The Thorny Triangle: Cyber Conflict, Business and the Sino-American relationship in the Global System

https://www.e-ir.info/2010/03/10/the-thorny-triangle-cyber-conflict-business-and-the-sino-american-relationship-in-the-global-system/

ATHINA KARATZOGIANNI, MAR 10 2010

[i]Introduction

The Google-China event in January 2010 is a snapshot example of developments in global politics, the world economy, and the major media transformation causing/accompanying these developments, in ways which will prove revealing in more than one disciplines of study. The history of the media and the internet censorship in China is well documented, as well as the various cyberconflicts[ii] linked to conflicts pertaining to the real world or tied specifically to internet freedom in general and to the Chinese approach to ICTs in particular.[iii] The purpose of this article is to sketch roughly the web of complex issues in which this cyberconflict is situated.

In the bigger picture, this cyberconflict event adds to the debate on the position of China in the world system, and creates insecurities about the ambitions, capabilities and hidden desires of the 'next hegemon',[iv] while it punches more wholes to the already uncomfortable Sino-American relationship.[v] Further, it raises questions about China's information warfare philosophy and military doctrine[vi] and the bizarre and contradictory ways they develop their virtual society, i.e. exploiting the technologies commercially, but using surveillance and censorship in ways contradicting liberal ideal of universal digital rights. On top of these concerns are the transformations the internet has brought in regards to civil society, citizenship and activism;[vii] the relationship between business and activism in China and beyond;[viii] the relationship between the state and the plethora of 'patriotic' hackers;[ix] and the question of the working class digital have-less inside China.[x]

China as the next hegemon in the global system[xi]

Faced with the collapse of American hegemony, there are three options of where the world could go from here. There could be an American-led global empire or world state based on the extraction of tribute; an East Asian-led world market society; or global chaos. The first of these options has been eliminated by American failure in Iraq and Afghanistan.[xii] Arrighi argues that America has made an attempt to block the spatial fix towards China by taking the financial flows away from emerging centres and trying to end the cycle of spatial fixes by creating a world government.[xiii] But with army morale collapsing, soft power at drastically low levels and the US forced to step back from further unilateral actions and adopt conciliatory positions towards China, the days of American rule even by mere domination are numbered; America has failed to convert military power into economic dominance.[xiv] With the American option eliminated, avoiding 'chaos' depends on the capacity of China, India and other Southern states to find an equitable and ecologically viable developmental model.[xv] The US crisis provides an opportunity to escape the vicious circle of North–South relations, an escape pioneered by China.[xvi] Arrighi seeks a 'new global leadership' in East Asia to provide 'system-level solutions to the problems left behind by US hegemony'.[xvii]

So why is China in particular put forward as a potential new hegemon? First, China is the best hope for spatial fix, given its size and population; this is happening already, Arrighi argues, via infrastructure investments.[xviii] Second, unlike the other East Asian powers, China is not a US vassal or a city-state, and it depends less on America than America depends on China.[xix] Third, China is the pioneer of a new model of economic organisation. The rise of

network production and smaller businesses had led to a shift of economic power to East Asia as a hybridisation of the tradition of marked-based non-capitalist development with Western capitalism.[xx] Finally, and most crucially, he argues that China offers a distinct development path to lead the world out of capitalism. The 'war on terror' may even have strengthened rival powers such as China by deflecting American interest elsewhere.[xxi] Chinese global trade his risen spectacularly during the 'war on terror', rising nearly 50 per cent in 2003 alone. China has also forged links with Europe, Latin America and Africa.[xxii] There is even talk of a Chinese–European alliance to constrain America.[xxiii]

Arrighi is not alone in making the argument that a new hegemon is emerging to replace America. Bergesen and Lizardo disagree with claims that present economic trends suggest that East Asia will be the next hegemonic centre,[xxiv] but also disagree with the idea that a permanent division of labour between military power in the United States and economic strength in Asia will yield a heretofore never-seen bifurcation of economic and military power[xxv] or something like a new 'empire' of global capital/capitalists free from the constraints of being situated in hegemonic states.[xxvi] Instead, they contend that this is the picture only when looking at data in the short term. Data on global distribution of the 500 largest firms today would support the 'empire' hypothesis of a tripartite division between America, Europe and East Asia; the same distribution discussed over time would support the idea of a transfer of power to East Asia.[xxvii] Ultimately, they argue that, while East Asia might take over hegemony in the short-term, Europe is the strongest long-term candidate. Andre Gunder Frank's last work concurs with Arrighi's view that China is the rising hegemon, suggesting that the world-system is resorting to its Asian core after a brief European blip.[xxviii] Para Khanna[xxix] argues that American power is being lost to a growing semi-periphery. Perry Anderson sees the situation leading to 'a modern equivalent of the Concert of Powers after the French Revolution and Napoleonic Wars', involving jockeying among leading powers without serious discord.[xxx] The argument regarding China as a rising hegemon had previously been made about Germany and Japan, before they went into system-induced crisis.[xxxi]

