Fighting the smokeless war: ICTs and international security

Book section

FIGHTING A SMOKELESS WAR: ICTs AND INTERNATIONAL SECURITY

(8403 WORDS)

Christopher R. Hughes

Several chapters in this volume have shown how the Chinese leadership places ICTs at the heart of the state's economic development strategy. Despite attempts to create an indigenous information industry sector, however, the hard reality remains that the core research and development upon which technologies like the Internet depend, as well as key administrative institutions like ICANN, [1] are based in the United States.[2] The emergence of such a degree of dependence is stimulating intense debates over the relationship between ICTs and international security in the PRC, in which the discussion revolves around a set of problems that can loosely be grouped under the heading of 'information warfare'.

Some writers trace the origins of information warfare back to the ancient Chinese strategist Sun Zi, who advocated achieving victory through deception, knowing the mind of the enemy and gathering intelligence.[3] History is in fact littered with examples of information determining the course of war. The United States may never have entered the First World War if the British had not intercepted and deciphered the 1917 Zimmerman Telegram that revealed a plan for the Germans to ally with Mexico.[4] The increasing sophistication and efficiency of ICTs, however, combined with the global integration of

networks, creates new potentials for information warfare which dramatically magnify its importance as a strategic threat.

In one respect this can be seen in the new possibilities for projecting what Keohane and Nye call ‘soft power’, the ability to establish norms, institutions and agendas through propagating one’s own culture and shaping the preferences of others.[5] Yet the spread of the Internet has also made possible new kinds of aggressive measures that can seriously disrupt important social infrastructures. These include actions such as triggering data overload, spamming and attacking software with viruses, Trojan horses and ‘worms’. It is also possible for manufacturers and engineers to leave hidden trapdoors in systems that make unwarranted surveillance possible. Great damage and inconvenience can also be caused by ‘hacking’, and even physical attacks by electromagnetic pulse, electronic countermeasures, and conventional military strikes.[6]

The implications of such developments for international security are still open to wide ranging debate in military circles throughout the world. On the one hand, radical proponents of what has come to be known as the Revolution in Military Affairs (RMA) propose that future conflicts will be decided by ‘cyber warfare’, aimed at disrupting, disabling or exploiting critical information nodes, and ‘net war’ that involves deception and psychological operations to influence the behaviour of the enemy through deterrence and the shaping of perceptions.[7] On the other hand, sceptics claim that information warfare presents more of an Achilles’ Heel for the technologically advanced societies in which both military and civilian critical infrastructures are highly dependent on digital

networks, raising the spectre of an 'electronic Pearl Harbour',[8] or an 'electronic Waterloo'.[9] Some commentators even suggest that technological backwardness and authoritarian politics might in themselves offer protection against information warfare. As Henry and Peartree put it, 'What use will niche-casting propaganda be against an enemy leader who does not have satellite television or an Internet connection? In 1997, half of the world's population had never even made a telephone call'.[10]

The PRC, an authoritarian developmental state going all out for siliconisation, thus presents an interesting case study. While the country is under-developed by many standards, the rate of connectivity among the elite urban population is far from politically insignificant. President Jiang Zemin himself has a personal Internet connection and logs on regularly. Such a situation thus presents Chinese policy-makers with something of a double-edged sword when it comes to considerations of security. While the technological lag behind potential adversaries, such as Japan, Taiwan and the United States, makes the country vulnerable to attack, new opportunities are also arising for launching information warfare against societies that have a very high degree of dependence on digital networks. This chapter will assess how policy-makers in China are responding to such a dilemma by looking at the debate ranging across a broad range of organisations, including the military, state ministries, the CCP and academia.

FIGHTING A SMOKELESS WAR

From an American perspective, the ability for new technologies to carry ideas across China's borders is not necessarily a bad thing. Secretary of State James Baker began to develop this theme at the end of the Cold War, when he explained, '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'.[11] Vice-President Al Gore was even more upbeat when he launched the Global Information Infrastructure (GII) project in March 1994, explaining that, 'To promote ... to protect ... to preserve freedom and democracy, we must make telecommunications development an integral part of every nation's development. Each link we create strengthens the bonds of liberty and democracy around the world.'[12] Secretary of State Madeleine Albright also claimed that the accelerated development of the Internet and telecommunications in China after its accession to the WTO would have an impact on the human rights and political situation by increasing contact with Americans and other foreign trading partners,[13] and reducing the power and reach of government censorship.[14]

From the point of view of the CCP leadership, though, the propagation of American culture and values inside China is part of what Deng Xiaoping called the 'smokeless war' to undermine the socialist system through a process of 'peaceful evolution'.[15] Chinese academics thus warn about the ways in which ICTs can destabilise politics by making it easier for new actors to organise themselves and challenge the status quo, strengthen Western pressures for 'global governance', and lead to the development of transnational organisations and structures that challenge the maintenance of 'information borders' and 'information sovereignty'. Concerns are also expressed over the ways in which the new

international regimes that are emerging to regulate the use of ICTs tend to be determined by the degree of hard and soft power that the most technologically advanced states are able to exert. Meeting the consequent challenges to state sovereignty is made even more complex, they claim, because the Internet magnifies the sources of post-Cold War instability in areas such as financial markets, environmental problems, terrorism, and non-military intervention in the domestic affairs of other states.[16]

Such concerns are located within a comprehensive analysis of the impact of ICTs on national security contained in a joint report by the Ministry of Information Industry (MII) and the CCP's Central Policy Research Office. This proposes that the threat of information warfare should be understood within a broad vision of global power that is based on an up-dated version of Mao Zedong's theory of the 'Three Worlds'. Just as Mao believed that the world was divided into three tiers of states, with the superpowers at the top, the developed states in the middle and the developing states at the bottom, in the information age is also supposed to be three types of state. At the top of the pile is the 'information hegemony state', asserting its control by dominating the telecommunications infrastructure, software development, and by reaping profits from the use of information and the Internet. After this comes the 'information sovereign state', exemplified by those European states that have accumulated sufficient know-how to exert independent control over their information resources and derive profits from them, and to protect themselves from information hegemony. At the bottom of the pile are the 'information colonial and semi-colonial states', which have no choice but to accept the information that is forced on them by other states. They are thus left

vulnerable to exploitation because they lack the means to protect themselves from hegemonic power.[17]

According to this theory, the present international situation has already revealed how certain states can combine their traditional military and economic advantages with their lead in information technology in order to contain the development of the PRC, exploit its resources, destroy its culture, and attack its politics, military and economy. By waging psychological warfare through e-mail and electronic newspapers, wreaking destruction by leaving Trojan horses and viruses in software that is sold to China, and by leaving 'back doors' in hardware, the technologically advanced states can obtain advantages that they cannot gain through military means.[18] The overall result is a kind of virtual Realism, in which the survival or death of the PRC and its ability to take initiatives in the struggle for development depends on whether it can consolidate and expand its 'information territory' and preserve 'information borders', defined not by geography but by the scope of politically influential information and the building of strong 'spiritual defences'.[19]

The armed forces are equally concerned about the threats posed to national security by information warfare. Among their fears are developments such as the provision of serial numbers for Intel processors since the launch of the Pentium III, which could allow foreign powers to identify users and provide them with access to all kinds of possibly sensitive information. Similarly, Microsoft operating systems since the launch of Windows 98 are viewed with suspicion due to their ability to interact with hardware and generate a code related to the user's name and address which can be transmitted to the

