvention software tools include website mirrors, archive sites, alternate DNS servers, proxy websites, and sneaker nets.

China relied on two United States' companies – Cisco Systems and Juniper Networks – who carried out its network upgrade in 2004 that enable the authorities to monitor Internet activities. Cisco also sold several thousand routers used to censor web content, and "firm's engineers have helped set it to spot 'subversive' key-words in messages."(Bennet, 2011) One can ask United States' cyber giants, Yahoo, Cisco Systems, and Microsoft, who helped China censor the Internet or operate online surveillance system, if they are committed to freedom of speech. Millions of Chinese people, and indeed everyone worldwide, depend on their products and services for reliable access to news and information ¬– as opposed to being complicit with repressive countries. Skype and TOM Online Inc., a Chinese wireless Internet company, jointly developed a Chinese version of Skype software. It employs a filtering mechanism that prevent text messages such as "Falungong" and Dalai Lama". However, relatively few words are censured and its messages are still being encrypted.

The first layer of Chinese Internet censorship takes place at the router level. Internet Access Provider (IAP) administrators have entered thousands of Internet website addresses (URLs) and keywords into the Internet routers that enable data to flow back and forth between Internet Service Providers (ISRs) cyber servers in China and elsewhere. Forbidden keywords and URLs are also plugged into Internet routers at the ISP level, thus controlling data flows between the user and the access providers. Router-level censorship is supplemented with additional filtering of political content by software at the ISR level.

For example when a Chinese Internet user types www.hrw.org (the Human Rights Watch website) into the address field of the browser an error message appears. Such a piece of software is called SmartFilter, developed by Secure Computing Corporation of San Jose, California. According to Human Rights Watch (2017):"Such filtering programs are used globally by households, companies, and organizations for all kinds of purposes: they enable employers to block employees from surfing pornography or gambling online from the office, and enable schools to prevent young students from accessing age-inappropriate content." (HRW, 2017) However, the Chinese government mostly blocks politically objectionable content by delegating censorship to Internet Content Providers (ICPs) who are liable for all content on their websites. Policing contents by automatic means or by company employees are typically implemented by requiring companies to sign a "voluntary pledge". This "Public Pledge on Self-discipline for the Chinese Internet Industry," initiated by the Internet Society of China (ISOC), commits signatories to "energetic efforts to carry forward the rich cultural tradition of the Chinese nation and the ethical norms of the socialist cultural civilization" by observing all state industry regulations. In particular, signatories vow to refrain "from producing, posting, or disseminating pernicious information that may jeopardize state security and disrupt social stability."(ISC, 2002) Yahoo signed the pledge!

Circumventing censorship by tech-savvy users becomes more difficult and it typically involves the use of proxy servers that can be seen by the ISP but not the final destination site. These proxies are quickly blocked but new ones pop up equally fast. Software tools like Tor can be set up to automatically discover new unblocked proxies. (Spring, 2006) It is difficult to gage how many users use proxies because surveys are not reliable. However, the Great Firewall, while not infallible, is successful enough to keep Chinese public opinion in line.

4. Towards Digital Totalitarianism

It is useful to examine the implication of policies that govern fingerprinting, real-name registration, censorship, and surveillance. In combination, these policies are the tools of totalitarianism, which is a political system in which "the state recognizes no limits to its authority and strives to regulate every aspect of public and private life wherever feasible."(Conquest, 1999) Winston Churchill applied this concept to Stalin's communist and Hitler's Nazi tyrannies. China's leadership requires fingerprinting on its new ID cards. Zhang (2011) states: "Effective on January 1, 2012, the new law will require citizens to have their fingerprints recorded when applying for, renewing, or replacing their resident identity cards. (ID Card Law, art. 3.)"(Zhang, 2011) Furthermore, China maintains an enormous database of face images enabling face recognition software to identify people almost instantaneously.

With 600 million closed-circuit television (CCTV) systems throughout the nation, questions of civil liberty and privacy are already raised. (Matthews, 2017) Authentication through facial recognition and other biometric features has been gaining traction in China. Images are sent to match with police databases in real time to catch criminals – or thought offenders. China's government wants to ascertain changing view and interests of its population. An election is one way to do that but the leadership eschews it. Instead, it collects data on a massive scale with the alleged aim of getting information on the honesty of regular citizens, public officials, and companies.

