Old wine in new bottles: China–Taiwan computer-based 'information warfare' and propaganda

GARY D. RAWNSLEY*

Interest in the theory and application of computer-based information warfare has escalated in Taiwan and China since the middle of the 1990s.[1] Academic communities on both sides of the Taiwan Strait attract generous government funding to analyse the political, social and economic consequences of their societies' growing dependence on computer networks,[2] while substantial investment is directed towards designing and creating new military structures, security architectures, training programmes and technology that facilitate offensive and defensive information warfare.[3]

The scale of this investment in preparing for information warfare suggests that Taiwan and China take very seriously the likelihood that they may be embroiled in such a conflict in the foreseeable future. And there are good reasons why they should acknowledge this possibility:

* The author acknowledges the advice and feedback on this research offered by the following: Dr Ming-Yeh Rawnsley (University of Nottingham, Ningbo, China); Dr Neil Renwick (Nottingham Trent University); staff and students in the Department of Government and Administration, Chinese University of Hong Kong; colleagues and students in the School of Politics and Institute of Asia–Pacific Studies (University of Nottingham); participants in the 2004 conference of the American Association of Chinese Studies; Dr Nicholas Thomas (University of Hong Kong); staff and students at Yonsei University, Seoul; Andrew Scobell (United States Army War College).

1 In this article I use the name 'China' to refer to the People's Republic of China (PRC), and 'Taiwan' to refer to the Republic of China (ROC) on Taiwan. This is merely shorthand, and should not be taken to indicate the author's position on the prevailing conflict over Taiwan's identity.

2 The 'world's first ICT ranking', produced by the International Telecommunications Union in 2003, described Taiwan as 'high access', with a digital access index (DAI, on a scale of 0 to 1, where 1 is the highest access) of 0.79; China was described as having 'medium access', with a DAI of 0.43. See www.itu.int/newsroom/press_releases/2003/, 19 Nov. 2003.

3 See David Finkelstein, 'China's national military strategy', in James C. Mulvenon and Richard Yang, eds, *The People's Liberation Army in the information age* (Santa Monica, CA: RAND, 1999); also Office of the US Secretary of Defense, 'The security situation in the Taiwan Strait', 26 Feb. 1999, at www.defenselink.mil/pubs/twStrait_02261999.html; Major General Wang Pufeng, 'The challenge of information warfare', Spring 1995, http://www.fas.org/irp/world/china/docs/iw_mg_wang.htm; and James Mulvenon, 'The PLA and information warfare', in Mulvenon and Yang, eds, *The People's Liberation Army*, pp. 175–86. For Taiwan, see Democratic Progressive Party Policy Committee, 'White Paper on national defense', 23 Nov. 1999, and the Ministry of National Defense's 2000 Defense White Paper.

- China's commitment to reunify Taiwan with the mainland, by force if necessary. In November 2003 Chinese Premier Wen Jiabao reiterated the longstanding policy of the Beijing government that China would pay 'any price to safeguard the unity of the motherland'.[4] The so-called 'Anti-Secession Law', passed by the Tenth National People's Congress (NPC) in March 2005, reinforces and codifies in Chinese law this enduring commitment.[5]
- The challenge posed to reunification by an ostensibly pro-independence administration in Taiwan under President Chen Shui-bian, which increasingly tests the boundaries of what is and is not acceptable to Beijing's 'One-China Principle'.
- The indisputable possibility, therefore, of war breaking out in the Taiwan Strait.

Military discourse and security studies on both sides of the Taiwan Strait suggest that any future conflict will take advantage of each society's increasing vulnerability to information warfare attack. This scenario is a direct consequence of the growing dependence on computer networks to maintain the operational capacity of social, political and economic infrastructures.[6] It is remarkable that China's government, infamous for the controls it imposes on internet use, is one of the most visible and transparent on the web, and that the government aims that by 2010 all central ministries, provinces, municipalities, autonomous regions and embassies in foreign countries will be connected to the internet.[7]

The information and computer sectors in Taiwan are far more advanced than their counterparts on the Chinese mainland, and Taiwan is one of the world's largest producers of computer components. Meanwhile, Beijing's 'Government On-Line Initiative', launched in 1998, aimed to ensure that 80 per cent of all government agencies at all levels of political life in China had websites.[8] Suspicion of China's capacity to launch a computer-based information attack against Taiwan has passed through several stages of intensity. The first date given by the Ministry of National Defense for a possible Chinese attack was 2010; that estimate was subsequently revised to 2005; and in 2000, General

[4] Quoted in David Lague, 'Chen launches his missile vote', *Far Eastern Economic Review*, 29 Jan. 2004, pp. 24–7 at p. 26.

[5] The Anti-Secession Law 'provides that in the event that the "Taiwan independence" forces should act under any name or by any means to cause the fact of Taiwan's secession from China, or that major incidents entailing Taiwan's secession from China should occur, or that possibilities for a peaceful reunification should be completely exhausted, the state shall employ non-peaceful means and other necessary measures to protect China's sovereignty and territorial integrity'. Wang Zhaoguo, vice-chairman of the Standing Committee of the NPC, 8 March 2005, at http:English.peopledaily.com.cn/200503/08.