Microsoft Website. Viruses are also a cause for concern. The CJH virus, for example, is claimed to have caused Chinese enterprises an overnight loss of more than RMB1 bn. at one point in 1999. The military also believe that the United States Secret Service disabled Iraqi air defences during the Gulf War by installing chips with a virus in computer systems that Iraq had acquired from France, which could be triggered by remote control.[20]

Debates in the main military newspapers thus show a high degree of concern over the implications of ICTs for military strategy and doctrine.[21] The vulnerablity of support systems to information warfare, for example, is a prominent theme in articles on military logistics published 2001 and brought together in a special edition of the online 'Military Affairs Salon' of the *People's Liberation Army News*.[22] The consensus on this topic is that informatization is essential in an age of increasingly mobile, multi-theatre, integrated warfare. As one report in the *People's Liberation Army News* points out, for instance, under the Ninth Five-Year Plan large amounts of capital were invested in informatization of the military's medical service, with the establishment of over 50,000 Websites and some 38 model informatized hospitals.[23] Yet such developments are held to present the enemy with a growing number of soft targets. Meanwhile, Chinese commentators draw attention to how the Pentagon has has continually upgraded the importance it attaches to its ability to conduct information warfare, evidenced by the emphasis given to information technology in its 2001 *Quadrennial Defense Review Report*,[24] and by the way in which it has been spending large amounts of capital on researching the use of viruses to disable and disrupt enemy computers since at least 1987.[25]

BUILDING INFORMATION BORDERS

Faced by such threats, military analysts urge building what some have called an 'Internet Great Wall' (*wangluo changcheng*).[26] Part of this involves defensive measures like the development of decentralised, mobile and stealthy information systems rather than concentrated and large-scale IT structures. National security information in particular, it is argued, should be located in distributed and localised systems.[27] There is also an awareness that securing information borders against the possibility of information warfare requires the mobilisation of all the nation's military and civilian expertise. This is reflected, for example, in the linkage made by military leaders between the world Revolution in Military Affairs and Jiang Zemin's ideological campaign of the 'Three Represents', which advocates that the CCP should represent 'China's advanced productive forces, the orientation of China's advanced culture, and the fundamental interests of the overwhelming majority of the people in China'. General Fu Quanyou, Chief of Staff and member of the Central Military Commission (CMC), sees such an ideology as being compatible with the strategies and tactics of 'modern people's war'.[28]

Such a view represents an interesting twist in the development of military doctrine that has been going on since the death of Mao Zedong in 1976. This originally moved away from the theory of 'people's war', according to which the enemy will be worn down by guerrilla tactics after penetrating deep into Chinese territory, towards one of 'active defence' along a 'strategic boundary' to stop an enemy before it can penetrate the

country's external borders.[29] High-technology took an increasingly central role in this doctrinal development thanks largely to international events like the expulsion of Argentine forces from the Falkland Islands by the Royal Navy in 1982, but most spectacularly the 1991 Gulf War. It was this conflict that most dramatically revealed how the integration of ICTs with battlefield activity through satellite links, tracking and targeting systems, and airborne warning and control systems (AWACS), can enhance command, control, communications, and intelligence (C3I) capabilities.

In 1993 the Central Military Commission thus announced a new doctrine of preparing to fight 'high-technology local wars under modern conditions' (xiandai tiaojian xia de gaojishu jubu zhanzheng). A further push towards high technology followed in 1997, just after the stand-off with the United States' Seventh Fleet during the Taiwan Strait crisis of the previous two years. It was then that the Central Military Commission announced the 'two basic changes' (liangge jibenxing zhuanbian) of: 'change from dealing with local wars under ordinary conditions to winning local wars under modern technology, especially high technology, conditions; change from an army of number and scale to an army of quality and efficiency, and from a manpower-intensive to a technology intensive army'.[30] President Jiang Zemin took this theme up when he made his report to the Fifteenth Congress of the CPC in September 1997 and promoted the professionalization of the PLA in order to fight a defensive war under conditions of high technology and advocated the building of a 'strong technological army'.[31]

Within these preparations for high-technology warfare, the concepts of electronic and information warfare have been recognised as special types of campaign. According to testimony by an official from Taiwan's Ministry of National Defense, Beijing began to develop plans for information warfare as early as 1985, started to implement them in 1995, and began to conduct exercises using computer viruses to interrupt broadcasting systems and military communication systems in 1997.[32] By the late 1990s articles in the *People's Liberation Army News* were openly discussing tactics such as disrupting an enemy's communications systems through ensuring electromagnetic control, combining 'active interference with passive interference, electronic interference with repressive interference'.[33] They might have been encouraged in this thinking by incidents such as the 'Army After Next' Winter War Games held by the United States military during the late 1990s, in which more than 50 per cent of the home side's military information infrastructure was degraded by laser and electromagnetic pulse bomb attacks on its communications satellites as the mock battle began.[34]

Information warfare has certainly become a central theme in military manouvres. A national training campaign to create a 'strong technological army' was launched at the end of 1998, and information warfare was pushed still higher up the military agenda at the time of the 1999 Nato campaign against Serbia. Many of the military exercises held at this time involved online simulated combat, often between 'red' and 'blue' teams, with the scenario being a conflict over Taiwan or with the states neighbouring the South China Sea. Some, such as the exercises held in the Lanzhou military region in October 1998, focused specifically on electronic surveillance and counter-surveillance, disruption and

counter-disruption, and destruction and counter-destruction measures. Special training corps for cyberwarfare have also been established in some areas, such as the one established by an armoured division in the Nanjing Military Region to coach personnel in computer skills, software development and Internet warfare. Information warfare is also treated as a central element of combined-forces operations involving manouvres coordinated by advanced information systems, and tactics such as launching electromagnetic attacks to degrade the enemy's information systems. Teaching aids on information warfare are compiled by the various branches of the armed forces, drawing on experiences from wars fought by other armies around the world, using CD-ROMs to provide accounts of basic concepts, techniques and weaponry.[35] Researchers in Taiwan claim that the PLA has already reached a fairly advanced stage in its ability to use information technology to achieve command and control of the battelefield in any conflict with the island, and to launch an attack concentrating on soft targets such as computer networks used for banks, business and transportation.[36]

The broadening out of the 'technological army' to embrace expertise among the general population began to be developed most visibly by middle-ranking military cadres after the humiliation of the PLA by the intervention of the United States Navy in the Taiwan Strait crisis of 1995-6. The most notable example is the emergence of the doctrine of 'unlimited warfare', advocated by Qiao Liang and Wang Xianghui, both linked to the PLA Airforce Academy. Drawing broadly on a range of Western and ancient Chinese strategists, Qiao and Wang advocate defeating the overwhelming military power of the United States by using information warfare conducted via the Internet, combined with

trade war and various permutations of terrorism, biological warfare, smuggling and the disruption of financial systems.[37] Such warfare would be 'popularised' (pingmin hua) in the sense that combatants would include teenage hackers as much as military professionals. Qiao and Wang are careful to point out, however, that the high degree of expertise required by such individuals distinguishes their doctrine from Mao's idea of 'arming the whole population'.[38]

Such views have fallen on fertile ground in the context of the upsurge of popular nationalism that was triggered largely by the Taiwan Strait crisis and further stimulated by the bombing of the PRC embassy in Belgrade in May 1999. There is ample evidence to show that the Internet was being used to launch information warfare from the PRC as early as 1998, when Indonesian Websites were targeted following the wave of atrocities committed against ethnic-Chinese Indonesians after the fall of the Suharto regime. Following the Belgrade incident, a much larger wave of activity took place against the Websites of NATO organisations, governments, and political parties. Similarly, when the president of Taiwan, Lee Teng-hui, made a statement seen in the PRC as tantamount to a declaration of independence on 9 July 1999, over 7,200 attacks were launched against public Websites on the island.[39] Public Websites in Japan were also attacked in January 2000 when historians held a conference in Osaka questioning the historical truth of the Nanjing Massacre. At one point, some 1,600 strikes were launched within the space of seven minutes against the Bank of Japan's computer system.