China theorized as the next hegemon is problematic, and this is before one even considers the political context in China, and a state attitude to self-valorisation by workers and peasants that may even overshadow America. One of the world's most brutal state–market complexes, the Chinese one-party regime is typified by social authoritarianism, the repression of national minorities, prohibition of independent associations such as free trade unions, abuses of civil and human rights including one of the world's most vicious regimes of biopolitics (from forced abortions and organ sales to an almost routine use of the death penalty), censorship of transgressive flows from Falun Gong to the Internet, moral and cultural policing (such as the activities of local civil wardens in extorting payments and harassing people for petty deviance), the almost total sidelining of non-economic values and the prioritising of stability and economics over freedom and welfare, and in general an extremely limited space for self- assertion by the oppressed. In comparison with, say, India, or most of Latin America, the Chinese poor are faced with far greater risks should they wish to squat unused land, or form associations to lobby for reform, or engage in informal economies, or promote indigenous ways of life in peripheral regions.

Aside from its desirability, it is not clear that Chinese hegemony is even possible at this point. Despite a few concentrations of high-tech industry and the globalisation of some coastal regions, in many respects China remains a firmly peripheral country within the world- system. Arrighi's showcase example of China's distinct model, the TVEs, is in many respects typical of peripheral countries, which maintain cheap labour by linking low-paid infrastructure to non-capitalist rural economies which subsidise low wages by meeting reproduction costs. It is not clear how China today has anything like a leading sector, which would give it a persistent market advantage. Granted, it has economic networks, but hardly the exclusive claim to these that America had to multinationals in its early years, and the products they are making are very much at the peripheral end of the world- trade system. China has inherited much of the semi- peripheral industrial production that formerly migrated to, then from, Southeast Asia in pursuit of low wages.

China's information warfare doctrine and alleged activities before January 2010

The environment of this cyberconflict[xxxii] has a longer and more controversial history than the one reported in the global media. Back in 1999, Mulvenon and Yang contemplated various scenarios in *The People's Liberation Army in the Information Age*, assessing the capabilities of the US and China in a possible confrontation. They write that there are important differences between Chinese and American Information Warfare (IW) literatures. People's Liberation Army (PLA) writers look at IW in strictly military terms, while Western authors accept the dichotomy between information warfare waged between states or militaries (cyberwar) and information warfare waged between substate actors and states (netwar). Both US and Chinese authors are guilty of over-using Sun Ji, especially the notion of 'winning the battle without fighting'. Chinese theorists are also forced to discuss from a technologically inferior standpoint, in opposition to an advanced foe.[xxxiii] Nevertheless, Mulvenon and Yang believe that IW presents the Chinese with a potentially potent, if circumscribed, asymmetrical weapon. 'Defined carefully, it could give the PLA a longer-range power projection capability against US forces that its conventional forces cannot currently hope to match… to attack its information systems, especially those related to command and control and transportation'.[xxxiv]

In 2007, the accusations against the Chinese attempting cyber-espionage pointed to problems in how governments understand cyberconflicts and their regulation. The Chinese government denied that the Chinese military is to blame for the cyberattacks involving systematic network penetrations against the US, Britain, Germany, France and New Zealand during 2007, also pointing out that such accusations are irresponsible and have ulterior motives. The Chinese argued that they have long opposed cybercrime and have explicit law and regulations against it and that China 'does not do such despicable things'. The German chancellor, Angela Merkel, after her own office and several government ministries were found to be infected with spyware, brought up the issue directly during her visit in China, warning that the two countries should observe 'a set of game rules'. The response by the Chinese government was to distance themselves from the accusation, while promising to cooperate with international efforts to combat cybercrime.

Although the Chinese government is rounded and blamed by most experts in the field for the various attacks occurring in recent years, the countries attacked in most cases avoid directly accusing the Chinese, and mostly 'raise the issue' with them or stress that they are not implying that they did it, like the French, hoping that the Chinese will control their military or their rogue citizens more effectively in the future or that they will not succeed in getting classified information next time.

