Christopher R. Hughes

China and the globalization of ICTs: implications for international relations

Article (Accepted version) (Refereed)

Author: Christopher R. Hughes

Title: China and the Globalisation of ICTs: Implications for International Relations

Running Title: China and the Globalisation of ICTs

Abstract

As the People's Republic of China accedes to the WTO, much speculation has been generated about the political impact of the opening of its telecommunications market to foreign firms and investors. Western policy-makers have tended to assume that the effect will be one of political liberalisation, but the view from Beijing sees siliconisation as useful for economic development but not a threat to the socialist one-party political system. This article evaluates the assumptions underlying such views, and draws out the implications for international politics. It procedes by looking at the potential for international economic, technological and security regimes to address the human rights concerns that arise when ICTs are adapted to work in the service of a surveillance state. It also focuses on the political implications that are consequent upon using ICTs for security cooperation between liberal-democratic and authoritarian states. It concludes by arguing that while current regimes are strong on addressing trade and technical issues concerning the globalisation of ICTs, the belief in a kind of technological determinism amongst policy-makers has left international regimes concerned with political issues deliberately weak. As concerns over the impact of the globalisation of ICTs on human rights become increasingly salient at both the international and domestic levels, however, a possible way of redressing this balance might be found in extending a communication analysis of security to include broader political issues.

Keywords: China, democracy, ICTs, Internet, human rights, global governance, globalisation, international security, trade, WTO.

Word Count: 8322

(Main text)

A Chinese Puzzle

‘ ... no nation has yet discovered a way to import the world’s goods and services while stopping foreign ideas at the border. It is in our interests that the next generation in China be engaged by the Information Age, not isolated from global trends shaping the future.’

Since US Secretary of State James Baker heralded the end of the Cold War in the Asia-Pacific with the above statement (Baker 1991/2:16), the idea that the globalisation of ICTs can transform an authoritarian state like China in harmony with American national interests has become something of a mantra for successive Washington administrations. In December 2000, US President Clinton compared cracking down on the Internet in China with ‘trying to nail Jello to the wall’ (Drake 2000).

If this view of the Internet is correct, though, decision-makers in Beijing seem to be remarkably relaxed about the prospect. Not only did China announce 1999 to be the ‘year of on-line government’ and 2000 the ‘year of on-line enterprise’, but in concluding the US-China bilateral agreement on China’s accession to the WTO on 2 February 2000**,** they made sweeping commitments to loosen their control over ownership of the telecommunications sector.

This article will attempt to evaluate the assumptions behind these opposed views over the political impact of ICTs in China and draw out some implications for international politics. As China enters the WTO, this is a worthwhile exercise not only for academic interest, but also due to the ethical considerations that are raised for the policies of foreign governments, international organisations and institutions, and investors and operators in China’s telecoms market.

The WTO Effect

The requirements that China has agreed to for opening up the telecoms sector to foreign investment and services on accession to the WTO will have a sweeping effect on the provision of information-related services in that country. Central to these is the equal treatment principle included in the General Agreement on Trade in Services (GATS) and in the US-China Agreement on accession that requires China to accord to services and service suppliers of other WTO members treatment no less favourable than that it accords to its own like services and service suppliers. This will mean allowing competition to the near-monopoly held so far by China Telecom, permitting significant foreign investment in indigenous enterprises, and abolishing tariff concessions and discriminatory procurement processes. **(**WTO 2000)

Caution is called for, however, before we assume that the consequent impact of the global telecommunications market in China will make ICTs into an effective tool for political transformation along liberal-democratic lines. First of all, it should be borne in mind that the scope of the WTO regime is in fact carefully restricted by

acknowledgements that states can legitimately impose regulations for reasons ranging from the protection of consumers to maintaining the overriding public interest or national security. As a report on e-commerce prepared for the WTO Secretariat puts it, 'Neither the GATT nor the GATS attempts to pronounce on the legitimacy of regulatory objectives as such, as long as the objective is not the protection of domestic industry'. (Bacchetta *et al*. 1998: 65)

That policy-makers in China believe this leaves enough room to impose some fairly comprehensive regulations was demonstrated quite clearly when a comprehensive raft of regulations to enhance state control over activity in cyberspace was introduced on 25 December 2000 (State Council 2000), just seven months after the conclusion of the US-China Agreement on accession. These regulations include, among others, measures that make ISPs responsible for surveilling content and activity that passes through their servers by requiring them to keep records of all content that appears on their sites and all users who dial on to their servers for 60 days, and to hand these records to the security agencies on demand.

The long list of activities that are proscribed by the December 2000 regulations includes familiar Internet crimes, such as the dissemination of pornography, the breaching of copyright and fraud. Yet it also includes activities that 'violate the fundamental principles of the constitution', 'damage national unification', 'damage unity between the different ethnic groups', 'damage state policy on religion by propagating "feudal beliefs"', and 'endanger social stability'. Such crimes may appear to be nothing out of the ordinary, until we realise that Article 1 of the Constitution states that China is a socialist system ruled by the people's democratic dictatorship, that the main challenges to national unification exist in Taiwan, Tibet and the mainly Islamic region of Xinjiang, and the most widespread religious movement is the Falun Gong. Threats to 'social stability' is a catch-all category. The kinds of people arrested for Internet crime since Shanghai-based software engineer Lin Hai was sentenced to two years in prison in early 1999 for providing email addresses to the US-based pro-democracy organisation VIP Reference, however, confirms that such categories can definitely be extended to include pro-democracy activists.