[6] On the vulnerability of such networks, see L. Scott Johnson, 'Toward a functional model of information warfare', *Studies in Intelligence* 1: 1, 1997. Lawrence Freedman has noted that 'In strategic thinking, dependence soon becomes a vulnerability and, by extension, a potential target.' See his *The revolution in strategic affairs*, Adelphi Paper 318 (Oxford: Oxford University Press, 1998), p. 52.

[7] R. J. Perrins, *China Facts and Figures Annual Handbook, 2001* (Gulf Breeze, FL: Academic International Press, 2001), p. 311.

[8] Nina Hachigian, 'China's cyber-strategy', *Foreign Affairs* 80: 2, March–April 2001, pp. 118–33. The number of Chinese websites increased by 60% in 2003 to 595,550: China Internet Network Information Centre, quoted in *South China Morning Post*, 16 Jan. 2004, p. A7.

Lin Chi-cheng of the Communications, Electronics and Information Bureau described how China's mobilization of information warfare was far surpassing Taiwan's.[9]

The vulnerability of Taiwan's information networks and social infrastructure have been tested by Taiwanese society's response to a series of crises that have disrupted the island over the past decade: Chinese missile tests in 1995 and 1996; the island-wide blackout of 29 July 1999; the earthquake of 21 September 1999; and the Pachang Creek tragedy of July 2000. Together with the increasingly belligerent attitude of the government in Beijing (encouraged by former Taiwan president Lee Teng-hui's announcement in 1999 that Taiwan and China should embark on special state-to-state relations, the election of Chen Shui-bian as president in 2000, his high-profile visit to the US in 2003, and the referendum movement in 2003–4 that seemed in Beijing to augur progress towards a popular referendum on Taiwan's independence), these episodes established the fragility of Taiwan's political, economic and social infrastructures (including such tangible elements as transport networks, power reserves and rescue/health-care systems).[10] They also demonstrated the urgent need for a consolidated command, control, communications and intelligence (C^3I) system that can launch a rapid response to crisis and structure relief and rescue efforts.

However, none of the above crises has given grounds for anxiety that Taiwan's military and social infrastructures are at significant risk from a computer-based information offensive launched in Beijing. Rather, newspapers, academic articles and military reports circulating in Taipei and Beijing testify that computer-based information warfare is so far limited to the relatively innocuous 'hacking' of internet sites. Since there has not been, and cannot be, a serious attempt to associate these violations of computer networks to military scenarios, we can conclude that the *perceived* threat from computer-based information warfare is disproportionate to the levels of attention and investment actually devoted to it on both sides of the Taiwan Strait. The case is rather that analyses of information warfare are unable to transcend the Cold War mindset of propaganda and psychological warfare that has characterized relations between Taiwan and China since the triumph of Chinese communist forces in 1949.

This article uses the approaches developed by students of 'critical security' to discuss the relationship between propaganda and information warfare in the Chinese context. This method is both intriguing and appropriate, because the characteristics of information warfare compel us to seek explanations other than those offered by traditional international relations theories. These characteristics

[9] 'Menace of tech warfare looms: Defence Ministry', *Taipei Times*, 24 July 2002; 'Military to test computer bugs', AFP, 8 Aug. 2000; 'Defense minister calls for budget increase', *China Times*, 2 Nov. 1999.

[10] In the United States, critical infrastructures were defined in Presidential Decision Directive 63 (PDD-63) of May 1998 as comprising 'information and communications; banking and finance; water supply; aviation, highways, mass transit pipeline, rail and water-borne commerce; emergency, fire, and continuity of government services; public health services; electric power, oil and gas production and storage'. See Steven A. Hildreth, 'Cyberwarfare', in John V. Blane, ed., *Cyberwarfare: terror at a click* (Huntington, NY: Novinka, 2001), p. 9.

may be summarized as an attempt to broaden beyond the state the range of actors involved in international politics (information warfare provides for the kind of 'extended security' that is so central in the work of Alan Dupont, and refers to 'non-state actors that challenge the state's traditional monopoly over taxation and organised violence'[11]); the realization of a taxonomy of threats other than (but including) national security; and the decreasing relevance of spatial and temporal limitations in determining actor behaviour. Information warfare is one of the 'realities' identified by James J. Hentz that threaten the 'conceptual edifice' of traditional security studies, but are ignored 'in favour of enduring assumptions that guarantee its primacy'.[12]

The critical security approach

We are advised that information warfare shatters the boundaries between military and societal autonomy, as well as between peace and war, thus allowing for unimaginable social disruption. Paul Dibb, for example, has theorized that interstate conflict will be transformed by the capacity to attack and disable an adversary's transport, energy supply and communications networks using computer technology.[13] L. Scott Johnson has described how a 'unified information warfare campaign can be conducted alongside multiple concurrent or consecutive combat operations, can extend beyond the immediate battlefield [and] can cross the boundaries between peacetime, crisis, and combat'.[14] We may begin to understand the relevance and implications of information warfare through approaches associated with studies of 'critical security' that challenge the privileged position of the state.[15] Ole Waever, for example, describes how critical security understands the importance of 'the ability of a society to persist in its essential character under changing conditions and possible or actual threats'.[16] By its nature, method and target, computer-based information warfare claims the capacity to pose a considerable threat to the persistence of a society's 'essential character'. If we use this approach, the threats to Taiwan are clear: computer-based information warfare that deliberately targets an enemy's political, economic, social and military infrastructures creates the possibility of a national crisis, in which Taiwan may then (though not necessarily) be exposed to attack from more conventional sources (the tactical application of information