Nevertheless, the reality of the situation is much more complex – interestingly a word used by President Bush to describe the American relationship with China – as it points to problems in reporting instances of cyberconflict without hyberbole; combating with formal international regulations cybercrime, cyberterrorism, information warfare and industrial espionage; putting more strain to bilateral relations with China on a global level; pointing to serious doubts over the Chinese government's control of their own military; and threatening the China's image in the community of states. Cyberattacks can also be in the future an extra problem for diplomatic relations with China, side by side with intellectual property rights, freedom of expression, aggressive industrial growth and monetary policy, environmental concerns, Tibet and Taiwan etc. China is currently feared by these powers. The reason is not China's plans for cyberattacks against navies. There were plenty of those lurking on the Internet, published years ago by military futurologists in China, where the information warfare field has produced all sorts of scenarios on par with the US. The Chinese information warfare theorists have been discussing this a long time now from a technologically inferior position, arguing that information warfare can provide them with an asymmetrical advantage.

China is feared because it is growing at great speeds and is hungry for information, as is currently every other country in the world. Understandably, competition on commercial, military technology and cutting-edge industrial secrets is fierce. Even if the compromised system is unclassified, combined information can produce good intelligence perhaps compromising industrial, military secrets and so on. For China to sustain its economic success, she must become a centre of innovation and technology, and she looks particularly keen to, which is why she is the main suspect.

When attacks happen, they normally either never become public or do become public years down the line. Governments and companies usually refrain to tell the world that their systems are vulnerable. The US has suffered attacks that have been traced to provinces in China since 2003 with Titan Rain, when systems at NASA and other networks (agencies in Arizona, Virginia, San Diego, Alabama) were attacked, retrieving information on aviation specifications and flight-planning software. This became public only in 2005. Therefore, it is especially curious that the attacks in June 2007 came out as quickly as they did. Reactions of the countries under attack will vary, as there is no regulation over information warfare on an international level. There is not even international cooperation on the issue of ICANN and Internet governance, despite efforts at a world summit, let alone against cyberterrorism. For example, as pointed out by American officials, tracing hackers who use Chinese networks is complicated by the lack of cyber investigation agreements between China and the United States. Generally, response varies from counter-attacks, for example such as the one reported by *The Times* during Titan Rain when US security expert Shawn Carpenter counter-hacked the intruders to the restrained reaction of the of New Zealand prime minister, Helen Clark, who says she knows which countries tried to hack into her government's computers but is refusing to name names commenting that 'that's not the way intelligence matters are handled'. Interestingly, she also said that it is something every country is experiencing.

The reaction of the former US president, George W. Bush, was that he was aware that 'a lot of our systems are vulnerable to cyber attack from a variety of places' and that he might bring the issue up with the Chinese, which he never did, confirming the role of his administration as a cheerleader to the 85 per cent of networks controlled by private business in his country. The UK's reaction is also interesting since alarm bells have been ringing for a long time by the country's experts, as the National Infrastructure Coordination Centre had warned of the attacks in 2005 and the scale as 'industrial'. Andrew MacKinlay, a Labour member of the Commons Foreign Affairs Committee, went on record as saying that the attacks came from China and accused the government of covering up the scale of the problem and appeasing the Chinese.

Not every country has cyberlaws, and there is no law that deems cyberattacks as military attacks against a nation, so it seems that everyone is doing it now that there is no international regulation, and now they can get away with it. In the case of China, even if their military was involved and the Chinese government was turning a blind eye or was buying the data from independent hackers (although one has to be sceptical as the Internet is controlled fiercely in China), who can be sure that other state or non-state actors did not disguise their attacks to come from China, since China was destined to be blamed anyway? British official Roger Cummings of the National Infrastructure Security Coordination Centre (NISCC) talks of 'countries' probing attacks against his country, while New Zealand also talks of 'countries', and the US mentions attacks by state and non-state actors. The whole reaction of these countries feels like there is more to this than China.

Indeed, there might be more to this than China and hackers, as some of the cyberattacks China is accused of, seem particularly clumsy to be orchestrated by senior state or military officials. Also, in China, as in everywhere else, the field is scattered, information warfare specialists and hackers are not under a centralized command, and it might not be easy to control their plans, scenarios and attacks. Also, all this 'China-but-other-countries-we-cannot-name and non-state actors too' is confusing, and under an unregulated environment, blaming China for attacks against so many different countries was somewhat suspicious. The Google incident in a way brought to focus this history of allegations and in the mind of many experts crystallized China as the major player engaged in cyberespionage.