This kind of cyberwarfare seems to have been getting more organised. In part, this can be seen in a growing division of labour, according to which 'freshmen' attack mainly vulnerable commercial Websites under the guidance of more experienced hackers called 'knights'. There also appear to be organised groups of hackers in the making. A 'Chinese Hackers' Union' claimed to have gathered over 1000 members within 12 days of the forced landing of a United States surveillance plane on Hainan Island after its collision with a Chinese fighter plane on 1 April 2001, who began placing Chinese flags and portraits of the missing Chinese pilot on United States Websites from April 30 onwards. Others quickly followed with similar actions, such as the 'Honkers Union' (literally 'red guests'), who claimed to have defaced some 700 United States Websites by the evening of 3 May. A portrait of Chairman Mao was the calling card left by another group, composed of radical leftists calling themselves the 'Chinese Hawks' and known for earlier attacks on Websites such as those run by the religious Falungong movement.

Although such aggressive activity appears to be the result of largely spontaneous campaigns, there is some evidence to suggest that the state support it at times. Successful hacking attacks against United States government computers after the Belgrade embassy incident, for example, were reported with a degree of pride in party-controlled newspapers, which printed the addresses of United States government Websites.[40] The Beijing municipal authorities even set up a special 'Sacred Sovereignty' Website on which people were encouraged to express their outrage over the Belgrade bombing, and from where they could obtain the email addresses of NATO governments and political parties. Military commentators have also urged the establishment of 'information warfare

brigades' that bring together expertise from across the whole spectrum of society, noting the example that has been set by the recruitment of hackers by states like the United States, India, the United Kingdom, France, Russia, Japan and Israel.[41] The use of the Internet by the Falungong movement outside China to spread its message inside the country and around the world has also been met with what looks like a systematic campaign of cyber-wafare against its Websites.

THE MILITARY-INDUSTRIAL NEXUS

The civilian authorities also have a major role to play in coordinating the mobilisation of computer expertise among the population at large. In part, this means changing the way that people think about information technology by instilling in users a sense of responsibility that will encourage them to install and develop the right kinds of systems for maintaining security. The development of professional support structures is also recommended, in the shape of enterprises dedicated to computer security which can act as 'Internet police' and 'Internet clinics', while also strengthening the research and development into core technologies.[42]

The civilian authorities are also charged with bringing about the improved co-ordination of the relevant organisations and laws that have developed alongside the growth of the Internet. As Wacker has shown above, the various agencies concerned with information security have already put in place a comprehensive set of regulations to control domestic

activity on the Internet. It is also worth stressing, though, that the development of this regulatory and organisational framework has been largely in response to developments that have taken place outside China. The first arrest that took place under the new raft of regulations was related to international activity, namely the case of Lin Hai. Lin was charged on 25 March 1998 with 'inciting subversion of state power' by providing large numbers of Chinese email addresses to 'hostile foreign publications', such as *VIP Reference*, a newsletter compiled by Chinese democracy advocates in Washington and sent to hundreds of computer users in China. When Wang Youcai was arrested in July 1998 he too was accused of sending email messages to dissidents in the United States while trying to organize an opposition party.

Apart from some efforts to combat domestic computer crime (particularly bank fraud) that began in the early 1980s, the fact that the regulatory project really began in March 1994 can also be seen in part to be a response to international events. This, after all, was the same time that Al Gore announced the Global Information Infrastructure initiative, and just when the Internet was beginning to break out of what Giese calls its 'academic ghetto' in China. Moreover, the reason why the Internet was able to spread beyond the campus at this time was the impetus provided by commercialisation following the lifting of the ban on commercial activity on the Internet by National Science Foundation of the United States in 1992. It was this policy more than any other that allowed the Internet and the World Wide Web to develop into the popular means of global communication that we know today. Combined with developments in other ICTs, such as satellite television, Western policy-makers were increasingly upbeat about the potential power of ICTs to

bring about the transformation of authoritarian states. The atmosphere at the time was encapsulated by Rupert Murdoch's famous hailing of satellite television as a threat to totalitarian regimes everywhere, as well as Gore's proclamation that the GII would be a force for the promotion of freedom and democracy.[43]

The security organs in China were thus well aware that there was a widely held belief in the West that the emerging communications networks could be used to exert 'soft power'. As well as developing regulations to control activity, they thus began to build defensive measures into the architecture of the Internet, such as the restriction of international links to four gateways located in the cities of Beijing, Shanghai and Guangzhou. Regulations introduced in January 2000 require all computer information systems involving state secrets to be neither directly nor indirectly linked with the international Internet.[44] At the same time it was also reported in the PRC press that Chinese companies were forbidden to buy products with encryption software designed by foreign countries, and no domestic organisation or individual would be allowed to sell foreign commercial encryption products.[45]

Policy-makers are aware, however, that such measures taken to prepare for information warfare will remain weak unless China's indigenous technological base can be raised to international standards. As Minister of Information Industry, Wu Jichuan, points out, China must not only adopt the right domestic countermeasures to stand up for its own interests and those of the developing world and avoid becoming an 'information colonial state' or 'semi-colonial state', it must also learn to work with other states. Needless to

say, the very rapid pace of technological development and the digital gap with the United States makes this a daunting task. Part of the solution is sought in the integration of the military and civilian information industry sectors.