Outside legal opinion tends to agree with the view that regulations such as the above do not conflict with WTO principles. As lawyer Mark Kantor puts it, 'The WTO rules do not, however, mandate free speech or a free press and authoritarian Chinese policies limiting access to uncontrolled information remain legally unaffected by these developments so long as discrimination between foreign and local providers does not occur' (Kantor 2000: 147). Complaints could be made by appealing to the 'fair play' requirements contained in Article VI of the GATS, which stipulates that regulatory decision-making should be conducted in general 'in a reasonable, objective and impartial manner'.

Such a complaint would have to prove that a policy related to the 'overriding public interest or national security' was an unwarranted excuse for the protection of domestic industries. Yet the national security caveat is given considerable scope by the way in which concepts of 'public interest' and 'national security' are not clearly defined by the WTO. It would be a brave company that would want to mobilise their government to challenge China in the WTO on such grounds. Not only would such action mean going through the lengthy and complex procedures of the WTO dispute resolution machinery, it

could also hamper individual efforts to penetrate the Chinese market. No doubt many CEOs in the telecommunications sector will remember the example of Rupert Murdoch, who claimed in September 1993 that satellite TV is a threat to totalitarian regimes the world over, only to witness the Chinese government promptly ban the ownership of private satellite dishes. The following April Murdoch began the process of amelioration by dropping the BBC from his Star TV network covering north Asia and China.

The position of firms bent on entering the Chinese telecommunications market under the WTO rules will be even more exposed than that of Murdoch in 1993, though. This is because the US-China Agreement accepts that they must work with indigenous partners, holding a maximum stake of 49 percent, rising to 50 percent after two years. Domestic Chinese regulations also stipulate that indigenous firms must gain approval from the Ministry of Information Industries (MII) before they are allowed to receive foreign capital, cooperate with foreign businesses or list domestic or overseas stocks (State Council 2000). So far this policy has been applied lightly, tolerating practices such as the listing of China-based stocks in overseas jurisdictions like the Cayman Islands. This indicates that its signficance lies more on the political side than the economic, by providing the MII with an effective veto over which foreign investors and businesses link up with which indigenous firms.

As the state has strong regulatory powers over the behaviour of indigenous players in the Chinese telecoms market, it has, by extension, considerable leverage over their foreign partners. This is partly due to the general lack of clarity concerning the distinction between 'public' and 'private' in the Chinese economic system. At the provincial end of the scale, this can be seen in a set-up like the Lantian Corporation, a local government financed project established to introduce intelligent agriculture in the province of Jilin, using technology donated by IBM, of which Shaun Breslin concludes that it 'isn't exactly state-owned but nor is it wholly private' (Breslin 2000: 24). At the other end of the scale, the US-China Agreement tacitly acknowledges the problem when it accepts that the big state-run telecoms monopolies are to be treated as 'private' firms by the WTO. While this benefits foreign competitors, because state-owned monopolies cannot be exempted from the equal treatment provisions of the GATS, it also means that foreign firms will be working in partnership with state-controlled firms when they claim to be working with the 'private' sector.

Links between indigenous firms and the state are also forged by personal relationships. At one extreme is President Jiang Zemin's son, Jiang Mianheng, who boasts a long list of directorships of Internet firms and has been appointed vice-president of the Chinese Academy of Sciences, making him something of a spokesman for the electronics industry. Or take Eastcom, a leading player in the mobile communications market that is now developing Internet services as a top-level domain registrar under ICANN. This 'private' firm actually grew out of the Equipment Supply Office of the Posts and Telecommunications Bureau of Zhejiang province. A look at Eastcom's board of directors dispells any illusions that Internet startups are the preserve of the young, and confirms that control is still in the hands of personnel who staffed the old state owned enterprises. Seven are over 50 years of age, four over 45, and only two below the age of 35, and 58-year-old chairman and CEO has been distinguished with the Model Worker Medal for Zhejiang Province (Eastcom 2000).

It is important to note this close relationship between the 'private' sector and the state in China when we consider what kind of partnerships are being forged as foreign investors enter the market under the supervision of the MII. Of more political concern is a key partnership like that established in 2001 between Legend Holdings and AOL-Time Warner. Although Legend is not a state owned enterprise, it has been cultivated by the government to be part of a 'national team' of very large enterprises that should be able to compete in the global economy. Since its foundation in 1984 with a $24,000 loan, it has become China's largest personal computer manufacturer, thanks largely to its merger with the Computing Institute of the Chinese Academy of Sciences and financing that derives largely from close ties with the Bank of China (Sutherland 2001).

Part of the appeal of this partnership to AOL-Time Warner is that it will allow AOL to 'bundle' its Internet services software on PC desktops, using the marketing strategy that has worked well in the United States. But this is not the only advantage. As the *International Herald Tribune* put it, 'Legend enjoys cordial relations with China's regulators and a strong reputation among Chinese consumers – assets that could help offset AOL's lack of operating experience in China and ease apprehensions among Chinese officials and consumers that the company will use its services to download US culture into China' (*IHT* 5 June 2001: 13).