Virtual society made in China: Business and citizen activism, censorship and surveillance, patriotic hackers, the state, and the digital have-less

Those using the internet against their governments seek power, participation and democracy, making demands that governments are not only unwilling to provide but, more importantly which prompt counterstrategies to crack down on these cyberdissidents. The internet is, therefore, a battleground for these opposing interests, and it remains to be seen whether it will develop into a powerful engine for democratization, or will fall under the pressure and regulation of authoritarian regimes. it is obvious that most governments get negative points for the freedom of their citizen's access to the network. Bypassing censorship and using techniques to get banned information or to transmit forbidden information affects media coverage in all these countries and this again can affect policy. Interestingly, the key words or the themes banned in most authoritarian regimes, if analysed discursively, point to either desired banned topics and ideologies, such as democracy, participation, revolution, reform, etc., or very negative ones, such as massacre, or historical events of oppression, repression and conflict. Online efforts, such as pro-democracy, activist or anti-government websites point to the fact that people believe in the power of the medium enough to organize and run thousands of these sites. In many cases, they are able to initiate and control events, and mobilize and recruit others for their cause, as in the case of sites in the Islamic world, in China, in Latin America, activist sites for anti-globalization and single-issue protests and mobilizations both on national and international levels.

In this author's previous work,[xxxv] Chinese dissidents were discussed as an empirical example of sociopolitical cyberconflict. Various groups, such as the Tibetan exile networks, the Falungong, and the Chinese Demcratic Party have used email spamming and proxy servers to access blocked sites, built sophisticated websites, mobilized through email lists, bulletin board sites, file-trading and e-magazines to express their dissent online. Dissident use of the internet exhibits characteristics that are typical of new social movement activity: The political opportunity structure opened by the internet to allow cyberdissidents to reach international public opinion (online dissent, activism and arrest is extensively reported by foreign media); the structure of the online dissident movement (it seems to have no central leadership and looks network-type in character, for example the internet was crucial for recruitment for the CDP party); the use of technologically enhanced tactics, opening up alternative information and coordination networks; collective identity (cyberdissidents increasingly show solidarity towards each other; and the problematic relationship with the state (there is a crackdown on dissidents by the state). The Chinese regime has had great difficulty in controlling information, and had to go to great lengths to shut down on specific cases such as the Urumqui revolt and even dropping off the news the Google strory swiftly after it came out.[xxxvi]

It is well known that the success of dissidents, movements and causes depends on how they mobilize, recruit, organize and frame their messages, how they link to other affinity networks and how they market themselves, grasping political opportunities and utilizing ICTs. [xxxvii] Yang in his *The Power of the Internet in China* devotes a chapter on what he calls the business of digital contention, focusing primarily on the marketing aspect of contention, what in the cultural industries is called 'bankable dissent'. Yang believes that no other cultural industry is more invested in contention than the Internet business:

Not only do activists sometimes adopt business strategies to promote their causes, but business firms have vested interests tin contentious activities and thus develop strategies to promote certain kind of contention, thus creating some kind of synergy between business and activism.[xxxviii]

Political channels in China are not open enough to the citizenry, so the Internet has come to be considered by default a freer space for public participation. Yang explains that small private business in China were initially economic activists lacking legitimacy and antagonizing the state, found supporting with free drinks and food the protesters in 1989. In the 1990s this relationship has become more complicated as activists not only adopted business strategies, but began to 'combine activism with business as they realise that they, too, have to make a living'.[xxxix]

Meanwhile internet businesses have started to promote contention to increase their internet traffic, by utilizing media events that monetarily become huge, such as hosting contentious websites, launching protest forums, boosting web traffic in affiliated sites. Yang interviewed a content editor who explained that 'within limits permitted by the government, we will continuously "stir fry" [*chaozuo*] a hot-spot incident.'[xl] Besides the evident association between the citizen participation, which is offered online but not offline in China, and the general unprecedented marketization occurring in the Chinese society, Yang offers a masterful explanation of the deeper causes for online contention, which ultimately in China may mean business:

…the social polarization, identity crisis, and growing citizenship consciousness that have accompanied China's great transformation brew an angst for self-expression, social recognition, and social justice. Online activism is the manifestation of these impulses in cyberspace.[xli]

Despite the dangers he clearly identified, Yang believes that the Chinese activist may resist and challenge the commercialization and the manipulation of contention by business, especially when the relationship between market and democracy is reformulated as a social relationship.[xlii]

Conclusion

Eventually, this brings us full circle to the Google-China cyberconflict, which rounds up empirically all the analysis so far. The attacks against Google were reported by Google itself in January 2010, although the attacks took place towards the end of 2009, with a declaration on changes in their China policy, due to attacks originating in China penetrating their network to steal intellectual property (source code) and hacking into gmail accounts held by human rights activists. At the same time revelations were made about similar attacks involving more than thirty companies, and the whole reportage in the media was also linked to a US-China Economic and Security review, released in November 2009, reporting to Congress a steep rise in attempts to infiltrate and disrupt US government sites form all over the world with China the largest single source. China, itself, also a more than frequent victim of cyberattacks, dismissed the report as fabrication.