Certainly, there are legitimate applications of facial recognition, such as monitoring ATMs (cashpoints) and restricting access to sensitive facilities. Banks and restrictive organizations store all their data in their own databases and facial images are of great advantage for their own security requirements. However, when these databases are being shared beyond its scope, a surveillance network emerges. Law enforcement agencies are very keen on getting hold of all information that any individual generates. After all, so they assert, "law-abiding citizens are not at risk from this kind of exposure. "

China's public security obsession will have benefits for its citizens, but comes at the expense of privacy. According to website Singularity Hub (2017, page 2): "Officials aim to enroll every Chinese citizen into a nationwide database by 2020, and they're already well on their way to doing so."(Matthews, 2017) Cyber security has to address potential data breaches. Interfaces involving face recognition and fingerprints are very secure but its data are stored in databases. Giving the enormous scale and its distributed characteristics give unauthorized individuals plenty of opportunities for database break-ins. Hackers potentially may gain access to private information, such as credit card or bank details, personal health information, personally identifiable information, including face images and finger prints. Information collected from online and offline activities give authorities – and criminals alike – a timetable of past and present tasks done by any individual.

Historically, bureaucratic tools are preferred measures to restrict freedom and invade privacy in the name of law and order. Almost everyone has a hukou (household registration) document that determines where citizens can get public services. Block-by-block surveillance called "grid management" is being set up in several parts of the country: police and volunteers keep tabs on groups of a few hundred people, supposedly to ensure the rubbish is collected and disputes resolved. It is part of a tradition of self-policing that stretches back to the Song dynasty in the 11th century. (Briefing, 2016) Nowadays, the ubiquitous use of closed-circuit television cameras is at the heart of governmental rule. Combining this with cyber controls of the Great Firewall two more features, the Golden Shield, an extensive online surveillance system, and the Great Cannon, a tool to attack hostile websites, forms the totalitarian apparatus. Keeping track of transactions made, websites visited and messages sent is ambitious but probably not impossible. The government must match the owner of devices with the digital footprints they leave. That is the reason why users are required to use their personal information when registering online. It is unclear why the enforcement of the new laws passed in 2012 and 2016 can be realized.

Lists are a Chinese specialty that is the pillar of the social-credit system that scores financial creditworthiness of citizens but also their social and possibly political behavior. These lists are exceptionally long and might prevent people on these lists from buying airplane, bullet-train or first- or business-class rail tickets; selling, buying or building a house; or enrolling their children in expensive fee-paying schools. It allows the state to integrate its many databases: everyone's hukou, information from electronic surveillance, the tourist blacklist, the national model-worker program and more. Even video games cheaters can be blacklisted in the social-credit database. The social-credit project could become a digital surveillance blueprint because no law exists that restrict what companies can do with personal information. The national-security law and the new cyber-security law give the government unrestricted access to almost all personal data. China would be the first digital totalitarian state.

5. Political Implications of China's Economic Growth

Economic liberty and the growth it generates will no doubt profoundly change China. People will be more affluent and knowledgeable about other countries—Chinese tourists are already finding their way across the globe. According to an article in The New York Times from May 28, 2013, Bishop stated: "China, argue that the deep economic changes needed to propel China's next few decades of growth will not succeed without significant, liberal political shake-up. The Chinese leadership does not appear to agree, and the outcome of the debate may be one of the most important events of this century."(Bishop, 2013) The question is, will internet restrictions negatively affect China's economic growth in the future.

It is worthwhile to examine how cyber giants perform globally. For example, Amazon opened in 1995 and its sales are currently around twenty-five billion dollars a year (Levin, 2010). Chinese Taobao started in 2003 and today has two hundred million active users. Facebook, founded a year later, has over five hundred million users. Over the same period, the number of Google searches, and the revenue Google generates from its advertising auctions, has doubled roughly every eighteen months.This growth of Internet markets has generated considerable attention from economists, which prompted a great deal of recent research. (Levin, 2010) Some of this work has focused on the market structure of platform industries, and the strategic issues that arise when platforms compete for users. Other strands of research have focused on novel market institutions, such as the keyword auctions run by the major search engines, eBay's consumer marketplace, and the retail competition created by price comparison sites.