[11] Alan Dupont, *East Asia imperilled: transnational challenges to security* (Cambridge: Cambridge University Press, 2001), p. 8.
[12] James J. Hentz, 'Introduction: new regionalism and the "theory of security studies"', in James J. Hentz and Morten Bøås, eds, *New and critical security and regionalism: beyond the nation state* (London: Ashgate, 2003), p. 4.
[13] Paul Dibb, 'The revolution in military affairs and Asian security', *Survival* 39: 4, 1997–8).
[14] Johnson, 'Toward a functional model of information warfare'.
[15] David Held and Anthony McGrew, 'Globalization and the liberal democratic state', in Yoshikazu Sakamoto, ed., *Global transformation: challenges to the state system* (Tokyo: United Nations University Press, 1994).
[16] Ole Waever, Barry Buzan, Morten Kelstrup and Pierre Lemaitre, *Identity, migration and the new security agenda in Europe* (New York: St Martin's Press, 1993), p. 23.

warfare).[17] Taiwan's policy communities have felt sufficiently vulnerable to organize an effective and coordinated military, political and social response to the possible threats to its infrastructure by external (Chinese) forces.

The prospect of information warfare thus draws attention to the fact that national security is no longer synonymous with *state* security. Critical security thought introduces instead the idea that analysts are now faced with a new catalogue of threats and with actors who can be both victims and aggressors. The global flow of information is one of many resources and non-military security issues affecting domestic and international politics with little regard for political or geographical boundaries and increasingly outside the prerogatives of state power.[18] Information warfare, and other problems addressed by critical security, therefore challenge traditional approaches to politics that are based on the notions of formal state autonomy and sovereignty.

This is not to argue that realist considerations have no value in assessing and understanding security. After all, much of East Asia's security architecture is designed around the essentially realist principles of balances of power and the maximization of state interests. As the political history of the region tragically demonstrates, strategic competition between states over territory and resources continues to provide the core motivation for military conflict.[19] Moreover, any examination of information warfare is incomplete without reference to the state, for it is the state that controls the military, directs its revolutions in military affairs, and manages the investment priorities of the military and defence-related industries.

Rather, critical security contests the realist model of security hierarchies, according to which military survival and national security are the primary interests in international politics, and the only relevant actor is the (unitary) state. The conflict in the Taiwan Strait establishes that we cannot understand insecurity in the international system as the simple absence of authority and the prevalence of anarchy. Instead, critical security requires us to acknowledge that the perception of security is socially constructed, and in particular is inseparable from the creation of identity, both of the self and of the 'other'.[20]

[17] Richard A. Bitzinger and Bates Gill outline four conventional scenarios in any conflict with Taiwan, from 'low-level intimidation' to invasion: *Gearing up for high-tech warfare? Chinese and Taiwanese defense modernization and implications for military conflict across the Taiwan Strait, 1995–2005* (Washington DC: Center for Strategic and Budgetary Assessments, Feb. 1996). On the tactical application of information warfare, see Freedman, *The revolution in strategic affairs*, p. 50.

[18] Jessica T. Matthews, 'Power shift', *Foreign Affairs* 76: 1, 1997; Robert O. Keohane and Joseph S. Nye, Jr, *Power and interdependence* (Glenview, IL: Scott, Foresman & Co., 1989); Robert O. Keohane and Joseph S. Nye, Jr, 'Globalization: what's new? What's not? (And so what?)', *Foreign Policy*, no. 118, Spring 2000.

[19] See Amitav Acharya, *A new regional order in South-East Asia: ASEAN in the post-Cold War era*, Adelphi Paper 279 (London: IISS, Aug. 1993).

[20] Alexander Wendt, *Social theory of international politics* (Cambridge: Cambridge University Press, 1999); Alastair Ian Johnston, 'Thinking about strategic culture', *International Security* 19: 4, 1995; Muthiah Alagappa, *Asian security practice: material and ideational influences* (Palo Alto, CA: Stanford University Press, 1998), p. 649.

Propaganda and psychological warfare

The approach outlined above provides the foundation for a more informed understanding of propaganda and the way in which it relates to security: 'Ideas and myths can kill,' wrote Prunier in 1995, 'and their manipulation by elite leaders for their own material benefits does not change the fact that in order to operate they first have to be implanted in the souls of men.'[21] Most propaganda turns on creating a dichotomy between the self and the 'other', and leans on history (or at least interpretations of history) to strengthen the claims that 'the other' is in some way inferior and/or threatening to self-identity.