After Google expressed the will to renegotiate censorship compliance with the Chinese, and the eventually materialized threat to walk out of their business operations in China, both the American and Chinese governments were dragged into an international incident over the role of multinational companies in foreign countries. Hilary Clinton asked the Chinese for an explanation over the allegations and urged companies to show consideration for human rights and freedom of expression as part of corporate responsibility, while the Chinese denied any government involvement as per usual, and termed Google's actions as information imperialism and an effort to impose the western cultural package accompanying the technologies. This reheated the hegemon debate and the insecurities felt by both powers forced to collaborate in a global world with a recurring mention of problems in the relationship, regarding American sales of weapons to Taiwan, the meeting between Obama and the Tibetan leader in exile, which infuriated the Chinese, and all sorts of issues linking to the antagonism over currency issues, trade issues, the climate change discussions, human rights and the crack down of media freedoms and dissidents inside China.

At the same time the incident yet again pointed to significant problems in the regulation of cyberconflict and the identification of the origin of attacks, the operation of multinationals and their ethical responsibilities, the political economy of global communications and the far-reaching activities of Google in this environment ironically seen by some as threatening to privacy. Also raised domestic issues in China and elsewhere pertaining to surveillance, censorship, activism and the market and specifically focused on the intricacies of the virtual society in China and the appaling record of the regime in that regard, bringing into focus the vastness and intercultural barriers of the Chinese

market, coupled with the inequalities linked to the Chinese working class.

The China-Google cyberconflict had a history itself dating back to 2002 with Google not being accessible in China and then accepting self-censhorship for the rest of the decade prompting many to view this accusations as a business decision and Google's leverage to renegotiate censorship in China. Whatever the final outcome of the China-Google cyberconflict, the effects are wide-reaching in this field of research, as it brings together in one discussion, a complex matrix of debates: global politics and world-system theorizing, global political economy, diplomacy, the opposition to the universalism of democracy and freedom as western values, cultural imperialism, multinational business and corporate responsibility, internet politics, international law, internet regulation discussions, the digital gap, digital rights as universal human rights and surveillance and censorship as a global issue and highlights yet again the contradictions in the state, market and society triangle.

—

Dr Athina Karatzogianni *is currently lecturer in Media, Culture and Society at the University of Hull. She has studied international relations, international conflict analysis and her doctoral research was a study of the theoretical significance of the network forms of new technologies, on the phenomenology of social protest and resistance and on the formation of identities and differences.*

[i] The author wishes to thank the Faculty of Arts and Social Sciences at the University of Hull and the support of its Dean, Professor George Talbot, while engaging in partnerships on his behalf in China, and in parallel conducting research for this article during October 2009. Also, to recognize the wonderful hospitality of all the universities and their people in Beijing and Shanghai. Andrew Robinson, Ned Rossiter and Bev Orton where kind enough to offer their help at various stages of research. The article concentrates also some sporadic work on China found in previous projects over the last decade.

[ii] Karatzogianni, A. (2006) *The Politics of Cyberconflict*, London and New York: Routledge.

[iii] For instance, see Mulvenon, J. and Yang, R. (1999) *The People's Liberation Army in the Information Age*, California: Rand; Chase, M. and Mulvenon, J. (2002) *You 've Got Dissent! Chinese Dissident Use of the Internet and Beijing's Counterstrategies*, California: Rand; Rawnsley, G.D. and Rawnsley, M.Y.T (eds) (2006) *Political Communications in Greater China: The Construction and Reflection of Identity*, London: Routledge.

[iv] Karatzogianni, A. and Robinson, A. (2010) *Power, Resistance and Conflict in the Contemporary World: Social Movements: Network and Hierarchies*, New York: Routledge, p.115.

[v] *The Economist* (24-30 October 2009) 'The odd couple', Special Report on China and America.

[vi] Reid, T. (8 September 2007) 'China's cyber army is preparing to march on America, says Pentagon', *The Times.*

[vii] Yang, G. (2009) The Power of the Internet in China: Citizen Activism Online, New York: Columbia University Press.

[viii] ibid. and interviews

[ix] Henderson, S. (2006) The Dark Visitor: Inside the World of Chinese Hackers. <http://www.lulu.com/content/1345238> and his site <http://www.thedarkvisitor.com/>

[x] Qiu, J.L. (2009) Working-Class Network Society: Communication Technology and the Information have-less in Urban China, Cambridge, Massachusetts and London: The MIT Press.

[xi] This section on China as the next hegemon has been extracted from Karatzogianni, A. and Robinson, A. (2010) *Power, Resistance and Conflict in the Contemporary World: Social Movements: Network and Hierarchies*, New York: Routledge, pp. 115-122.

[xii] Arrighi, G. (2007) *Adam Smith in Beijing: Lineages of the Twenty- First Century*, New York: Verso, pp. 7 and 164.