This kind of integration can be said to have begun, in fact, when military science and technology began to be transferred to the civilian sector in 1985. Integrating the two sectors was further boosted when the Ninth Five Year Plan (1996-2000) aimed to raise the efficiency and international competitiveness of scientific and industrial research by exposing it to market demand and developing partnerships with foreign firms. Jiang Zemin took the civilian-military link a step further in his report to the Fifteenth Congress of the CPC in September 1997 when he advocated the establishment of an 'orbital defence industry mechanism that interacts with the socialist market economy system'.[46] Section 24 of the current Tenth Five-Year Plan also sees defence industries as being of strategic economic importance. It urges that they should be combined with the civilian sector to promote the task of 'strengthening the armed forces through science and technology', and promises to accelerate the building of 'a technology-intensive army, streamline the armed forces in a Chinese way, increase their capability of fighting defensive wars under conditions of modern technology, especially high technology, and be prepared to meet any contingency'.[47] Some military commentators are also arguing for the armed forces to strengthen logistical management techniques by learning from and helping to strengthen the civilian e-commerce sector, apparently influenced by an initiative in this area taken by the United States Department of Defense in 1999.[48]

The PLA can, in fact, claim to have played a key role in meeting the challenge of the Information Revolution, by reportedly having devoted more than 400 million work days and organized 25 million vehicle trips to participate in and support 10,000-odd key national and local infrastructure projects, including the laying of 20,000 kilometers of optical cable telecommunication lines. It is also claimed that the military has used its advanced scientific and technological achievements over the past five years to support more than 1,000 national economic construction projects, solve urgent problems for more than 150 scientific research projects, transfer some 10,000 scientific and technological findings to the civilian sector, train nearly one million scientific and technological personnel, and help civilian enterprises complete 900-odd technical transformation projects which enabled 320 enterprises to get out of the red and become profitable.[49]

On the civilian side, many of today's key corporations in the information industry sector began to flourish under initiatives such as the '863 Plan', launched in March 1986 as a response to the Reagan administration's 'Strategic Defense Initiative' (or 'Star Wars'), under which the Chinese government aims to promote world leading high technology firms. In 1999 the State Ministry of Science and Technology decided to make defence-related information technology a high priority within this scheme, bringing academic and scientific research organisations together with large enterprises to lay the foundations for the 'leapfrog style development' of a new state information infrastructure based on indigenously developed Chinese technology, with a special emphasis on key Internet technologies such as routers.[50] This scheme was given a new shot in the arm in February 2001, when the government marked its fifteenth anniversary with an injection of USD 1.8

bn. into the State High-Technology Research and Development Plan, with development of the information industry and especially information security at the top of the agenda.[51] The Ministry of Science and Technology has also established special production bases in Chengdu, Southwest China, and in Shanghai to concentrate on the development and manufacture of security-related information technology.[52]

Some of the key players in the 'national team' of very large enterprise groups that have been fostered by such initiatives to survive in the global market are to be found in the IT sector. The Legend group is a good example. Founded in 1984 with a USD 24,000 loan, by 1999 it had grown to be the largest electronics goods producer in China and the fifth largest in Asia, with its main product being PCs. A merger with the Computing Institute of the Chinese Academy of Sciences (CAS), and financing that derives largely from the Bank of China, gives Legend close links with the state.[53] A similar example is the Capital Iron and Steel Group, which announced in March 2001 that it was teaming up with the Beijing Association of Science and Technology to establish an international information automation research centre to engage mainly in intelligence information processing as well as high-tech research and development in complicated system and intelligence control. The automation research institute products they have developed include a dialogue system between humans and machines, advanced robot-controlled machines and lie detectors. Military analysts claim that there have already been encouraging signs in the indigenous development of applied technology and materials technology that can be used to build an information security umbrella. In 2000, the construction of a routing

device that can withstand test attacks was hailed as a great success in building a 'strategic pass for information resources entering and leaving national territory and borders'.[54]

Despite such optimism, however, there is also a realisation in China that the preservation of national, economic and personal security is being made ever more complex by the increasingly widespread use of ICTs among the general population. This was one of the points stressed by the director of the Bureau of Public Information Network Security Control (under the Ministry of Public Security), Li Zhao, when he adddressed a special meeting on how to deal with the 'Code Red II' virus in August 2001.[55] Yet when it comes to controlling the behaviour of the population, there is already something of a comic air surrounding attempts to stop 'spiritual pollution' through crude measures such as the mass closure of Internet cafes or campaigns by the Beijing municipal authorities to confiscate satellite television receiving equipment.[56] ICTs have in fact already developed beyond the stage where such measures can be effective. As Walton explains, the sheer volume of data that is now flowing across ICTs, fuelled by the move towards broadband, means that the technology used to control communications is 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.[57] The only way to achieve such levels of sophistication in China is to harness foreign know-how to the cause of strengthening national security.

WESTERN KNOWLEDGE TO PRESERVE CHINESE ESSENCE

Sometimes foreign know-how can be appropriated directly, by acquiring the information technology necessary for waging information warfare from leading North American and European firms. According to Taiwan's Ministry of Defence, the PRC has introduced advanced technology from Britain and France for use in simulated wars. Walton details how leading North American and European firms take part in annual 'Security China' trade exhibitions and supply 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.[58]

Appropriating foreign technology to safeguard national security poses a serious problem, however, because the United States sees maintaining the global dominance of its own information industry as constituting a national security objective.[59] From this perspective, the granting of limited access to the PRC telecommunications and Internet market that was included in the China-United States agreement on PRC accession to the WTO is highly significant as a way by which to introduce foreign technology to China. The trick for the Chinese side was to secure agreement that foreign firms and investors can only operate in the Chinese market if they form partnerships with indigenous firms. Moreover, according to domestic PRC regulations, such partnerships have to be approved by the

MII.[60] The MII is thus left with considerable leverage to influence the behaviour of foreign firms in the PRC.

The kind of partnership that is evolving under this formula is already becoming clear as multinational enterprises such as Microsoft, AOL-Time Warner and Hong Kong Telecom form partnerships with members of the PRC's 'national team'. Microsoft paved the way when it struck a deal with Legend in March 1999 to develop boxes to enable Internet access via television sets. At the same time, Microsoft CEO Bill Gates also announced in the Special Economic Zone of Shenzhen a 'strategic cooperation plan' with Rupert Murdoch's Hong Kong Telecom. There is little reason to expect that such firms will operate as agents of 'peaceful evolution' in China. There has been much speculation in the world's press, for example, that Murdoch is only able to play a significant role in the Chinese market because of the considerable lengths to which he has gone to restore his credibility with the Chinese leadership since his 1993 statement about cable television undermining authoritarian regimes. This has included banning the BBC from his Star TV service for China and North Asia, helping Deng Xiaoping's daughter publicise the biography of her father around the world, and criticism of the Dalai Lama for good measure. As for AOL-Time Warner, the *International Herald Tribune* summed up the situation well when it chose Legend as its partner to enter the market for Internet services in May 2001, stating: '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 United States culture into China'.[61]

In September 2001 AOL-Time Warner and Murdoch's News Corporation again made significant inroads into the PRC telecoms market when Xu Guangchun, minister of the State Administration of Radio, Film and Television, announced that they would be permitted to broadcast directly to a part of Guangdong Province.[62] 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 television 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. The head of Star TV, James Murdoch (son of Rupert) is reported to have described the banned Falun Gong movement as 'dangerous' and an 'apocalyptic cult'. At one dinner in Hong Kong, AOL-Time Warner CEO Gerald Levin is said to have introduced the CCP leader as 'my good friend Jiang Zemin' and 'a man of honour, dedicated to the best interests of his people'.[63] Moreover, it also became apparent that the PRC is not entirely powerless when it comes to spreading its own 'spritual pollution' around the world when it was revealed that these foreign corporations had agreed to throw their support behind efforts to permit China Central Television's (CCTV) English-language channel to broadcast in the United States.