For example, close examination of propaganda and media content in China reveals a political discourse rooted in the theme of historical 'victimhood'. This offers a focus of identity to which the Chinese can attach themselves:

> The territorial dismemberment of the country, the humiliation of a proud state by an avalanche of 'unequal treaties' and the dislocating tensions added to existing internal forces of disorder represent a powerful *leitmotif* of subordination, resentment and anger in nineteenth- and twentieth-century Chinese social commentary and political discourse.[22]

Victimhood remains a useful discourse of nationalist and patriotic mobilization in China, as the anti-Japan demonstrations of April 2005 demonstrate, bringing to the surface questions of identity and suffering at the hands of 'the other'.

Until 2000 Taiwan continued to maintain that it was 'Free China', in stark and simple contrast with the mainland. Throughout the Cold War, Taiwan opted to package its propaganda in the familiar rhetoric of the period. Taiwan's description of the PRC was decidedly negative. *A decade of Chinese communist tyranny*, published by the Asian People's Anti-Communist League in the 1960s, set the tone. It opens with a comparison between the 'communist controlled area' and a zoo, 'with people there being placed under ruthless exploitation by the aggressor and traitor alike'. It describes the 'gangsters' (a theme overworked in reference to the Chinese communists, suggesting both the illegality of their power and the brutality of their methods) as 'inhuman and devoid of all moral scruples'—all of this in the first two paragraphs of a closely printed book of 483 pages![23] Cold War propaganda encouraged the use of such stereotypes and the substitution of names that reinforce the stereotype—'reds' instead of 'communists', for example. The 1957/8 edition of the *China Yearbook* even went so far as to refer to the communists as 'the sons of Satan'.[24]

The exchange of such propaganda across the Taiwan Strait has served a symbolic and long-term (strategic), rather than short-term (tactical), purpose, and has acted as a dependable alternative to the outbreak of military conflict. This is

[21] G. Prunier, *The Rwanda crisis, 1959–1994: history of genocide* (London: Hurst, 1995), p. 40.
[22] Neil Renwick and Qing Cao, 'Modern political communication in China', in Gary D. Rawnsley and Ming-Yeh T. Rawnsley, eds, *Political communications in greater China: the construction and reflection of identity* (London: RoutledgeCurzon, 2003), p. 63.
[23] Asian People's Anti-Communist League, *A decade of Chinese communist tyranny* (Taipei: 1960).
[24] *China Yearbook, 1957–1958* (Taipei: Government Information Office, 1958), p. i.

most clearly demonstrated by the eruption of limited military activity in 1954 and 1958 against Matsu and Kinmen (Quemoy), islands that belonged to the Republic of China on Taiwan and were the front line in the propaganda war between Taiwan and China until 1979. Chinese shelling of these islands, and Taiwan's own bombardment of the mainland in response, was designed to have more symbolic than military value, and was pivotal in the psychological and propaganda offensive across the Taiwan Strait. Beijing decided to shell the islands only on odd-numbered days, and Taiwan's military launched its own shells against the mainland the rest of the week. A practice that continued until 1979, this combat by timetable confirmed the political and symbolic, rather than military, intention of cross-Strait warfare,[25] especially as the shells contained nothing more harmful than printed propaganda that dispersed upon impact.[26]

The continuing propaganda offensive across the Taiwan Strait is a form of information warfare that has enjoyed little success beyond the recurrent exchange of political symbolism and rhetoric. Nevertheless, it is essential that we do not underestimate its potential; a strategy of propaganda and psychological warfare that is carefully designed and integrated into the decision-making process is indispensable to the effective prosecution of a military campaign.[27] The problem with propaganda and psychological warfare, however, has been their lack of precision; they tend to pursue a *mass* audience through media of *mass* communication. Therefore, traditional approaches to propaganda and psychological warfare have demonstrated a tendency to grope for success in the dark. We lack a clear and empirically grounded theory of propaganda—a deficiency which, together with the notable absence of scientifically reliable methods of measuring its impact, seriously limits its application and value. While propaganda and psychological warfare strategies accomplished through the mass media are efficient and potentially lucrative mass communicators of the symbolism and emotion associated with the Cold War, they are largely untested as methods of measured strategic disruption, or as systems for the precise targeting of information.

Advocates of using computer networks as part of a new approach to information warfare claim that they are able to circumvent the problems associated with traditional propaganda and psychological warfare. Computer technology allows for precise targeting, measurement of effect, and the possibility of causing social disruption on an extraordinary scale, while meeting the non-violent aspirations of propaganda (it is preferable to persuade one's enemy to

[25] See letter from Secretary of State Dulles to Foreign Secretary Lloyd, 24 Oct. 1958, in *Foreign relations of the United States, 1958–1960*, vol. 19: *China* (Washington DC: Department of State, 1996), p. 451.

[26] Secretary of State John Foster Dulles in conversation, 12 Sept. 1958, quoted in *Foreign relations of the United States, 1958–1960*, vol. 19: *China*, pp. 168–71. For further details of Kinmen and Matsu as the outposts of the propaganda war, see G. D. Rawnsley, 'Taiwan's propaganda cold war', *Intelligence and National Security* 14: 4, 2000, reprinted in R. J. Aldrich, G. D. Rawnsley and M. Y. T. Rawnsley, eds, *The clandestine Cold War in Asia* (London: Frank Cass, 2000).