[xiii] ibid., pp. 221–2, 226, 228.

[xiv] ibid., pp. 182, 203–4, 273, 284.

[xv] ibid. p.10.

[xvi] ibid., p. 95.

[xvii] ibid., p. 165.

[xviii] ibid., p. 220.

[xix] ibid., p. 8.

[xx] ibid., pp.145, 171.

[xxi] ibid., pp. 74–5.

[xxii] Arrighi, G. (2005) 'Hegemony Unravelling-1', *New Left Review* 32, March–April,

p.78.

[xxiii] ibid. 79 citing Shambaugh 2004.

[xxiv] Bergesen, A.J. and Sonnett, J. (2001) 'The Global 500: mapping the world economy at century's end', *American Behavioral Scientist* 44, 10, pp. 1602–15.

[xxv] Arrighi, G. and. Silver, B.J. (1999) *Chaos and Governance in the Modern World System,* Minneapolis: University of Minnesota Press.

[xxvi] Robinson, W. (1996) *Promoting Polyarchy: Globalization, US Intervention, and Hegemony*,

New York: Cambridge University Press; Bergesen, A.J. and Lizardo, O.A. (2005) 'Terrorism and hegemonic decline', in J. Friedman and C. Chase- Dunn (eds) *Hegemonic Declines: Present and Past*, Boulder: Paradigm Publishers.

[xxvii] Bergesen and Lizardo, 2005

[xxviii] Frank, A.G. (1998) *ReOrient: Global Economy in the Asian Age*, Berkeley: University of California Press.

[xxix] Khanna, P. (2008a) 'Waving goodbye to hegemony', New York Times, 27 January.

Online. Available at: www.nytimes.com/2008/01/27/magazine/27world-t.html; Khanna, P. (2008b) *The Second World: Empires and Influence in the New Global Order*, New York: Random House.

[xxx] Anderson, P. (2007) 'Jotting on the conjuncture', New Left Review 48, November–

December. Online. Available at: www.newleftreview.org/?page=article&view=2695.

[xxxi] Albert, M. (1993) *Capitalism against Capitalism*, trans. P. Haviland, London: Whurr.

[xxxii] Karatzogianni, 2006, pp. 94-120.

[xxxiii] Mulvenon, J. and Yang, R. (1999) *The People's Liberation Army in the Information Age*, California: Rand, p.182; also, Qiao Liang and Wang Xiangsui (2002) *Unrestricted Warfare: China's Master Plan to Destroy America*, Pan American Pub lishing Company.

[xxxiv] ibid., p. 175.

[xxxv] Karatzogianni, 2006, pp. 128-142.

[xxxvi] Tam, F. (16 January 2010) 'Reporting of search giant's tilt at censors is muzzled', *South China Morning Post.*

[xxxvii] Karatzogianni, 2006, pp. 121 and 174.

[xxxviii] Yang, G. (2009) *The Power of the Internet in China: Citizen Activism Online*, New York: Columbia University Press.

[xxxix] ibid., p.112.

[xl] ibid., p.115

[xli] ibid., p.118

[xlii] ibid., p.124

Bibiliography

Agence France-Presse (15 January 2010) 'Attacks part of campaign to steal codes, track activists, experts say' *South China Morning Post.*

Agence France-Presse and Reuters (15 January 2010) 'Fellow US technology giants forced to consider their options' *South China Morning Post.*

Arrighi, G. (2005) 'Hegemony Unravelling-1', *New Left Review* 32, March–April,

pp. 23–80.

Arrighi, G. and. Silver, B.J. (1999) *Chaos and Governance in the Modern World System,* Minneapolis: University of Minnesota Press.

BBC (21 January 2010) 'Hilary Clinton calls on China to probe Google attack'. Online. Available at: <http://news.bbc.co.uk/1/hi/world/americas/8472683.stm>

BBC (22 January 2010) 'China condemns "groundless" US criticism of web control'. Online. Available at: <http://news.bbc.co.uk/1/hi/world/asia-pacific/8474011.stm>

Beijing Review (1 October 2009) '60 Years On: The birth and growth of the People's Republic of China', vol.52, no. 39.

Blood, R. (January 2010) 'Google's decision is pragmatic not idealistic'. Online. Available at:

<http://www.rebeccablood.net/archive/2010/01/im_neither_as_impressed_with.html>

Buckley, C. (25 January 2010) 'China steps up defense of Internet controls'. Reuters. Online. Available at: <http://www.reuters.com/article/idUSTRE60L1DK20100125?feedType=nl&feedName=usmorningdigest>

Chase, M. and Mulvenon, J. (2002) *You 've Got Dissent! Chinese Dissident Use of the Internet and Beijing's Counterstrategies*, California: Rand

ChinaScene (22 October 2009) From widely read Chinese media, *China Daily*.