It is important to note, then, that Chinese policy-makers do not see any incompatibility between maintaining national information security and working in harmony with foreign interests. This also applies to the way in which the Chinese government is trying to work in accordance with the practices of international society. Indeed, a considerable part of the MII-CCP report is concerned with explaining the nature of legislation introduced by technologically advanced states to control the use of ICTs.[64] Jiang Zemin himself has emphasised that the internationalisation of the information network demands regulation at the international level and has called for more active Chinese participation in the organizations that draw up relevant treaties, as well as a stepping up of international exchanges and cooperation in this field.[65]

In this respect, PRC policy makers are aware that their own efforts to maintain information borders can be considerably strengthened by the growing international awareness that the globalisation of ICTs poses a threat to the security of all sovereign states. In fact, it is precisely because the Internet does not recognise borders that leaving any part of it unregulated will create a loophole for activities that can destabilise any other part of the world. Such activities range from organised crime syndicates launching large-scale attacks against financial systems, to drug dealing, money laundering, the spreading of child pornography and terrorism.[66]

Just as in the field of conventional warfare, states have already been made painfully aware that mutual restraint is needed to avoid unneccessary mutual damage being inflicted by information warfare. Internationally, the possibility of new kinds of

destruction has already led to a growing movement to modernise the laws of war to accommodate the information age. 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 the use of force. Without such a definition, it will be difficult to decide what constitutes legitimate self-defence. 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.[67]

There are already indications that electronic information warfare is starting to conform with this dynamic anyway. When Taiwan's hackers responded to assaults on their island's computer systems from the PRC in 1999 with eight waves of their own attacks, for example, the chaos became so great on both sides that calls for a ceasefire went out. Similarly, the PRC authorities were made painfully aware of the consequences of encouraging cyberwarfare to be launched from their own territory after hacking attacks against United States targets following the Hainan spy-plane incident triggered off counter-attacks by American hackers. An official of the State Office for Computer Network and Information Security claimed that 13.8 per cent of attacks on international networks between the middle of April and early May that year had been aimed at mainland China. One technician claimed that the networks of the enterprise he worked for had been probed and scanned no less than 80,000 times a day, with 100 actual attacks per day. [68]

The disincentives for engaging in information warfare become even more serious when other governments see the PRC as a likely adversary in any digital conflict. The United States is clearly the most significant potential adversary in this respect. But technologically advanced societies like Japan and Taiwan are also very important. In August 1999, for example, the Ministry of National Defence of the ROC on Taiwan announced that it had established a committee to deal with information warfare to counter moves by the mainland, which would invite experts and party representatives to study its comprehensive strategy to combat information warfare.[69] Among twelve measures announced in the National Defense Policy White Paper issued by the Democratic Progressive Party of Taiwan, just before Chen Shui-bian won the presidential election in March 2000, was the deployment of digital forces and the development of corresponding doctrines to increase the flexibility, mobility, and general readiness of the island's standing forces.[70] Such plans have not gone without notice in Mainland China, especially the establishment of a special Internet warfare unit, the 'Tiger Brigade' (*laohu dui*), in January 2000, let alone the talent that the island has shown for creating computer viruses.[71]

The need for self-restraint and regulation at the international level becomes even more pressing when third party states are liable to be drawn into cyber conflicts, either due to the way in which packets of data travel through their part of the Internet as they find the least congested route between any two points in the world, or through the deliberate use by hackers of servers in third countries to launch attacks on their enemies. In the wake of

the Hainan spy-plane incident, for example, South Korea's Ministry of Information and Communication felt the need to warn government organisations, universities and private institutions to take precautions against Chinese and American hackers using their Internet sites as a stopover to attack each other's computer systems. Seoul also set up a special task force under the Korea Information Security Agency (KISA) to provide professional support and advice for possible victims.[72]

Although an international legal structure for controlling information warfare is still lacking, however, conditions within which cooperation on international information security can take place are already being put in place. One aspect of this is a steady convergence between the domestic legislation enacted within various states around the world. Sometimes the parallels are striking. 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, meantime, the Regulation of Investigatory Powers (RIP) Act also requires ISPs to retain all communications data originating or terminating in the United Kingdom, or routed through United Kingdom networks. Employers in the United Kingdom 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.[73]

In addition to this convergence between the domestic regulations introduced by states around the world, well before the events of 11 September 2001 it was also clear that interconnectivity was driving states with very different political systems and cultures to move towards international collaboration on issues of information 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.[74] 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.

Collaboration between states can also be seen in the growing tendency to share information on individuals and organisations that is accumulated on digital databases, again well before 11 September 2001. When the United Kingdom's House of Lords held an inquiry into this phenomenon in 1999, it was so concerned that it felt the need to issue a strong warning about the dangers of giving in to pressures from third party countries for access to data on EU databases while it remained unclear which data protection rules could be applied and which body, if any, was responsible for supervising data flows.[75] Among the states with which the EU has been exploring the possibility of exchanging data accumulated on its various intelligence databases were the United States and Russia.[76] This chain could be extended further by the fact that Russia is a member of the 'Shanghai Six', under which it cooperates with the PRC, Uzbekistan, Kazakhstan, Kyrgyzstan and Tajikistan to maintain security in Central Asia. This is the region, of

course, where the PRC has long been engaging in a ‘strike hard’ campaign against the secessionist movement of the Islamic Uighur population in Xinjiang.

The events of 11 September 2001 have, of course, immensely strengthened this tendency towards international cooperation on issues of state security. The agreement signed on 21 October 2001 at the APEC summit in Shanghai committed several states, among them the United States, the PRC and Russia, to taking measures to counter ‘all forms of terrorist acts’. This includes working together to strengthen activities to protect critical sectors, including telecommunications; cooperation to develop electronic movement records systems that will enhance border security; and strengthening capacity building and economic and technical cooperation to enable member economies to put into place and enforce effective counter-terrorism measures.[77] At the global level, too, states have been called on by the UN Security Council to accelerate and intensify the exchange of operational information regarding the actions or movements of terrorist organizations, and specifically in relation to their use of information technology.[78] It needs hardly be stated that the concept of ‘terrorism’ is yet to be defined by international law. The activities that the Security Council connects it with are broad enough, though, including ‘transnational organized crime’, trade in illicit drugs, money laundering, illegal arms trafficking and the movement of potentially deadly materials. Perhaps the most visible indication of how the pendulum has swung from notions of justice towards international order is the uncertain fate of the CIA’s project to sponsor SafeWeb to provide software to enable anonymity for Internet users in authoritarian states such as the PRC.[79]

CONCLUSION

It has been argued above that the Information Revolution and the spread of the Internet is seen to pose a threat to the national security of the PRC by elements in the military, the government, the CCP, academics and the general population. Responses are thus being devised at all levels, ranging from military doctrine and training, to domestic regulation, industrial policy, and international cooperation. Perhaps the range of policy positions being proposed is best encapsulated by the various recommendations made by delegates to the Chinese People's Political Consultative Conference (CPPCC), when this united front organisation discussed issues of network security in March 2001. Yang Yixian, a CPPCC delegate with professional expertise in the development of Internet security systems, suggested that a nongovernmental organ be set up between government departments and enterprises according to international practice, with the task of managing all problems involving network security in a unified way and avoiding possible loopholes caused by the barriers between different state bureaucracies or regions. Hong Kong delegate Lau Nai Keung stressed the need to make full use of his territory's international status to set up an authoritative international cooperative organization that could intensify international cooperation in the management of the network. Mi Zhenyu of the PLA's Academy of Military Sciences, on the other hand, proposed that China's information industry should concentrate its energies on developing indigenous software and hardware products. Meanwhile, Xu Wenbo, secretary-general of the 'Network Civilization Project Organizing Committee', urged the government to intensify control, examine and screen unhealthy contents, and promote national culture in the network environment.[80]

It is the task of top-level authorities like the MII to render such different recommendations into a coherent whole. The response to the various suggestions made at the CCPPCC meeting from Zhang Chunjiang, Vice Minister for Information Industry (one of the authors of the MII-CCP report discussed above), was that building network security is indeed a complex job calling for legal support, technical guidance, and cultural involvement. From the perspective of bureaucratic politics, it might be added, there is also a piece of the cake for just about anybody who can portray the information age as a threat to national security. In this respect, it is important to note that the above discussion took place in the context of the unveiling of the Tenth Five-Year Plan.