With the convergence of interactive digital services and cable television, it is also worth noting that AOL-Time Warner and Rupert Murdoch's News Corporation are also making inroads into the Chinese cable television market. In April 2001, the minister of the State Administration of Radio, Film and TV, Xu Guangchun, announced that these firms would be permitted to broadcast via cable directly to a part of Guangdong Province. At the same time, Xu announced that overseas companies (including those listed in Hong Kong and Taiwan) would be forbidden from taking direct equity stakes in mainland cable TV concerns, unless they confined themselves to just leasing equipment to local companies. It did not go unnoticed that the way had been paved for the triumphs of AOL and the Murdoch empire through the building of personal links between their top managers and the CCP elite, with the head of Star TV, James Murdoch (son of Rupert) describing the banned Falun Gong movement as 'dangerous' and an 'apocalyptic cult', and AOL-Time Warner CEO Gerald Levin introducing the CCP leader as 'my good friend Jiang Zemin' and 'a man of honour, dedicated to the best interests of his people' at a dinner in Hong Kong (*The Guardian* 6 September 2001). It might also be remarked that one of the conditions for granting permission to AOL-Time Warner and News Corporation to broadcast into China was that they should support efforts by China Central Television to broadcast its English-language channel to the US, standing the globalisation of liberalism thesis on its head somewhat (*Financial Times* 5 September 2001).

Commercialisation and the question of architecture

That the state will retain considerable leverage over the behaviour of foreign firms and investors in China's telecoms market under WTO rules has significant political implications that arise from the way in which ICT architecture will develop under market mechanisms. There is certainly awareness amongst Chinese policy-makers that the choice of ICT architecture is not politically neutral, especially when it comes to considerations

of national security. The mass of regulations introduced since 1994 stipulates that computers carrying sensitive information must be separated from the Internet, and puts in place fire walls and machinery to permit surveillance of information flows between domestic and foreign computers. Efforts to develop indigenous architecture and code are also under way, with much attention focused on attempts to make Red Flag Linux an alternative to Microsoft products. Much defensive technical work is also carried out under the auspices of military research and development, with the PLA claiming to have made breakthroughs in areas such as the manufacture of routers capable of resisting information warfare attacks (Liu and Zhang 2000).

Such attempts to adapt the architecture of ICTs in ways that can be used to maintain state security should not be sneered at. China overtook Taiwan in the volume of its hardware production in the middle of 2000, and has joined India in supplying software engineers and services to the world. However, the fact remains that China is entering a global market in which thirty-five out of the world's top thirty-six IT hardware companies (ranked by R&D expenditure) are based in the US. In 1998 Cisco and Lucent, both American corporations, accounted for 52% of the world market capitalisation in the telecoms hardware sector. Their combined market capitalisation was a staggering US$300 bn. Development of the Internet in China has relied heavily on such foreign expertise and investment. The upgrading of the fixed-line network for Internet use has relied largely on buying equipment from Cisco. The fibre-optic transmission trunk that was built in the 1990s was constructed by firms like Lucent, Alcatel, Nortel and Ericsson (Nolan and Hasecic 2000: 167-9).

The MII and security agencies are of course painfully aware of the technological lead enjoyed by foreign firms. Lacking ways to close the gap, they have to try to ensure that a combination of regulation and market mechanisms can harness the expertise possessed by foreign entrants into the domestic market in ways that strengthen the power of the state, and not the reverse. An extensive investigation by Greg Walton for the Montreal-based International Centre for Human Rights and Democratic Development, (Walton 2001) thus details how leading North American and European firms take part in annual 'Security China' trade exhibitions and are supplying crucial assistance for converting the Internet into a massive surveillance system, known as the 'Golden Shield'. Leading foreign firms, he explains, are lured by lucrative contracts with central and local government into helping with the construction of a 'massive, ubiquitous architecture of surveillance', the ultimate aim of which is 'to integrate a gigantic online database with an all-encompassing surveillance network'. This will include linking up cutting edge technologies such as speech and face recognition, closed-circuit television, smart cards, credit records and Internet surveillance technologies.

As Walton points out, the sheer volume of data that is now flowing across ICTs, fuelled by the move towards broadband, means that the technology to control communications is now moving away from old-style firewalls in favour of dispersing monitoring and censorship architecture throughout the system, down to the level of individual PC platforms. It is somewhat ironic that the kind of cooperation between foreign firms and the Chinese state that this requires bears out the argument developed by commentators on the impact of ICTs in the United States who see that the

commercialisation of architecture is having a detrimental impact on civil liberties (Lessig 1999: 39-42).

Whereas the Internet may well have once been a network for the open exchange of information among scientists who believe that knowledge would flourish under conditions of unfettered communication (Naughton 1999), fundamental changes had to occur when the ban imposed on commercial activity by the National Science Foundation of the United States was lifted in 1991. While the massive private investment that this stimulated certainly spread access to the Internet and encouraged the design of more user-friendly technology, new functions also had to be installed in the architecture if the Internet was to be used for business purposes. At a minimum, these facilities include the ability to efficiently collect and process data about users and their activities, usually without them knowing it (Lessig 1999: 39-42).

Chinese observers of the commercialisation of the Internet are just as aware as their foreign counterparts are of developments such as the ability of Microsoft software to transmit information to the Microsoft website without the knowledge of users (Zhang and Ni 2000: 35, 52). Such functions are of course indispensable if commercial organisations are to be able to build customer data bases of immense size and sophistication. As the Internet develops in China largely for the purposes of e-commerce, the same kind of data-collecting architecture is being adopted there as a matter of course.

In fact, Internet firms wanting to perform functions such as the registering of domain names under ICANN, can even be required to install certain kinds of data collecting and processing technology in order to meet international standards. Eastcom, an ICANN accredited firm, thus uses network architecture mostly provided by Cisco and an IBM DB2 Enterprise Extended Edition 7.1 for its database . This is due to the database's ability to 'support business intelligence applications such as data warehousing and on-line analytical processing', and its 'proven ability to help customers find competitive advantage, better customer service or reduced costs by mining their data for the knowledge required to make better decisions.'