CNET News Staff (24 January 2010) 'Google's challenge in China'. Online. Available at: <http://news.cnet.com/8301-1023_3-10433833-93.html?tag=mncol;txt>

Easton, T. (2009) 'Blow, then burst: China maybe inflating the world's next economic bubble', The World in 2010, *The Economist.*

Elegant, S. (18 November 2009) 'Cyberwarfare: The issue China won't touch', Time in partnership with CNN. Online. Available at: <http://www.time.com/time/world/article/0,8599,1940009,00.html>

Fletcher, O. (18 November 2009) 'China Defense ministry site fends off hackers' IDG News Service. Online. Available at: <http://www.pcworld.com/article/182468/china_defense_ministry_site_fends_off_hackers.html>

Frank, A.G. (1998) *ReOrient: Global Economy in the Asian Age*, Berkeley: University of California Press.

Franklin, D. (2009) Editorial, The World in 2010, *The Economist.*

Gralla, P. (15 January 2010) 'Apple: Still kowtowing to Chinese censorship', Computer World Blogs, Online. Available at: <http://blogs.computerworld.com/15412/apple_still_kowtowing_to_chinese_censorship>

Good Morning China (Aril 2009) 'The Chinese "Machine", Greek monthly magazine supported by the PRC embassy in Greece and the Sino-Hellenic Trade Forum (*author's own translation from Greek*).

Global Times (22 October 2009) 'Google books draws fire over copyrights'.

Henderson, S. (2006) The Dark Visitor: Inside the World of Chinese Hackers. <http://www.lulu.com/content/1345238> and his site <http://www.thedarkvisitor.com/>

Hafner, K. and Richtel, M. (20 January 2006) 'Google resists U.S. subpoena of search data', New York Times. Online. Available at: <http://www.nytimes.com/2006/01/20/technology/20google.html?_r=3>

Hvistendahl, M. (23 April 2009) 'Hackers: the China Syndrome'. Popular Science. Online. Available at: <http://www.popsci.com/scitech/article/2009-04/hackers-china-syndrome>

Huang, C and Reuters (16 January 2010) 'Beijing plays down fallout of Google row', *South China Morning Post.*

Imagethief (12 January 2010) 'Google detonates the China corporate communications script'. ONline. Available at: <http://news.imagethief.com/blogs/china/archive/2010/01/12/google-takes-a-

match-to-the-china-corporate-communications-script.aspx>

Information Warfare Monitor (29 March 2009) 'Tracking *GhostNet*: Investigating a *Cyber Espionage* Network', JR02-2009. Online. Available at: <http://www.scribd.com/doc/13731776/Tracking-GhostNet-Investigating-a-Cyber-Espionage-Network>

Jacobs, A. (13 January 2010) 'Google's threat echoed everywhere except China', *The New York Times.* Online. Available at: <http://www.worldpoliticsreview.com/article.aspx?id=4960>

Jiangtao, S. and Agencies (15 January 2010) 'Beijing stands firm on internet censorship' *South China Morning Post.*

Jia, W. (22 October 2009) 'New era of China-Asean tie-up', *China Daily*.

Karatzogianni, A. (2006) *The Politics of Cyberconflict*, London and New York: Routledge.

Karatzogianni, A. (2009) (ed.) *Cyber Conflict and Global Politics*, London and New York: Routledge.

Karatzogianni, A. and Robinson, A. (2010) *Power, Resistance and Conflict in the Contemporary World: Social Movements: Network and Hierarchies*, New York: Routledge.

Khanna, P. (2008a) 'Waving goodbye to hegemony', *New York Times*, 27 January.

Online. Available at: <www.nytimes.com/2008/01/27/magazine/27world-t.html>

Khanna, P. (2008b) *The Second World: Empires and Influence in the New Global Order*, New York: Random House.

Krugman, P. (24-25 October 2009) 'The Chinese disconnect', *The International Herald Tribune.*

Kwok, K and Chen, S. (15 January 2010) 'Fears that life without Google "will leave the mainland blind", *South China Morning Post.*

Martinsen, J. (13 January 2010) 'Google, Baidu, and wild speulation', Danwei. Online. Available at: <http://www.danwei.org/front_page_of_the_day/google_vs_baidu.php>

Ministry of Commerce website, People's Republic of China. Online. Available at: <http://english.mofcom.gov.cn/>

Minter, A. (27 April, 2009) 'Far from Black and White: Mara Hvistendahl on China's "Patriotic" Hackers', Shanghai Scrap. Online. Availble at: <http://shanghaiscrap.com/?p=2825>