Yet, despite the complexities of the security problems generated by digitalisation, it has been argued above that policy-makers do also look to the increasing global interconnectivity of digital networks as a source of strength when it comes to building network security. When looking at some of the more extreme visions of information warfare, we would do well to remember that this is not the first Revolution in Military Affairs to have taken place in history. The age-old need for states to exercise self-restraint and engage in cooperation for the sake of maintaining order and security provides reasons for believing that the dangers posed by information warfare will have to be dealt with at the international level in the same way that other kinds of technological developments have eventualy fallen under regimes of global governance. Events since 11 September 2001 have served to reinforce this tendency. It is not hard to unravel this paradox when we think about the nature of state security. As Buzan points out, ‘States of

all types benefit from the widespread feeling among individuals that anything is better than reversion to the state of nature. So long as the state performs its Hobbesian task of keeping chaos at bay, this service will be seen by many to offset the costs of other state purposes, whatever they may be'.[81]

Seen from the longer historical perspective of Chinese nation-building, policy-makers in the PRC thus face the task of harnessing the forces that are generated by economic and technological globalisation in ways that buttress national information security rather than erode it. In many ways, this is an interesting extension of the nineteenth-century neo-Confucian formula of using Western functional knowledge (*yong*) to preserve Chinese essence (*ti*).[82] Or, as Jiang Zemin put it in a July 1991 speech to commemorate the 70th anniversary of the founding of the CCP, 'take the ancient to serve the modern, the foreign to serve China' (*gu wei jin yong, yang wei zhong yong*).[83] It is thus that China's long revolution continues into the information age.

---

[1] ICANN, the Internet Corporation for Assigned Names and Numbers, is a private organisation established by the Clinton administration to administer the addresses upon which the direction of digital traffic on the Internet depends. See the chapter by Ermert and Hughes in this volume for the politics and international controversies surrounding this organisation.

[2] On the relative strengths of information industry in the PRC and the United States see P. Nolan and M. Hasecic, 'China and the Third Industrial Revolution', in *Cambridge Review of International Affairs*, vo. 13, no. 2, pp. 164-80.

[3] H. Ryan and E.C. Peartree, 'Military Theory and Information Warfare', in Henry and Peartree (eds), *The Information Revolution and International Security*, Washington DC: CSIS Press, 1998, p. 108.

[4] H.H. Frederick, *Global Communication and International Relations*, California: Wadsworth, 1993, pp. 220-222.

[5] R.O. Keohane and J.S. Nye Jnr., 'Power and Interdependence in the Information Age', *Foreign Affairs*, 1998, vol. 77 no. 5, p. 86.

[6] CSIS Taskforce**,** Global Organized Crime Project, *Cybercrime... Cyberterrorism... Cyberwarfare ... Averting an Electronic Waterloo*, Washington: CSIS Press, 1998.

[7] J. Arquilla and D. Ronfeldt, 'Information Power and Grand Strategy: In Athena's Camp', in S.J.D. Schwartzstein (ed.), *The Information Revolution and National Security*, Washington DC: CSIS Press, 1996.

[8] Henry and Peartree, 'Military Theory and Information Warfare', p. 116.

[9] CSIS Taskforce**,** Global Organized Crime Project, *Cybercrime... Cyberterrorism... Cyberwarfare ...*

[10] Henry and Peartree, 'Military Theory and Information Warfare', p. 120.

[11] J.A. Baker III, 'America in Asia: Emerging Architecture for a Pacific Community', *Foreign Affairs*, 1991/2, vol. 70 no. 5, p. 16.

[12] Al Gore, 'Remarks Perpared for Delivery to International Telecommunications Union, Buenos Aires', 21 March 1994. Online. Available HTTP:

<http://www.iitf.nist.gov/documents/speeches/032194_gore_giispeech.html> (accessed 20 February 2002).

[13] M. Albright, 'Permanent Normal Trade Relations for China, Remarks at Agilent Technologies Health Care Solutions Group', 6 April 2000. Online. Available HTTP: <http://secretary.state.gov/www/statements/2000/000406.html> (accessed 3 April 2002).

[14] M. Albright, 'Address to the World Trade Center' Denver, Colorado, 9 May 2000. Online. Available HTTP: <http://secretary.state.gov/www/statements/2000/000509a.html> (accessed 6 February 2002).

[15] Deng Xiaoping, 'Women you xinxin ba zhongguo de shiqing zuo de geng hao' ('We Have the Confidence to Conduct China's Affairs Better'), *Deng Xiaoping Wenxuan, di san juan*, (*Selected Works of Deng Xiaoping, Vol. 3)*, Beijing: Renmin chubanshe, 1993, pp. 325-6.

[16] Yu Xiaoqiu, 'Dui xinxi jishu yu guojia anquan ruogan wenti sikao' ('Some Considerations on Information Technology and National Security'), *Xiandai guoji guanxi* (*Contemporary International Relations*), 2001, vol. 3, pp. 6-12.

[17] Zhang Chunjiang and Ni Jianmin, *Guojia xinxi anquan baogao*, (*Report on National Information Security*), Beijing: Renmin chubanshe, 2000, pp. 37-8.

[18] Zhang and Ni, *Guojia xinxi anquan baogao*, pp. 4-5.

[19] Zhang and Ni, *Guojia xinxi anquan baogao*, pp. 4-5.

[20] Y. Liu and W. Zhang, 'High-Tech Development and State Security', *Jiefangjun bao* (*Liberation Army Daily*), 11 January 2000, p. 6. (English version in BBC Summary of World Broadcasts, FE/3764 G/6, 15 February 2000).

[21] See the special edition on information warfare of 'PLA Military Affairs Salon Online' ('Jiefangjun bao wang ban jun shi shalong') of *Jiefangjun bao* (*PLA News*). Available HTTP: <http://www.pladaily.com.cn/item/vote/hacker/content/002.htm> (accessed 14 May 2002), and the special edition on 'The Logistics Front' ('houqin zhanxian'). Online. Available HTTP: <http://www.pladaily.com.cn/gb/hqzx/2001/06/04/sjlq.html> (accessed 14 May 2002).