[27] See Philip M. Taylor, *Munitions of the mind* (Manchester: Manchester University Press, 1996); Gary Rawnsley, *Radio diplomacy and propaganda: the BBC and VoA in international politics, 1956–64* (Basingstoke: Macmillan, 1996).

capitulate via propaganda than through a violent military campaign). Through internet chat rooms, discussion groups and the prevalence of email, it is now possible to deliver customized news to the desktops of subscribers anywhere in the world. In other words, networked computers allow psychological operations to target specific members of the desired audience—even individuals—thereby yielding better results than mass-based propaganda and psychological warfare. Moreover, computer technology allows for 'semantic attacks', whereby an external actor is able to control a system that appears to insiders and audiences to be working properly (involving the distortion of television images, misleading signals, and the simple spread of black propaganda).[28] Richard Szafranski has developed this idea and created the concept of 'neocortical warfare', which refers to the ability to 'control or shape the behaviour of enemy organisms, but without destroying the organisms'.[29] Lawrence Freedman has observed that in neocortical warfare the 'focus would be on enemy minds rather than capabilities'.[30] In other words, computers can be an extremely valuable addition to the arsenal of propaganda and psychological warfare techniques.

The reason that computer networks are so useful in propaganda is because of the process known as 'connectivity'. Connectivity refers to the process whereby separate and previously autonomous units are integrated into a highly structured network that is connected by computer systems.[31] This structure represents a new form of horizontal organization that is less dependent on functional hierarchies and centralized decision-making than previous forms; hence, what is known as 'strategic information warfare' is designed to infect the network, disrupting society's ability to remain connected and thus function efficiently.[32] The main targets within this network are non-military—that is, attacks are directed at societal connectivity—because this presents an opportunity for the hostile state to paralyse another nation-state system. The ultimate target of information warfare is the adversary's decision-making process, and especially systems that are concerned with the way information is used, rather than generated and distributed; information warfare may go further than simply disrupting or deleting vital information flows, retaining the capacity also to shape perceptions, decisions, opinions and behaviour. Attacks aim to confuse, delay, manipulate or paralyse the enemy, and the disabling of information flows means that the quality of decision-making will be 'sub-optimal'.[33] In this sense, propaganda and psychological warfare are types of information warfare; computers, however, enable more precise targeting and greater anonymity.

[28] Freedman, *The revolution in strategic affairs*, p. 56. 'White' propaganda is open about intention and source. 'Black' propaganda aims to deceive, usually concealing or lying about the source.
[29] Richard Szafranski, 'Neocortical warfare? The acme of skill', *Military Review* 74: 11, Nov. 1994, pp. 41–55.
[30] Freedman, *The revolution in strategic affairs*, p. 56.
[31] John Arquilla and David Ronfeldt, eds, *In Athena's camp: preparing for conflict in the information age* (Santa Monica, CA: RAND, 1997); Richard J. Harknett, 'Information warfare and deterrence', *Parameters: US Army War College Quarterly*, Autumn 1996, pp. 93–107.
[32] Roger C. Molander, Andrew S. Riddle and Peter A. Wilson, *Strategic information warfare: a new face of war* (Santa Monica, CA: RAND, 1996).
[33] Ajay Singh, 'Information warfare: reshaping traditional perceptions', at www.idsa-india.org/an-mar-4.html.

China's information warfare capacity: rhetoric or reality?

The policy community in Beijing has analysed the implications of computer-based information warfare since the 1991 war against Iraq, which demonstrated China's inferiority to American military technology, raising the fear of asymmetric warfare in any future conflict with the US. The lessons of that conflict led the People's Liberation Army (PLA) to the following conclusions:

> (a) modern war is high-tech war, and technology can not only fulfil tactical and combat missions but can also fulfil strategic objectives; (b) regional warfare can serve as a viable means for political resolution and render large-scale warfare unnecessary; (c) the existence of high-tech weapon systems holds out the possibility of 'quick resolution' by conducting long-distance, high power, and precision attacks; and (d) high-tech weapon systems have changed the needs of force composition and resulted in new types of combined operation.[34]

From the Chinese literature on the 1991 Gulf war, we can see that the PLA believed information warfare played a crucial role in the coalition's victory, even affirming that the American military deployed computer viruses to disrupt Iraq's information systems.[35] The PLA's leading information warfare expert and former Director of the Strategy Department at the Academy of Military Science in Beijing, Wang Pufeng, called the 1991 Gulf war the 'epitome' of information warfare, and thus exhorted the PLA to devote serious attention to understanding its lessons.[36]

A new strategy of 'local war under high technology conditions' (*gao jishu tiaojian xia jubu zhanzheng*) was expressed in an important article by Wang published in 1995. 'In the near future,' he wrote, 'information warfare will control the form and future of war. We recognize this developmental trend of information warfare and see it as a driving force in the modernization of China's

[34] Andrew N. D. Yang and Col. Milton Wen-Chung Liao (ret.), 'PLA rapid reaction forces: concept, training, and preliminary assessment', in Mulvenon and Yang, eds, *The People's Liberation Army*, p. 49. There is evidence in the available Chinese literature that the authors have borrowed heavily from the US discourse on information warfare. See James Mulvenon, 'The PLA and the information age', in Mulvenon and Yang, eds, *The People's Liberation Army*, p. 178.