Moscaritolo, A. (20 November 2009) 'Cyberattacks against the U.S. "rising sharply", SC

Magazine, Online. Available at: <http://www.scmagazineus.com/report-cyberattacks-against-the-us-rising-sharply/article/158236/>

Mulvenon, J. and Yang, R. (1999) *The People's Liberation Army in the Information Age*, California: Rand

O'Connor, R. (13 January 2010) 'Google to China: Drop dead – But what took so long?', Alternet. Online. Available at: <http://www.alternet.org/media/145154/google_to_china:_drop_dead_-_but_what_took_so_long>

Perez, B. (15 January 2010) 'Mainland exit could cramp expansion into mobile phones' *South China Morning Post.*

Qiao Liang and Wang Xiangsui (2002) *Unrestricted Warfare: China's Master Plan to Destroy America*, Pan American Pub lishing Company.

Qiu, J.L. (2009) *Working-Class Network Society: Communication Technology and the Information have-less in Urban China*, Cambridge, Massachusetts and London: The MIT Press.

Reid, T. (8 September 2007) 'China's cyber army is preparing to march on America, says Pentagon', *The Times.*

Rowan, D. (August 2009) 'The man with all the answers', *Wired Magazine*.

Scanian, O. (20 November 2009) 'Beijing implicated in US cyber espionage report', www.opendemocracy.org. Online. Available at: <http://www.opendemocracy.net/security_briefings/201109>

Schneier, B. (23 January 2010) 'U.S. enables Chinese hacking of Google'.CNN. Online. Available at: <http://www.cnn.com/2010/OPINION/01/23/schneier.google.hacking/index.html>

Shambaugh, D. (2004) 'China and Europe: the emerging axis', *Current Histor*y, 103,

674, September, pp. 243–8.

Shankland, S. 'China warns U.S. over web censorship stance', cnet news.com. Online. Available at: < http://news.cnet.com/8301-30685_3-10439469-264.html?tag=mncol;txt>

Shiels, M. (14 January 2010) 'Security experts say Google cyber-attack was routine', BBC. Online. Available at: <http://news.bbc.co.uk/1/hi/technology/8458150.stm>

Shujuan, L. (22 October 2009) 'Flutter over new Twitter', *China Daily [Business]*.

Shuo, W. (16 January 2010) 'Shift control – delete?', *South China Morning Post.*

Slocum, M. (14 January 2010) 'Google and China: What's the real story and where does it go form here?', O'Reilly Radar. Online. Available at: <http://radar.oreilly.com.cn/blog/2010/mslocum/google-and-china-whats-the-rea>

Tandon, S. (19 November 2009) 'China ramps up espionage against US: study', AFP. Online. Available at: <http://www.google.com/hostednews/afp/article/ALeqM5ihohq4QxuZLBXKBlFfbEuHs8_NKA>

Tze-wei, Ng and Kwok, K. (23 January 2010) 'Beijing snaps back at Clinton internet criticism', *South China Morning Post.*

Tam, F. (16 January 2010) 'Reporting of search giant's tilt at censors is muzzled', *South China Morning Post.*

The Economist (24-30 October 2009) 'The odd couple', Special Report on China and America.

Vascellaro, J.E., Dean, J. and Gorman, S. (13 January 2010) 'Google warns of China exit over hacking', *The Wall Street Journal*. Online. Available at: http://online.wsj.com/article/SB12633375 7451026659.html?mod=WSJ_hps_LEADNewsCollection

Villenueve, N. (1 October 2008) 'Breaching Trust: An analysis of surveillance and security practices on China's TOM-Skype platform', Information Warfare Monitor/ONI Asia Joint Report, JR01-2008. Online. Available at: <http://www.infowar-monitor.net/breachingtrust/>

Villenueve, N. (12 January 2010) Google's new approach'. Online. Available at: <http://www.nartv.org/2010/01/12/googles-new-approach/>

Villenueve, N. (7 January 2010) 'Malware market'. Online available at:

<http://www.nartv.org/2010/01/07/malware-market/>

Weitz, R. (19 January 2010) 'Global insights: Solving the Goggle cyber mystery', World Politics Review. Online. Available at: <http://www.worldpoliticsreview.com/article.aspx?id=4960>

World Sentinel (21 November 2009) 'Intelligence Ops greatest Chinese threat to United States of America'. Online. Available at: <www.worldsentinel.com/articles/view/129692>

Yang, G. (2009) *The Power of the Internet in China: Citizen Activism Online*, New York: Columbia University Press.

Yanlin, W. and Wenjun, C. (25 October 2009) 'China encourages innovation', *Shanghai Daily.*

Yu, V. (16 January 2010) "Big Brother" a constant, chilling presence for bloggers and activists', *South China Morning Post.*