[22] See in particular, Song Shikui 'Jianli kuaqu lianhe baozhang wangluo' ('Establish a Cross Region United and Secure Internet'), *Guofang bao*, 12 July 2001, p. 3. Online. Available HTTP: <http://www.pladaily.com.cn/gb/jskj/2001/07/12/20010712017055_jslt.html> (accessed 14 May 2002); Yang Liuguo, 'Zhishi houqin baozhang de te zheng' ('Characteristics of Securing Knowledge Logistics'), *Guofang bao*, 4 June 2001, p. 3. Online. Available HTTP: <http://www.pladaily.com.cn/gb/hqzx/2001/06/04/20010604017060_hqggrd.html> (accessed 14 May 2002); Weng Changling, 'Xinxi fangwei – xinxi zhanzheng de zhongyao yi huan' ('Information Defense – An Important Link in Information Warfare'). Online. Available HTTP: <http://www.pladaily.com.cn/item/vote/houqing/content/7-015.htm> (accessed 14 May 2002); and the various comments in the special edition on logistics in *Jiefangjun bao*, 10 April 2001, p. 6. Online. Available HTTP: <http://www.pladaily.com.cn/gb/hqzx/2001/04/10/200104100001081_hqggrd.html> (accessed 14 May 2002).

[23] 'Wo jun weisheng xinxihua jianshe chuju guimo' ('Informatisation of the Military Medical System Takes Shape'), *Jiefangjun bao* (*PLA Daily*), 6 November 2001, p. 1.

Online. *Jiefangjun bao wang ban jun shi shalong*. Available HTTP: <http://www.pladaily.com.cn/gb/hqzx/2001/11/06/20011106001006_hqggrd.html> (accessed 14 May 2002).

[24] Department of Defense (United States), *Quadrennial Defense Review Report, September 20 2001*. Online. Available HTTP: <http://www.defenselink.mil/pubs/qdr2001.pdf> (accessed 14 May 2002).

For a Chinese military commentary on the Department of Defense report, see Teng Fei, '21 shiji Meiguo jundui fazhan de qushi' ('Trends of United States Military Development in the 21st Century'). Online. Available HTTP: <http://www.pladaily.com.cn/item/vote/houqing/content/7-002.htm> (accessed 14 May 2002).

[25] Yang Shisong and Wu Hao, 'Zhuizong wang shang duxiao' ('In Search of the Online Poison Peddlars'), *Jiefangjun bao wang ban jun shi shalong*. Online. Available HTTP: <http://www.pladaily.com.cn/item/vote/hacker/content/008.htm> (accessed 14 May 2002).

[26] Ma Yaxi, 'Gouzhu "wangluo changcheng"' ('Construct an "Internet Great Wall"'). Online. Available HTTP: <http://www.pladaily.com.cn/item/vote/hacker/content/002.htm> (accessed 14 May 2002).

[27] Y. Liu and W. Zhang, 'High-Tech Development and State Security', *Jiefangjun bao*, 11 January 2000, p. 6. English version in BBC Summary of World Broadcasts, FE/3764 G/6, 15 February 2000.

[28] 'General Fu Quanyou calls for accelerating army's modernization' BBC Monitoring, Global Newsline, Asia Pacific Political File, 10 April 2001. Originally from Xinhua News Agency, Beijing, (domestic service, in Chinese), 10 April 2001.

[29] For overviews of changes in Chinese strategic thinking since the 1980s see N. Li, 'The PLA's Evolving Warfighting Doctrine, Strategy and Tactics, 1985-95: A Chinese Perspective', *China Quarterly*, 1996, No. 146, pp. 443-463; P.H.B. Godwin, 'From Continent to Periphery: PLA Doctrine, Strategy and Capabilities Towards 2000', in the same volume, pp. 464-487.

[30] Dai Yifang, 'Amplify the Guidance Role of Military Theories, Ensure the Smooth Implementation of the "Two Basic Changes"', *Guofang*, 1997, vol. 5, pp. 4-5.

[31] Jiang Zemin, 'Gaoju Deng Xiaoping lilun weida qizhi, ba jianshe you Zhongguo tese shehui zhuyi shiye quanmian tuixiang ershiyi shiji' ('Hold High the Great Banner of Deng Xiaoping Theory, Take the Task of Building Socialism With Chinese Characteristics Forwards to the 21st Century'), in *Zhonggong shiwu da baogao budao duben* (*Guide to the CCP 15th Party Congress*), Hong Kong: Mingliu chubanshe, 1997, p. 32.

[32] V. Lai, 'ROC Defense Ministry Sets Up Information Warfare Committee', Asia Intelligence Wire, Central News Agency, 16 August 1999.

[33] *Jiefangjun bao*, March 24, 1998.

[34] Henry and Peartree, 'Military Theory and Information Warfare', p. 122.

[35] 'Air force Publishes First Information Warfare Teaching Aid', BBC Monitoring, Global Newsline, Asia Pacific Political File, 20 April 2001. Original Chinese version in Zhongguo Xinwen She (China News Society), Beijing, 20 April 2001.

[36] 'Japanese Newsletter on Taiwan Information Defense Concerns'. Online. Available HTTP: <http://www.usembassy-china.org.cn/english/sandt/taiinfowar.html> (accessed 14 November 2002).

[37] Qiao Liang and Wang Xianghui, *Chaoxian zhan: dui quanqiuhua shidai zhanzheng yu zhanfa de xiangding*, (*Unlimited War: Doctrine for War and Tactics in the Age of Globalization*), Beijing: Jiefangjun wenyi chubanshe, 1999, pp. 141-158.

[38] Qiao and Wang, *Chaoxian zhan*, p. 44.

[39] Lee Teng-hui first proposed his two states theory on 9 July 1999 in response to questions submitted by Deutsche Welle (Voice of Germany). The figure of 7,200 attacks was given to a meeting of legislators by Zhang Guangyuan, head of the Information Office of the ROC National Security Bureau. *Lianhe bao* (*United Daily News*) (overseas edition), 17 August 1999, p. 3.

[40]*Beijing Qingnian Bao* (*Beijing Youth News*), 'Hulianwang shang de jiaoliang' ('Showdown on the Internet'), 11 May 1995, p. 11.

[41] Qian Fang, 'Fangwei "heike": junshi shang de yi ge jipo renwu' ('Protect Against "Hackers": An Urgent Task in Military Affairs'), *Jiefangjun bao wangluo ban – jun shi shalong* (*PLA Daily Online – Military Affairs Salon*). Online. Available HTTP: <http://www.peopledaily.com.cn/item/vote/hacker/content/txtyindaqianghacker.htm> (accessed 14 May 2002).

[42] Wu Jichuan, 'Gouzhu mianxiang 21 shiji de guojia xinxi anquan tixi' (Construct a National Information Security System to Face the 21st Century'), Preface to Zhang and Ni, *Guojia xinxi anquan baogao*, pp. ii-iv.

[43] Al Gore, 'Remarks Perpared for Delivery to International Telecommunications Union'.

[44] Public Security Bureau, 'Provisions on Secrecy Management of Computer Information Systems on the Internet', promulgated 1 January 2000. English translation available online. Available HTTP: <http://www.usembassy-china.org.cn/english/sandt/netsecret.htm> (accessed 15 October 2001).

[45] *Yangcheng wanbao*, Guangzhou, 20 Feb 2000. Online. Reprinted in SWB FE/3772 G/9, 24 February 2000. Original HTTP not provided.

[46] Jiang Zemin, 'Gaoju Deng Xiaoping lilun weida qizhi', p. 32.