The largest 20 Internet corporations by nationalities are:

- 13 are US-American (Amazon, Google, Facebook, Uber, eBay, etc.)
- 4 are Chinese (Tencent, Alibaba, Baidu, etc.)
- 1 is Japanese (Rakuten)
- 1 is Spanish (ODIGEO)
- 1 is German (Zalando)

The United States clearly dominates the cyberspace globally. In contrast, the size of the Chinese Internet giants is due to their enormous domestic market, which restricts foreign competition. In return, the law on cyber security impedes China's companies' ability to compete in international markets. Alibaba's fate is tied to the Chinese market because in the third quarter of 2016, "only 7 percent of its revenue came from commerce outside China"(Mozur, 2017) In 2013, the United States government officially classified it as a barrier to trade, noting that eight of the 25 most trafficked sites globally were now blocked here. The American Chamber of Commerce in China says that 4 out of 5 of its member companies report a negative impact on their business from Internet censorship. (Denyer, 2016) American Chamber of Commerce in China chairman James Zimmerman labeled the country's Internet controls "a counterproductive effort that is impeding China's business growth."(Zimmerman, 2016) Cyberspace restrictions isolate China technologically from the rest of the world, limiting the country's access to global ideas and innovations. Excessive control over email and Internet traffic risks slowing, if not altogether halting, legitimate commerce. To attract and promote world-class commercial enterprises and promote economic development, China needs to encourage the use of the Internet as a crucial medium for sharing information and ideas. "Efforts to restrict access to information and censorship are only brief, momentary measures that will never fully curb the ambitions and creativity of its own people. At some point the current leadership's restrictive policies will come into question and be resigned to anachronistic footnotes in history."(Zimmerman, 2016) Cyberspace Administration of China, the country's Internet controls bureau regularly scrutinizes technology products sold by big foreign companies. While IBM and Microsoft have provided supervised access to source code, – the digital foundations of software – Apple rejected such requests.

It is clear that Internet restrictions limit business competiveness. The European Union is concerned about Chinese acquisition while, at the same time; it is coming up with stricter rules on foreign investment. South Korea used the same technique but no other country, apart from China, managed to grow on such a monumental scale. A little more than a decade ago, China started producing socks and cigarette lighter. Nowadays, it is at the global frontier of new technology in everything from mobile payments to driverless cars. Having benefitted enormously from the commercial system, China has now become one of its guardians. (The Economist, 2017) Overbroad restrictions may break it.Going forward, innovation is the key that drives economic advancement but it also relies on fresh ideas on a global scale that cannot possibly be done within China alone. Hence, China's leadership allows its businesses and its English-speaking elite VPN unfettered access to the free Internet. Members of China's rich upper class know how to "work the system" and are able to get hold of unbiased information while the poor lower class do not have that much of a need. Consequently, the middle class is the main force demanding more political freedom. According to McKinsey's 2016 global sentiment survey, for instance, found that China's working-age consumers, compared with peers in other regions, are most inclined to prioritize spending over saving or paying off debt. As they spend more, they are also likely to broaden their patterns of consumption, which are currently limited by the quality and variety of Chinese goods and services. In fact, Chinese consumers are increasingly trading up from mass products to premium products. (McKinsey, 2016) As they scouting the cyberspace for deals, they also find indications of free speech that influenced the creation of the products they seek.

As China is moving from imitation to innovation, its design centers are focusing on developing innovative new products for global markets. For that to be successful, the middle class is increasingly pushing for open access to the free Internet.According to a study by consulting firm McKinsey & Company, "76 percent of China's urban population will be considered middle class by 2022. That's defined as urban households that earn US$9,000 – US$34,000 a year."(Iskyan, 2016) Adjusting for purchasing power, the middle class amounts to over 50 millions households by 2022. They are situated between the elite and the masses. Its young members (under 35) have amassed wealth, will they not try to accrue political power, too, and is their trust in their government on the wane? Many of them are bemoaning the lack of political accountability. After it brutally crushed its pro-democratic demonstrations in 1989, China's government survived by delivering fast economic growth and stability, but did not quashed political individual aspirations entirely. Few people want the vote but, nevertheless, they want the rule of law and greater individual autonomy, which creates a threat to the state's monopoly on power.

Hong Kong has the vote already under the "one country, two systems" principle after the United Kingdom ceded sovereignty to China in 1997. After the transition, debates have continued between pro-China and democratic factions and characterized the political landscape. Their middle classes are becoming more restive with demand from more democracy to independence. This was epitomized by the so called "umbrella revolution" that was a civil disobedience movement that demanded full democracy for Hong Kong citizens and the resignation of its chief executive, Leung Chun-ying. China has the power to vet Hong Kong's chief executive as a means to maintain political control to prevent Western-style freedom from swapping over to the mainland. The movement was mainly supported by younger Hong Kongers while most of the older generation was actively opposed to it, fearing that China might withdraw the freedoms that Hong Kong has.