[35] 'Army paper on information warfare', *Jiefangjun bao*, 25 June 1996, p. 6; Liu Huaqing, 'Unswervingly march along the road of building a modern army with Chinese characteristics', *Jiefangjun bao*, 6 Aug. 1993, both in *Foreign Broadcast Information Service—China* (*FBIS*), 20 Nov. 1996.

[36] *Information warfare and military revolution* (*Xinxi zhanzheng yu junshi geming*) (Beijing: Military Sciences Publishing House, Dec. 1995), p. 144. 'Major General Wang Pufeng is nominally the author of . . . [what] appears to be the first full-length book on IW published in China . . . Attaching his name to the book at least indicates that the subject is taken very seriously by the PLA High Command': Harlan W. Jencks, 'Wild speculations on the military balance in the Taiwan Strait', in James R. Lilley and Chuck Downs, eds, *Crisis in the Taiwan Strait* (Washington DC: National Defense University, 1997), p. 161, n.12. It is clear, however, that the coalition forces won victory over Iraq by using a carefully designed combination of information warfare and conventional methods of military attack. See Edward Waltz, *Information warfare: principles and operations* (Norwood, MA: Artech House, 1998), pp. 7–8. For more on Chinese approaches to information warfare see Chen Huan, 'The third military revolution', in Michael Pillsbury, ed., *Chinese views of future warfare* (Washington DC: National Defense University, 1997), and You Ji, 'The revolution in military affairs and the evolution of China's strategic thinking', *Contemporary Southeast Asia*, no. 21, Dec. 1999.

military and combat readiness. This trend will be highly critical to achieving victory in future wars.'[37] There is evidence that the PLA has situated information warfare at the forefront of its own revolution in military affairs (RMA): the US Department of Defense has claimed China is developing strategies to create computer viruses and penetrate the information systems of potential antagonists.[38] China has allegedly established an information warfare simulation centre, and has organized exercises involving virus attacks (in 1997), computer confrontation (1999) and the internet (2000).[39] Chinese military strategy now acknowledges the importance of knowing how to create and plant computer viruses, hack into the systems of other countries, and conduct computer-based psychological warfare.[40] This is assimilated into a new interpretation of 'people's war' that recognizes how thousands of Chinese armed with networked computers could launch a serious and concerted attack against any enemy.[41] At the end of 2000 there were 22 million internet users in China;[42] this increased to 79.5 million in 2003—an increase of more than one-third on 2002—and computers with installed internet access jumped by 10.1 million to 30.9 million.[43] Projections for 2005 estimate 130 million users in a new version of Mao's 'people's war'.[44] However, we should not assume from this that China boasts 130 million potential cyberwarriors. First, it is a leap from being a net user to being part of the operationalization of RMA technology in combat scenarios. Second, this imagined situation raises the issue of government control of the internet, and whether that control can be relaxed to allow a 'people's information war' to be conducted. Could the Chinese be trusted with the capabilities they are offered? How would the government guarantee that such freedoms would not be used against it by domestic hackers and dissidents?[45]

A report by Michael Sheridan in the *Sunday Times* (1 September 2002) nourished fear of Chinese computer-based information warfare. Sheridan alluded to 'a systematic campaign by the Chinese government to take on America and other powers on the 21st century battlefield of cyber warfare'. He referred to a 'secretive department controlled by the Ministry of Information Industry' and a

[37] This strategy involved more active, but low-level intimidation of Taiwan. See Bates Gill, 'Chinese military hardware and technology acquisitions of concern to Taiwan', in Lilley and Downs, eds, *Crisis in the Taiwan Strait*, pp. 105–28; Major-General Wang Pufeng, 'The challenge of information warfare', Spring 1995, at http://www.fas.org/irp/world/china/docs/iw_mg_wang.htm.

[38] Office of the US Secretary of Defense, 'The security situation in the Taiwan Strait'.

[39] Tim Thomas, 'China's technology stratagems', *Jane's Intelligence Review*, Dec. 2000.

[40] Wang Houqing and Zhang Xingye, eds, *Beijing science of campaigns* (Beijing: National Defense University Publishing House, 2000).

[41] Thomas, 'China's technology stratagems'; Ehsan Ahrari, 'China changes its strategic mindset—part two', *Jane's Intelligence Review*, Dec. 1999; Wang Pufeng, 'The challenge of information warfare'.

[42] Timothy Thomas, 'The internet in China: civilian and military uses', *Information and Security* 7, 2001, pp. 159–73.

[43] Information from the China Internet Network Information Centre, quoted by *South China Morning Post*, 16 Jan. 2004, p. A7.

[44] Thomas, 'The internet in China'. The concept of 'people's war' via the internet is most fully explored in Shen Weiguang, *The Third World War: total information war* (Beijing: Xinhua Publishing, 2000).