The degree to which data collection, processing and censorship of content is now developing into an architecture for the surveillance state appears to come into conflict with elements of international human rights standards. Article 19 of the *Universal Declararation of Human Rights* (Art, 12), for example, declares that: 'Everyone has the right to freedom of expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers'. The right to receive and impart information and ideas regardless of frontiers is also enshrined in the *International Covenant on Civil and Political Rights*, to which China signed up in 1998.

It is more than likely, however, that human rights may be a poor foundation upon which to appeal against measures taken to control ICTs under the rubric of maintaining national security. Just as with the WTO, both the *Declaration* and the *Covenant* also legitimate sweeping powers for states to maintain 'morality, public order, general welfare in a democratic society' (*Declaration*, Art. 29) when the protection of national security or public order, or of public health or morals is at stake (*Covenant*, Art. 19). The kinds of activities that are outlawed in Chinese cyberspace, such as publishing content that is 'subversive', 'supports cults', 'harms the reputation' of China or hurts efforts to 'unify' Taiwan with the PRC, can be seen as lying entirely within this list of exceptions. Perhaps

Perry Keller sums up the overall situation at present when he points out that the international regimes developed so far to underpin a Global Information Society have been established by economic law, leaving the 'other foundational leg' of international human rights law less well developed (Keller 2000: 267).

Global Governance?

If the global regimes established to govern international trade and human rights are too weak to have a significant impact on the ways that states use ICTs to surveil their citizens, the types of international organisation established to oversee their technological standardization cannot be expected to play much of a role either. In fact, these are carefully designed in ways that deliberately prevent them being able to intervene in domestic politics. Take the case of ICANN. As the organisation charged with overseeing the allocation of IP number blocks, maintaining the Internet root server system, determining the policy for adding new Top Level Domains (TLDs), and coordinating the assignment of technological parameters, ICANN has enormous potential power to shape the architecture of the Internet. Yet while ICANN expects accredited registrars like Eastcom to install powerful data collecting and processing architecture, it has no power to constrain national security agencies from mining the data that is collected.

A look at the structure of ICANN reveals how it is an organisation carefully crafted so as to be too weak to ever mount a challenge to the authority of states, or to be 'captured' by any one state. It is precisely to ensure this that the Clinton adminstration established ICANN as a private, non-profit-making organisation. Granted, a token gesture of democratic governance has been lent to ICANN by making nine of its nineteen directors 'at large' representatives of five 'world regions', elected by an on-line ballot that was conducted in October 2000. The lucky winner for the 'at large' directorship to represent all Internet users in the Middle East, Pakistan, India, China, Japan, Australia, Afghanistan and 'countries to the East', including the East Indian Ocean islands and Antarctica, (but excluding US and L.American possessions) was the Maryland-based Japanese employee of Fujitsu, Masanobu Katoh, who polled no less than 13,913 votes! That China finds this type of democracy acceptable is clear from the fact that it supported the establishment of ICANN and endorsed its principles when it joined the inaugural meeting of ICANN's Governmental Advisory Committee on March 2 1999.

While international organizations dedicated to the economic and technological governance of ICTs are de-politicised, however, the state-centric nature of the international system seems to provide little incentive for addressing political concerns at the global level. Perhaps the greatest pressure mitigating against such cooperation is the need to maintain international security. This is quite simply because, if the porosity of borders heralded by the globalisation of ICTs really poses a threat to the Chinese state, it poses a threat to all other states as well. Schneier neatly sums up the situation when he points out that: 'Any organised crime syndicate with enough money to launch a large-scale attack against a financial system would do well to find a country with poor computer crime laws, easily bribable police officers, and no extradition treaties' (Schneier 2000: 21). The implication of this is that the greater the threat posed to state jurisdiction and international order by interconnectivity, the stronger will be the counter-measures that have to be taken by states to protect their sovereignty and maintain order.

This is not a new phenomenon. As Frederick points out, 'Throughout history, one clear pattern is apparent. Every time a new innovation in communication technology appears, sooner or later international law arises to regulate it.' (Frederick 1993: 245) But the degree of interconnectivity presented by a technology like the Internet means that all states have an increased stake in ensuring that it is regulated in less-developed economies such as China, if holes are not to be created through which the 'Four Horsmen of the Information Apocalypse' (Schneier 2000: 67), namely terrorists, drug dealers, money launderers, and child pornographers, can ride out. This has the potential to generate a serious conflict between the principles of order and justice at the global level.

The way in which this predicament stands the liberal vision of globalisation on its head, however, can be seen when states that hold very different political values have to collaborate to maintain security. In November 2000, for example, a network was cracked that involved the use of the Internet by criminals in China and the Republic of China on Taiwan to illicitly siphon off money from a South African bank. Such successful police action must have resulted from extensive co-operation between the security agencies from both sides of the Taiwan Strait, yet their governments do not even talk to each other.

The challenge that such international cooperation presents liberal-democracies has become clearer since the terrorist attacks that took place against New York and Washington on 11 September 2001. When leaders of the states that make up the Asia-Pacific Economic Cooperation forum (APEC) issued a statement on counter-terrorism at Shanghai on 21 October, for instance, they called for measures to counter 'all forms of terrorist acts'. These measures included the following: strengthening activities to protect critical sectors, including telecommunications; cooperation to develop electronic movement records systems that will enhance border security; strengthening capacity building and economic and technical cooperation to enable member economies to put into place and enforce effective counter-terrorism measures (APEC 2001). APEC, however, includes states as diverse as China, the United States, Australia, Brunei, Canada, Chile, Hong Kong, Indonesia, Japan, Malaysia, Mexico, New Zealand, Papua New Guinea, Peru, Philippines, Russia, Singapore, South Korea, Taiwan, Thailand and Vietnam.