According to Associated Press (August 17, 2017): "A Hong Kong court sent young activist Joshua Wong and two other student leaders to prison Thursday for their roles in huge pro-democracy protests nearly three years earlier, in the latest sign that tolerance for dissent is waning in the Chinese-ruled former British colony."(AP, 2017) The three students were being punished for leading unlawful protests that brought major streets to a standstill for 11 weeks. These protest were directed against China's plan to restrict elections in Hong Kong. China's middle class affluence and its accompanying political aspiration create challenges for the government. Sustained economic development leads to democracy, not the survival of dictatorship. It remains to be seen but the writing is on the wall.

6. Summary and Conclusion

China must balance its interests between political goals – minimal freedom – and economic benefits – maximal freedom – at a time when China enters the innovational phase of its economic cycle. Restricting access to the free Internet will significantly harm idea exchanges and economic development alike. Democracy and capitalism work well together, but – as China demonstrates – one without the other seems to work, too. Chinese private entrepreneurs have not become a force for democratic change. The introduction of market forces in China suggested that a civil society might emerge sooner or later even under the tightest of controls and will bring about the freedom of public discourse. However, for the last three decades these expectations have not taken place because an authoritative dictatorship, represented by China, and capitalism are going together – for now. Moving away from its low wage economic model towards innovation, China's middle class demands more freedom of expression. The Chinese experience demonstrates that while economic freedom is necessary, it is not by itself sufficient to bring about political freedom.

China's leaders have so far used one type of freedom to achieve their economic ends while brutally tramping down on the other. China's current political system, if it remains in place, may be undermining its economic expansion and profit making. China cannot rely on low wages forever as it faces competition from other countries. Innovation is a global affair that relies on exchanges of science, technology, information, and ideas. For that to be successful, China must loose its control on political discourses. In contrast, China's government maps out a path towards totalitarianism and it using its domestic cyberspace as a powerful weapon. With its social-credit system almost everybody can be identified and her or his digital footprints – including financial, social and political behavior date – are being accumulated. Together with the concept of cyber- sovereignty – absolute state control of communication – becomes a digital surveillance blueprint for the first digital totalitarian state. China's Internet czar, Lu Wei describes the balance between freedom and order, however, the balancing act between freedom of expression and censorship is much more exiting to observe in the realms of political freedom and economic affluence.

Bibliography

AP, K. C. (2017, August 17). Young leaders of massive 2014 Hong Kong protests get prison. Retrieved from Associated Press: https://www.yahoo.com/news/hong-kong-activist-wong-braces-possible-prison-sentence-034454213.html

Bennet, I. (2011, February 23). U.S. Internet Providers and the 'Great Firewall of China'. Retrieved from Council on Foreign Relations: https://www.cfr.org/backgrounder/us-internet-providers-and-great-firewall-china

Bishop, B. (2013, May 28). In China, Weighing Economic and Political Freedoms. Retrieved September 14, 2017, from The New York Times: https://dealbook.nytimes.com/2013/05/20/in-china-weighing-economic-and-political-freedoms/

Briefing. (2016, December 17). China invents the digital totalitarian state. Retrieved from The Economist.

China and the Internet. (2010). International Debates, 8 (4).

ChinaPowerCSIS. (2008). How web-connected is China? Retrieved from http://chinapower.csis.org/web-connectedness/

Conquest, R. (1999).Reflections on a Ravaged Century.

Conteh-Morgan, E. (2015). China's Worldview and Representations of Its Engagement with Africa. ASFJ – Africa &Francophonie, 6 (3), 16-34.