[45] See Michael Chase and James Mulvenon, *You've got dissent! Chinese dissident use of the internet and Beijing's counter-strategies* (Santa Monica, CA: Rand, 2002); also 'Guerrilla warfare, waged with code on the internet', *New York Times*, 13 Oct. 2002.

government-led initiative to 'break internet encryptions and codes used by foreign firms and governments'. Sheridan's source, allegedly an employee of this secret department, tapped into the paranoia that saturates the discourse about information warfare (especially when the world is mobilized in a 'war against terror'): '"If you knew how much we could learn from your computer you would never use the internet in China … We can break almost any password and get into your bank account. We can read your e-mails and send e-mails from your computer to your boss—in Chinese and in English."'[46] Similarly, after the websites of Taiwan's National Security Bureau (NSB) and Vice-President Lien Chan were attacked in March 2000, the director of the NSB Information Department said: 'Although they were not from China and there has been no indication of any hacker attempts from China, *it does not mean China will not do it*.'[47]

As with most 'evidence' about the development of information warfare, such stories, while they may be true, nevertheless feed upon the growing paranoia that societies are vulnerable to collapse induced by the deliberate placing of worms, viruses and 'logic bombs' into computer networks.[48] The danger is that the 'connectivity' that characterizes societies in the information age may be targeted by viruses that contaminate and spread through networks, causing maximum disruption to capacity to function.

In information warfare across the Taiwan Strait, the primary target of Chinese attack must be the US military. The key to PLA success would be subduing Taiwan as quickly as possible, thereby achieving the desired outcome before US forces arrived, or preventing US involvement prior to the outbreak of hostilities. In this scenario, information warfare could help the Chinese launch pre-emptive strikes against US targets to delay or disrupt American deployment in Taiwan's defence:

> For the PLA, using IW against US forces to Taiwan offers an attractive asymmetric strategy. American forces are highly information-dependent … If PLA information operators … were able to hack or crash these systems, thereby delaying the arrival of a US carrier battle group to the theater, while simultaneously carrying out a coordinated campaign of short-range ballistic missile attacks, 'fifth column', and IW attacks against Taiwanese critical infrastructure, then Taipei must be quickly brought to its knees and forced to capitulate to Beijing.[49]

However, Pentagon assessments have downplayed the evidence of China's capacity to wage computer-based information warfare:

[46] Michael Sheridan, 'China's net warriors take on West', *Sunday Times*, 1 Sept. 2002, p. 24.
[47] 'NSB websites attacked', *Taipei Times*, 7 March 2000 (emphasis added).
[48] Viruses can be considered 'Trojan horses', hidden within a host programme and triggered upon execution; worms 'obliterate or alter data as they bore through system memory'; and 'logic bombs' 'embed themselves in an executable file until activated by a specific event, such as a date': Freedman, *The revolution in strategic affairs*, p. 55.
[49] Mulvenon, 'The PLA and information warfare', pp. 183–5.

Although the PRC has achieved certain results in information warfare tactics, their basic capability and technology in information science and technology is still at the elementary research and development stage. The major reason is that its domestic information industry is still mainly in re-processing manufacture and there is no real research and development capability to be mentioned.[50]

The American military therefore disputes the possibility that the PLA could overwhelm either the US or its allies by using computer-based information warfare. In addition to clear deficiencies in military morale, the PLA is also behind in terms of training, logistics and technology. The threat, therefore, is 'more hype than reality'.[51]

Information warfare: looking in the wrong direction?

The mistake that many militaries have made in adjusting to the information age is in preparing for attack from and against networked computers, and thus ignoring the possibilities for the physical destruction of societies through the application of conventional military technologies. As far back as 1990, the US National Academy of Sciences prepared a report on computer security that began: 'We are at risk. Increasingly, America depends on computers … Tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb.'[52] Yet it was not computers that hijacked four aeroplanes on 11 September 2001 and navigated them towards the World Trade Center and the Pentagon. Nor are computers responsible for the terrorist destruction in Bali, Kenya, Saudi Arabia, Turkey, Israel, Spain or Iraq. The gravest threat remains the religious fanatic or terrorist who, believing in a higher cause, walks into a crowded marketplace or boards a bus and triggers a bomb that kills him- or herself along with hundreds of others.

This reservation was succinctly captured by Professor Lawrence Freedman in a 1996 article in which he warned against devoting too much attention to cyberterrorism: 'an enemy', he wrote, 'might well be unsure about relying on clever and subtle forms of electronic warfare to disable a critical facility' because of the increasing number of firewall protection mechanisms, 'especially when something cruder, simpler and probably more violent will do. Why become a

[50] Office of the US Secretary of Defense, 'The security situation in the Taiwan Strait'.

[51] Argument advanced by Bates Gill and Michael O'Hanlon, 'China's hollow military', *National Interest* 56, Summer 1999; Michael O'Hanlon, 'Why China cannot conquer Taiwan', *International Security* 25: 2, 2000. 'Does the possible enemy have the capability to wage a large-scale cyber attack against the US? It is far from clear even in the intelligence community if strategic rivals like China or Russia already have the technology and, even more important, the knowledge and qualified personnel to hack into computers that control critical infrastructures. Traditional means of intelligence do not help very much in this field, because the capabilities for an attack largely consist of software, commercial off-the-shelf hardware components, and an Internet connection.' See Ralph Bendrath, 'The cyberwar debate: perception and politics in US critical infrastructure protection', *Information and Security* 7, 2001, pp. 80–103.