The context for surveillance cooperation between states with different domestic political regimes is already being put in place by the convergence of domestic legislation around the world. In the case of China, it is clear that the MII that China is looking to foreign legislation for ideas on how to exert state control over the flow of information **(**Zhang and Ni 2000: 271-92). The parallels can be quite remarkable. For example, Chinese legislation now requires ISPs to keep records of all content and all users that appear on their servers for scrutiny by the security agencies if required. In the United Kingdom, the Regulation of Investigatory Powers (RIP) Bill also requires every ISP to retain all communications data originating or terminating in the UK, or routed through UK networks. Employers in the UK are permitted to monitor the email of their staff, and the Home Office is considering granting powers to the security agencies to have access to records of every phone call, email and internet connection made in Britain. The director general of the national criminal intelligence service, Roger Gaspar, even compared the proposed new data bank to the national DNA database under development (*The Guardian* 4 December 2000).

Yet, as Mathiesen points out with reference to the integration of European Union databases, even democratic parliaments are not equipped with sufficient knowledge and

insight, or enough power, to monitor how security agencies collect and use data (Mathiesen 1999: 31). When data is exchanged between states, this problem is magnified. Serious questions over the implications for civil liberties that arise from exchanging data on citizens between member states of the European Union, for example, were raised when the House of Lords held an inquiry into the linking up of European Union databases. More relevant to the case of China is that the inquiry acknowledged that there was growing pressure from third countries for access to such information, and warned that this may aggravate the risk of error or misuse as it may not always be clear which data protection rules apply and which, if any, body is responsible for supervising the data flows' (House of Lords 1998-9: 17).

As the exchange of data becomes ever broader, accountability is inevitably weakened, especially when it extends to a state like China, which lacks the balancing institutions being put in place by liberal-democratic governments to protect citizens from unwarranted surveillance, such as data protection officers and legislation. Yet the European Union, since 1999 at least, has been exploring the possibility of exchanging information on individuals accumulated on its various intelligence databases with the United States and Russia (House of Lords 1998-9: 12). Not only are both of these states, as APEC members, now committed to collaborating with each other in the war against terrorism, but Russia is also a member of the 'Shanghai Six', which brings it together with China, Uzbekistan, Kazakhstan, Kyrgyzstan and Tajikistan to maintain security in Central Asia. The main concern for China in Central Asia has long been the secessionist movement of the Islamic Uighur population in Xinjiang under the rubric of its 'strike hard' campaign. Its fight against 'splittists' is of course much wider, taking in areas such as Tibet and Taiwan as well. As there is still no internationally accepted definition of 'terrorism', though, it is unclear where international cooperation starts and ends on such issues.

It may be the case that the need to maintain international order gives liberal-democracies a strong incentive to turn a blind eye to draconian measures adopted by a state like China to maintain security in its portion of cyberspace. At worst, as liberal-democracies are faced by the threat of terrorism -- let alone lorry loads of illegal immigrants appearing at their borders -- they will have to give in to pressure to exchange information with the security agencies of authoritarian states and assist them in ensuring that their areas of cyberspace are well monitored. The Information Revolution, therefore, is already being followed by something of a counter-revolution, as states seek to restore order.

Or virtual Realism?

It would be wrong, however, to conclude that the international need to exchange information between databases means that that there are no ways to limit the ways in which they manipulate the shape and usage of ICTs. The most compelling case for political accountability, however, is based not on human rights concerns but on the growing awareness of the military vulnerabilities consequent upon the growing dependence on globalised ICTs for economic purposes. After all, if there is near hysteria in the United States over the prospects of information warfare (CSIS 1998), the Chinese military is equally concerned over the threat to their national security posed by an over-

reliance on hardware and software sourced from American based firms (Liu and Zhang 2000).

This mutual concern over security provides a far stronger motivation for developing institutions to regulate ICTs at the global level than do fears over human rights abuses. Particularly pressing, for example, is the need to evolve international law in ways that can re-define the legitimate use of force in a way that keeps up with technological change. In particular, such a development implies the evolution of a new interpretation of the UN Charter and customary international law that can accommodate the definition of cyber-warfare as a form of the use of force. Without such a definition, it will be difficult to decide what constitutes legitimate self-defence against cyber-warfare. Moreover, when such definitions are decided, they will have to be made enforceable by the construction of multilateral treaties that facilitate tracking, attribution and trans-national enforcement (Grove et al. 2000: 99-100).

Despite the need to evolve the laws of war to cope with cyber-attacks, however, limitations on information can already be found in agreements such as the 1947 declaration on *Measures to be Taken Against Propaganda and Inciters of a New War*, in which the UN General Assembly condemned 'all forms of propaganda, in whatsoever country conducted, which is either designed or likely to provoke, or encourage any threat to the peace, breach of the peace or act of aggression (Frederick 1993: 251). Moreover, given the weaknesses of international human rights regimes, it is somewhat ironic that another body of international law that already acknowledges the need for constraints on the use of information to attack states is the *Covenant on Civil and Political Liberties.* This is because Article 20 of the *Covenant* prohibits the transmission of certain types of information that constitute propaganda advocating war, or advocating national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence. It could also be argued that the 'communication analysis' of peace and war that can already be found in some international institutions should be extended to cover ICTs. The most notable example of this is the preamble to UNESCO's constitution, which points out that 'since wars begin in the minds of men, it is in the minds of men that the defences of peace must be constructed'. It continues by adding that 'State parties ... are agreed and determined to develop and to increase the means of communication between their peoples and to employ these means for the purposes of mutual understanding and a truer and more perfect knowledge of each other's lives' (Frederick 1993: 253).