Cook, S. (2017, May 23). China's Next Internet Crackdown. Retrieved July 15, 2017, from The Diplomat: http://thediplomat.com/2017/05/chinas-next-internet-crackdown/

Denyer, S. (2016, May 23). China's scary lesson to the world: Censoring the Internet works. Retrieved September 29, 2017, from The Washington Post - Asia & Pacific: https://www.washingtonpost.com/world/asia_pacific/chinas-scary-lesson-to-the-world-censoring-the-internet-works/2016/05/23/413afe78-fff3-11e5-8bb1-f124a43f84dc_story.html?utm_term=.f1bba7769b1a

Financial Times. (2017, June 1). China's cyber security law and its chilling effects. Retrieved from https://www.ft.com/content/60913b9e-46b9-11e7-8519-9f94ee97d996

Freedom House. (2016). Retrieved from Silencing the Messenger: https://freedomhouse.org/report/freedom-net/freedom-net-2016

GIFC. (2008). Background: Firewall of Shame. Retrieved July 15, 2017, from Global Internet Freedom Consortium,: http://www.internetfreedom.org/Background.html#Firewall_of_Shame

HRW. (2017, September 5). UN: China Blocks Activists, Harasses Experts. Retrieved from Human Rights Watch: https://www.hrw.org/news/2017/09/05/un-china-blocks-activists-harasses-experts

HRW. (2017, September 5). UN: China Blocks Activists, Harasses Experts. Retrieved from Human Rights Wat: https://www.hrw.org/news/2017/09/05/un-china-blocks-activists-harasses-experts

Human Rights Watch. (2015, November 2). China: New Ban on 'Spreading Rumors' About Disasters. Retrieved July 14, 2017, from Human Rights Watch: https://www.hrw.org/news/2015/11/02/china-new-ban-spreading-rumors-about-disasters

Human Rights Watch. (2014, January 15). Human Rights Watch. Retrieved July 14, 2017, from Reeducation Through Labor in China: https://www.hrw.org/legacy/campaigns/china-98/laojiao.htm

Infogalactic. (2016, January 4). Internet in China. Retrieved July 15, 2017, from Infogalactic: the planetary knowledge core: https://infogalactic.com/w/index.php?title=Internet_in_China&oldid=170333

Internet Society. (2015). Global Internet Report 2014. Retrieved from https://www.internetsociety.org/sites/default/files/Global_Internet_Report_2014.pdf

ISC. (2002, July 19). Internet Society of China. Retrieved from Public Pledge of Self-Regulation and Professional Ethics for China Internet Industry: http://www.isc.org.cn/20020417/ca102

Iskyan, K. (2016, August 27). China's middle class is exploding. Retrieved from Business Insider: http://www.businessinsider.com/chinas-middle-class-is-exploding-2016-8

Levin, J. (2010). The Economics of Internet Markets. Stanford University, Economics, Stanford CA.

MacKinnon, R. (2015, January). Fostering Freedom Online: The Role of Internet Intermediaries. Retrieved July 14, 2017, from University of Pennsylvania Scholarly Commons: https://pdfs.semanticscholar.org/0ec2/6f3adb435355bf354b31c87bf1fc9d73c45e.pdf

Matthews, K. (2017, July 28). The Biggest Facial Recognition System in the World Is Rolling Out in China. Retrieved from SingularityHub: https://singularityhub.com/2017/07/28/the-biggest-facial-recognition-system-in-the-world-is-rolling-out-in-china/

McKinsey. (2016, September).The CEO guide to China's future. Retrieved from McKinsey Quarterly: https://www.mckinsey.com/global-themes/china/the-ceo-guide-to-chinas-future

Mozur, P. (2017, Jan 24). The New York Times. Retrieved from https://www.nytimes.com/2017/01/24/business/alibaba-china-results-ma.html?mcubz=3

Poston, D., & Wong, J. (2014). The Chinese Diaspora Population in circa-2011. Retrieved from http://paa2014.princeton.edu/papers/140495

Schneier, B. (2015). Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World. New York, NY: W.W. Norton & Company.

Sonnad, N. (2017, August 26). In China you now have to provide your real identity if you want to comment online. Retrieved from Quartz: https://qz.com/1063073/in-china-you-now-have-to-provide-your-real-identity-if-you-want-to-comment-online/

Spring, T. (2006, February 28). Outsmarting the Online Privacy Snoops. Retrieved from PC World: http://www.pcworld.com/news

The Economist. (2017, September 23). How China is battling ever more intensely in world markets. Does China play fair?

Zhang, L. (2011, November 4). Library of Congress. Retrieved September 23, 2017, from China: New ID Card Law Requires Recording Fingerprints: http://www.loc.gov/law/foreign-news/article/china-new-id-card-law-requires-recording-fingerprints/

Zimmerman, J. (2016, May 17). Censorship in China Also Blocks Business Growth. Retrieved from The Wall Street Journal: https://www.wsj.com/articles/censorship-in-china-also-blocks-business-growth-1463504866