[47] '*Shiwu jihua gangyao quanwen*' (*Complete Text of the Outline of the Tenth Five Year Plan*). Online. Available HTTP: <http://www.chinaemb.or.kr/chn/9272.html> (accessed 10 April 2002).

[48] Liao Rugeng, 'Miandui dianzi houqin, women que shenme?' ('Facing Electronic Logistics, What do We Lack?). Online. Available HTTP: <http://www.pladaily.com.cn/gb/jskj/2001/01/31/20010131002004_jslt.html> (accessed 14 May 2002).

[49] State Council, *White Paper – China's National Defense*', Information Office of the State Council (PRC), 1998. Online. Available HTTP: <http://tigger.uic.edu/~rodrigo/white_paper_98.htm> (accessed 5 April 2002).

[50] 'China Develops Router Technology for High-Speed Internet Use', Xinhua News Agency, Beijing, (domestic service, Chinese), 9 August 2001. English version in BBC Monitoring, Global Newsline, Asia Pacific Economic file, 21 September 2001.

[51] 'China to invest 15 billion yuan in high-tech development', Xinhua News Agency , Beijing, (English), 14 February 2001.

[52] 'China Sets Up Information Security Production Base in Southwest', Xinhua News Agency, Beijing (English), 17 August 2001.

[53] On the 'national team' see D. Sutherland, 'Policies to Build National Champions: China's "National Team" of Enterprise Groups', in P. Nolan (ed.), *China and the Global Business Revolution*, Palgrave, Basingstoke and New York, 2001, pp. 67-140.

[54] Liu and Zhang, 'High-Tech Development and State Security'.

[55] 'China to Boost Efforts Against Internet, Network Related Crimes', Xinhua News Agency, Beijing (domestic service, Chinese), 27 August 2001. English version in BBC Monitoring, Global Newsline, Asia Pacific Political File, 29 August 2001.

[56] 'China to crack down on illegal satellite TV receiving facilities', Xinhua News Agency, Beijing, (domestic service, Chinese), 12 December 2001. English version in BBC Monitoring, Global Newsline, Asia Pacific Political File, 14 December 2001.

[57] G. Walton, *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, 2001. Online. Available HTTP: <http://www.ichrdd.ca/frame.iphtml?langue=0> (accessed 29 October 2001).

[58] Walton, *China's Golden Shield* .

[59] See *Quadrennial Defense Review Report*. See also CSIS Taskforce**,** Global Organized Crime Project, *Cybercrime... Cyberterrorism... Cyberwarfare* ..., p. 66. For an historical overview of the development of the Clinton administration's policies towards ICTs see Ethan Kapstein, *Hegemony Wired: American Politics and the New Economy*, Paris: Institut des relations internationales, 2000.

[60] State Council, 'Hulianwang xinxi fuwu guanli banfa', ('Methods for Managing Internet Information Service'), 25 September 2000. Online. Available HTTP: <http://www.cnnic.net.cn/policy/18.shtml> (accessed 9 December 2001).

[61] Clay Chandler, 'AOL Picks Partner for China Foray', *International Herald Tribune*, 5 June 2001, p. 13.

[62] 'Tune Into China', *Financial Times*, 5 September 2001, p. 16.

[63] D. Gittings and J. Borger, 'Homer and Bart Realise Murdoch's Dream of China Coup', *The Guardian*, 6 September 2001, p. 6.

[64] Ni and Zhang, *Guojia xinxi anquan baogao*, pp. 271-84.

[65] 'China: President urges tighter controls, more political debate on Internet', Xinhua News Agency, Beijing, (domestic service, Chinese), 11 July 2001. English version in BBC Monitoring, Global Newsline, Asia Pacific Political File, 13 July 2001.

[66] B. Schneier, *Secrets and Lies: Digital Security in a Networked World*, New York: John Wiley and Sons Inc., 2000, pp. 21, 67.

[67] G.D. Grove, S.E. Goodman and S.J. Lukasik, S.J. **(**2000**)**, 'Cyber Attacks and International Law', *Survival*, 2000, vol. 42 no. 3, pp. 89-104.

[68] 'Chinese Computer Security Official Interviewed on Recent Hacking', original in Xinhua News Agency, Beijing, (domestic service, Chinese) 3 May 2001. English version in BBC Monitoring, Global Newsline, Asia Pacific Political File. 4 May 2001.

[69] V. Lai, 'ROC Defense Ministry Sets Up Information Warfare Committee'.

[70] Taiwan Democratic Progressive Party, *National Defense Policy White Paper*, (1999). Online. Available HTTP: <http://www.taiwandc.org/dpp-pol2.htm> (accessed 7 April 2002).

[71] Wang Jun, 'Taiwan zhuzhong wangluo zhan' ('Taiwan Pays Attention to Netwar'), *Jiefangjun bao wangluo ban – jun shi shalong*, (*PLA Daily Online – Military Affairs Salon*). Online. Available HTTP: <http://www.pladaily.com.cn/item/vote/hacker/content/010.htm> (accessed 14 May 2002).

[72] Yonhap news agency, Seoul, in English, 6 May 2001

[73] R. Norton-Taylor, 'Spies Seek Access to Phone E-Mail and Net Links', *The Guardian*, 4 December 2000, p.8.

[74] 'Nanfei daohui an, Chen Jiyang tou an', ('South African Financial Scandal, Chen Jiyang Involved), *Lianhe bao* (*United Daily News*), (overseas edition), 11 November 2000, p. 3.

[75] House of Lords, Select Commitee on the European Communities, *European Union Databases*, (23rd Report, Session 1998-99), (London: The Stationery Office, 1999).

[76] House of Lords, Select Committee on the European Communities, *European Union Databases*, (23rd Report, Session 1998-99), (London: The Stationery Office, 1999), p. 12.

[77] APEC, 'APEC Leaders Statement on Counter-Terrorism', 21 October, 2001. Online. Available HTTP: <www.apecsec.org.sg> (accessed 10 April 2002).

[78] UN Security Council, 'Resolution 1373', 28 September 2001. Online. Available HTTP: <http://www.un.org/Docs/scres/2001/res1373e.pdf> (accessed 12 April 2002).

[79] On SafeWeb, see the chapter by Gudrun Wacker in this volume.

[80] 'CPPCC members discuss issue of network security', Xinhua News Agency for Hong Kong, Beijing, 1 March 2001.

[81] Buzan, Barry (1991), *People States and Fear* (Second Edition), New York, London: Harvester Wheatsheaf, p. 43.

[82] The *ti-yong* formula of saving Chinese cultural essence (*ti*) by using Western functional knowledge (*yong*) was formulated by the Confucian reformer Zhang Zhidong (1837-1909). See Joseph Levenson, *Confucian China and Its Modern Fate*, Berkeley and Los Angeles: University of California, 1965, pp. 59-79.

[83] Jiang Zemin, 'Jianshe you Zhongguo tese de shehui zhuyi wenhua' ('Build a Socialist Culture with Chinese Characteristics'), in *Mao Zedong, Deng Xiaoping, Jiang Zemin lun shijie guan rensheng guan jiazhi guan*, (*Mao Zedong, Deng Xiaoping and Jiang Zemin on Concepts of World View, Humanity and Values*), Central Party Documentation Research Dept of CCP (ed.), Hong Kong: Mingliu chubanshe, 1998, p. 380.