The relevance to China of this connection in international law between communication and peace can be illustrated by some fairly dramatic examples: When the Chinese embassy in Belgrade was hit by Nato missiles on 8 May 1999, the Beijing municipal authorities not only felt the need to bus students in to besiege Western embassies, they also established a 'Sacred Sovereignty' website where people could express their outrage, learn the e-mail addresses of Nato governments and political parties, and study the techniques of hacking and service-denial attacks. Even the most liberal of the Party-controlled newspapers published such addresses and reported hacking attacks with pride (*Beijing Qingnian Bao* 1999). Since then, waves of hacking attacks have been launched against traditional foes in Taiwan and Japan. In August 1999, over 7,000 attacks were made on public web-sites in Taiwan following an announcement by the island's president that was seen in China as tantamount to a declaration of independence. Taiwanese hackers responded with some eight waves of their own attacks

until the call went out for a ceasefire (Liao 1999). Chinese hackers have attacked Japanese sites, too, most conspicuously when a conference was held in Osaka in January 2000 to discuss whether the 1937 Nanjing Massacre was a fabrication. At one point, some 1,600 strikes were launched against the Bank of Japan's computer system within the space of seven minutes. Moreover, this kind of information warfare is becoming increasingly organised, as demonstrated by the waves of hacking attacks launched against sites in the United States almost exactly a month after a US reconnaissance aircraft was forced to land on Hainan Island by Chinese jet fighters on 1 April 2001 (Hughes 2001).

Given the linkage in international law between certain types of propaganda and warfare, it is worth asking who should be held responsible for this burgeoning international aggression in Chinese cyberspace. The Chinese state itself cannot avoid all culpability, when the CCP has been using ICTs to mobilise nationalism to legitimate its own claim to power. The foreign ministry web site, for example, promotes the CCP's view of its mission of national salvation in the international context, the 'Strong State Forum' of the *People's Daily* is a hotbed of nationalist fervour, and the electronic version of the PLA newspaper, *Liberation Army Daily*, reminds surfers from time-to-time of the existence of China's nuclear deterrent during times of tension with in foreign relations. Other sites are aimed at more specific nationalist projects, such as those used by 'united front' organisations to promote Beijing's version of Tibetan identity (http://www.tibet-web.com), and to promote 'unification' with Taiwan by helping Taiwanese who want to invest in the mainland (http://www.tailian.org.cn). In this respect, the Internet is being used as another example of what Althusser calls 'ideological state apparatuses', along with schools, the legal system, culture, religion and the media (Althusser, L. 1978: 244).

The resulting activity that occurs in Chinese cyberspace indicates how difficult it is for the state to stop the nationalistic politics that it so assiduously cultivates from spilling over and threatening to destabilise foreign relations. This phenomenon can be seen unfolding since at least 1998, when the Internet was used to disseminate information inside China about atrocities committed against the ethnic Chinese community in Indonesia following the fall of the Suharto regime. A patriotic student movement soon burgeoned, and when news was posted that the Chinese foreign ministry was adopting a soft policy towards Jakarta (a sensible stance calculated not to risk reprisals against the Chinese-Indonesians), outbursts of anger in the chat rooms showed that citizens were not impressed by the failure of their government to stand up for compatriots overseas. Disappointment with the government's stance turned to disgust and patriotic condemnation when the Beijing municipal authorities refused to grant permission for a demonstration to the Indonesian embassy, organised partly by Internet (Hughes 2000).

Similarly, when the *People's Daily* web site tried to ameliorate soured Sino-Japanese relations by setting up a 'China-Japan Forum', the result was a barrage of anti-Japanese invective. Prominent members of the government, including even foreign minister Tang Jiaxuan, have suffered probably the worst possible accusation possible for a Chinese citizen, being condemened as a pro-Japanese traitor. Even criticism of the failure of President Jiang Zemin's Taiwan policy appeared on the *People's Daily* website shortly after the election of the secession-orientated Chen Shui-bian as the island's president in March 2000.

Seen from this angle, the impact of the Information Age is indeed having an impact on Chinese politics. A survey conducted under the auspices of the Chinese

Academy of Social Sciences found that 60.8 percent of respondents believe that the Internet is giving them more opportunity to express their political views, 51 percent think it gives them more opportunities to criticize government policies, 55.9 percent think it gives them a better knowledge of politics, and 43.8 percent think it will allow high officials to have a better understanding of the views of the common people (Guo 2001). Yet there is little reason to assume that this net increase in political activity amounts to the importation of 'foreign ideas' or enhances international stability in the way that James Baker had expected at the end of the Cold War. One of the first messages to appear on the 'Strong State Forum' chat room after the terrorist attacks on the United States of 11 September, for example, read, 'Now is the best time to attack Taiwan' ('Zhunbei' 2001). More of the same kind of material, along with a wave of anti-American rhetoric, appeared over the following days.

Although ICTs play a role in the organisation of pro-democracy campaigns, dissident activities by non-Han ethnic groups, and the organization of religious movements like the Falun Gong *outside* Chinese firewalls, there is no evidence so far of the Internet playing a significant role in such campaigns *inside* the country. This may be due in part to the way in which the state has continued its well-established tradition of stifling dissent by imposing harsh penal measures well into the Information Age. That the arrests that have taken place for pro-democracy related activities since the imprisonment of Lin Hai in 1999 have not been very numerous, indicates the success of a traditional policy of 'killing the chicken to frighten the monkeys', rather than leniency on the part of the state (Keller 2000: 265). Some foreign observers have already noticed that a strong culture of self-censorship over Internet usage has already developed (IHT 2000). Such a pattern of behaviour fits in well with a tendency for post-colonial states with an authoritarian bent to build what Zinnbauer has called 'the paralysing perception of a surveillance state' (Zinnbauer 2000: 28).

While evidence of ICTs being used for democratic activity and organisation remains thin, though, nationalist activity grows by the day and by the international crisis. It is important to acknowledge the existence of such a tendency, because it draws our attention to the need to understand the political impact of ICTs as being partly determined by cultural norms that originate outside cyberspace. This observation is in line with the theoretical perspective developed by critics of the Internet such as Lawrence Lessig, who draws our attention to the importance of the manipulation of what he calls 'norms' in the regulation of cyberspace (Lessig 1999: 85-8). Social scientists such as such as Castells also emphasizes the close relationship between culture and the use of ICTs, as when he reminds us that 'The transition between modes of development is not independent of the historical context within which it takes place; it relies heavily on the social matrix initially framing the transition, as well as on the social conflicts and interests that shape the transformation of that matrix' (Castells 1999: 21).

It is only when we escape from deterministic mythologies about the nature of technological change and acknowledge the reality of this kind of complex political relationship between ICTs and international security, that a more realistic way of thinking about global governance can be developed. The fact that international institutions favour the actions of sovereign states to maintain domestic order, does not mean that political choices on issues of global importance are impossible regarding ICTs so long as the relationship between communication and state 'security' is properly understood. As

lawyers know all too well, the very existence of international law is only made possible in the present world system by the realisation that states need to adhere to certain standards of behaviour if they are to preserve both themselves and the overall system (Bull 1977). Approaching the problem of global ICT governance from this perspective of the self-interests of states is likely to have far more support from governments around the world than is the advocation of human rights and liberal-democracy. Perhaps it is only when the nexus between communication, international security and human rights is properly understood, that the extension of global governance to the political sphere can become a feasible project.

Communications, order and justice

It has been argued above that the advent of the 'Information Age' presents a more complex picture than that of authoritarian states being transformed by waves of 'foreign ideas' and 'global trends shaping the future'. While the case of China shows that the globalisation of ICTs does have a political impact on states, this tends to reflect attempts to manipulate architecture and the collection and processing of data for the causes of strengthening the legitimacy and security of regimes, rather than the promotion of liberal-democratic transformation. The following tentative conclusions can also be drawn:

First, assumptions that the Information Age will be a benign global force for upholding human rights and enhancing social stability could be dangerously misleading if they excuse policy-makers and citizens from addressing the serious political issues that do arise from the impact of ICTs. The case of China provides ample evidence to remind us that the impact of ICTs is determined as much by the political and cultural contexts within which they are embedded, as it is by the nature of the technology itself.

It is equally misleading to view ICTs as politically 'neutral' technologies. Walton gives us the perfect example to illustrate the dangers of such an understanding when he describes how images recorded by UK-manufactured cameras installed during the 1980s to monitor traffic in Tiananmen Square were broadcast on Beijing television after the crushing of the 1989 democracy movement in order to help the police trace and punish participants in the events (Walton 2001). The installation of surveillance technology in Chinese ICTs is no more politically neutral than was the construction of low bridges on the roads to Long Island by Robert Moses was, for the purpose of stopping immigrants and the poor reaching his beaches.

This is an important point to bear in mind when assessing the role of investors and firms with their bases in North America and Europe. As such actors are playing a decisive role in shaping the kind of architecture that is being developed in China, they are already coming under scrutiny from human rights organisations. This began to happen when the New York-based Human Rights Watch started to call on foreign ICT firms to stop turning a blind eye to repression after the arrest of Huang Qi and his wife Zeng Li in June 2000. Their crime was to have allowed their 'www.6-4tianwang.com' website, used mainly to help find missing people, to carry a demand for the political rehabilitation of the 1989 Democracy Movement by a former Beijing professor who had lost his son in the Tiananmen Massacre (Human Rights Watch 2000). Walton's report for the International Centre for Human Rights and Democratic Development has taken the criticism of the role of foreign firms in helping to construct a surveillance state a significant step further.

Yet if the globalisation of ICTs is neither an automatic transmission belt for liberal-democratic values, nor politically neutral, then the political dynamics that result from this process need to be properly addressed by international institutions. Leaving the global governance of ICTs to organisations concerned with trade and technical standards is far from sufficient, and can even make the situation worse.

Managing the political impact of the Information Age demands that our understanding of the relationship between security, communication and human rights is developed in ways that can keep up with the pace of technological change. While maintaining international security will remain of paramount concern, especially since 11 September 2001, if appealing to the interests of states in their own preservation leads to the buildingof a comprehensive and attributable global regulatory system, this also needs to take into consideration human rights concerns. In a world system that remains state-centric despite the globalisation of ICTs, taking concerns over security as the starting point from which to address broader social issues may be a feasible project for those concerned about the promotion of international human rights standards. It is certainly a more effective way of addressing the real political problems that have to be faced in the Information Age than is starting out from assumptions that the social values of any particular society will inevitably be disseminated throughout the world.

References

Althusser, L. (1978) 'Ideology and Ideological State Apparatuses', *Lenin and Philosophy and Other Essays* (Vol. 3) New York: New Monthly Review Press.

APEC (2001), 'APEC Leaders Statement on Counter-Terrorism', 21 October, URL (consulted Oct. 2001): www.apecsec.org.sg

Bacchetta, M., P. Low, A. Mattoo, L. Schuknecht, H. Wagner, M. Wehrens, (1998), *Electronic Commerce and the Role of the WTO*, Geneva: World Trade Organisation.

Baker, J.A. III (1991/2), 'America in Asia: Emerging Architecture for a Pacific Community', *Foreign Affairs*, 70(5): **pp ??**

Breslin, S. (2000) 'The Virtual Market', *China Review*, Autumn/Winter 2000: 22-24.

Beijing qingnian bao (*Beijing Youth Daily*) (1999), '*Hulianwang shang de jiaoliang*' ('*Showdown on the Internet*'), 11 May: 2.

Bull, H. (1977), *The Anarchical Society*, London: Macmillan.

Castells, M. (1999) *The Informational City*, Oxford: Blackwell

CSIS Taskforce**,** (1998) *Cybercrime... Cyberterrorism... Cyberwarfare ... Averting an Electronic Waterloo*, Washington: CSIS Press.

Drake, W.J. (2000), 'Dictatorships in the Digital Age: Some Considerations on the Internet in China and Cuba', *iMP: The Magazine for Information Impacts*, October 2000, URL (consulted Nov. 2000): http:www.ceip.org

Eastcom (2000), URL (consulted Nov. 2000): www.eastcom.com.

Frederick H.H. (1993), *Global Communication and International Relations*, California: Wadsworth.

Grove, G.D., Goodman, S.E., Lukasik, S.J. **(**2000**)**, 'Cyber Attacks and International Law', *Survival* 42(3): 89-104.

Guo, L. (2001), '*Hulianwang shiyong zhuangkuan ji yingxiang de diaocha baogao*', ('Report on a Survey into The Conditions and Influence of Internet Usage'), URL (consulted 1 July 2001): www.Chinace.org.ce/itre

House of Lords, (1998-9) Select Commitee on the European Communities, *European Union Databases*, 23rd Report, Session 1998-99, London: The Stationery Office.

Hughes, C.R. (2000), 'Nationalism in Chinese Cyberspace', *Cambridge Review of International Affairs*, 13(2): 195-209.

- (2001), 'Nationalist Chat', *The World Today*, 57(6): 6-8.

Human Rights Watch (2000), 'China: Foreign Companies Should Protest Internet Detention', URL (consulted 27 June 2000): www.hrwatchnyc.igc.org

IHT (*International Herald Tribune*) (2000), 5 October **(title and page?).**

Kantor, M. (2000) 'Foreign Direct Investment in Chinese Telecoms: Changes in the Regulatory Scheme, *Cambridge Review of International Affairs*, 13(2).

Keller, P. (2000) 'China's Impact on the Global Information Society', in Christopher T. Marsden (ed.), *Regulating the Global Information Society*, London and New York: Routledge.

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

Liao Minru (1999), '*Liang an haike zhan – bu fen wangyou fen tingzhi*' ('Cross-Strait Hacking War - Some Hackers Want to Call a Stop'), *Lianhe Bao* (*United Daily News*, Taiwan – overseas edition), 14 August: 3

Liu, Y. and W. Zhang 2000, 'High-Tech Development and State Security', *Jiefangjun bao* (*Liberation Army Daily*), 11 January: 6. (English version in BBC Summary of World Broadcasts, FE/3764 G/6).

Mathiesen, T. (1999), *On Globalisation of Control: Towards an Integrated Surveillance System in Europe*, London: Statewatch.

Naughton, J. (1999) *A Brief History of the Future: The Origins of the Internet*, London: Weidenfeld and Nicolson.

Nolan, P. and Hasecic, M. (2000) 'China, the WTO and the Third Industrial Revolution', *Cambridge Review of International Affairs*, 13(2): 164-80.

State Council (2000), '*Hulianwang xinxi fuwu guanli banfa*', ('Methods for Managing Internet Information Service'), URL (consulted Nov. 2000): http://www.cnnic.net.cn/policy/18.shtml

Schneier, B (2000) *Secrets and Lies: Digital Security in a Networked* World, New York: John Wiley and Sons Inc.

Sutherland, D. (2001), 'Policies to Build National Champions: China's "National Team" of Enterprise Groups', in Peter Nolan, *China and the Global Business Revolution*, Palgrave, Basingstoke and New York.

Walton, G (2001) *China's Golden Shield: Corporations and the Development of Surveillance Technology in the People's Republic of China'* Montreal: International Centre for Human Rights and Democratic Development, URL (consulted 29 October 2001): http://www.ichrdd.ca/frame.iphtml?langue=0

WTO (2000), US-China WTO Agreement, URL (consulted Nov. 2000): http://www.usChina.org/public/wto/ - bilat

Zhang, C. and J. Ni (2000), *Guojia Xinxi Anquan Baogao*, (*Report on National Information Security*), Renmin Chubanshe: Beijing.

'Zhunbei zao da' (2001), message posted on *People's Daily Strong State Forum* under pseudonym 'Prepare to strike early, strike hard, strike with nuclear war', URL (consulted Sept. 12 2001): http://bbs.people.com.cn/

Zinnbauer, D, 'Whither the Panopticon?: Civil Society Activism and State Surveillance in the Age of the Internet, Some Evidence From Malaysia', research paper delivered to Development Studies Institute, L.S.E., November 2000.