[52] National Academy of Sciences, Computer Science and Telecommunications Board, *Computers at risk: safe computing in the information age* (Washington DC: NAS, 1990). See also *Protecting the homeland: report of the Defense Science Board Task Force on Defensive Information Operations* (Washington DC: Office of the Undersecretary of Defense for Acquisition, Technology and Logistics, March 2001).

hacker when it is as easy to be a bomber?'[53] The key to understanding this argument lies in Freedman's repudiation of virtual war: 'Territory, prosperity, identity, order, values—they all still matter and provide the ultimate test for a war's success. War is not a virtual thing, played out on screens, but intensely physical. That is why it tends to violence and destruction. Information technologies may help limit this tendency but they can never eliminate it.'[54]

But hacking remains the only way that the Chinese on both sides of the Taiwan Strait are able to operationalize their information warfare capacity. On 8 August 1999, an unidentified hacker from Hunan province in China accessed the websites of Taiwan's Control Yuan, the cabinet-level Construction and Planning Administration, and Pingtung County government. He infected these websites with a message in English and Chinese for his compatriots: 'Taiwan is an indivisible part of Chinese territory and always will be!' This sparked what the media in Taiwan referred to as a 'cyber alert', and prompted the immediate creation of a security department within the Institute for Information Industry to help government agencies protect themselves from further attack. Only two days later, Taiwanese attacked China's Railways Ministry in revenge and planted the following message: 'Only one Taiwan exists and only one Taiwan is needed.' The Shaanxi Science and Technology Information Network was infected with the call to 'Reconquer, Reconquer, Reconquer the mainland!' Beijing later admitted that 19 government sites had been attacked by pro-Taiwan hackers who planted programmes that made the websites play the Taiwan anthem, display Taiwan's flag and shout pro-Taiwan slogans at the viewer. After a Chinese F-8 fighter jet collided with an EP-3 American spy plane over Hainan on 1 April 2001, Chinese hackers claimed to have defaced over 1,000 American websites.[55]

In August 1999, hackers thought to be living in China were allegedly responsible for 70,000 separate attacks on Taiwan's computer networks.[56] Targets included government agencies such as the Investigation Bureau, the ministries of Economic Affairs and Justice, and the National Assembly. The gravity of the perceived threat to Taiwan is indicated by the creation in 2003 of a new unit within the Ministry of National Defense to protect the security of military and civilian computer networks.

However, Taiwan is at the forefront of development of offensive information warfare strategies, as is suggested by its growing reputation as a nursery for the development of new computer viruses. In 1990 Taiwanese hackers were responsible for the 'Bloody' or '6/4' virus to protest against the 1989 crackdown against student protests in Beijing's Tiananmen Square; the 'Michelangelo'

[53] Lawrence Freedman, 'Operation overload in the shadow of the Somme', *Times Higher Education Supplement*, 8 Nov. 1996 (section on Multimedia, pp. iv–v).
[54] Freedman, 'Operation overload'.
[55] Israelis and Palestinians attacked each other's websites following the breakdown of negotiations in October 2000; Pakistani hackers defaced 600 Indian websites following an escalation in the conflict over Kashmir, March 2000. I am grateful to Athina Karatzogianni, PhD candidate in the School of Politics, University of Nottingham, for drawing these incidents to my attention.
[56] *United Daily News* (Taipei), 3 Nov. 1999.

virus was discovered in a Taiwan firm in 1992; in 1997 the 'Con-Air' virus, protesting against social problems in Taiwan, was developed by opponents of the KMT government; and in 1998 and 1999 Taiwanese were responsible for the CIH or Chernobyl virus, which can destroy floppy drives and hard disks of machines running Windows 95 and 98. CIH reportedly affected 360,000 Chinese computers (by 26 April 1999) causing an estimated 1 billion Renminbi (Chinese currency) in damages. The extensive development of new penetrative and destructive viruses led Major-General Chen Wen-chien, deputy director of the Ministry of National Defense's communication electronics and information bureau, to be optimistic about Taiwan's chances: 'Should the People's Liberation Army launch an information war against Taiwan,' he said, 'the military, armed with 1000 computer viruses, would be able to fight back.'[57]

The important thing to note from these reports is that hackers in both China and Taiwan attacked *websites*, not the mainframe networks that are responsible for the operational capacity of the nation's political or economic infrastructure. There is evidence to suggest that even if a military wished to do this, it would be impossible to put into effect: speaking after the outbreak of cyber-hostilities in 1999, Carl Nicolai, director of Transend (an independent Taipei service provider), admitted that 'the Taiwan military is completely shut-off from the Internet'.[58] Besides, information systems are not particularly easy targets; computer-dependent networks are now more than ever aware of the threat from viruses and hackers, and thus recognize the need to install security mechanisms and routines (reducing dependence on single systems, backing up data, installing up-to-date virus detection systems, firewalls, etc.). Social disruptions that have occurred as a result of computer failure—for example, in the Stockholm underground system in 2000, in the power failure in Auckland, New Zealand, in 1998, and in the blackouts in New York and London in 2003—were local in origin and concentration. They were (relatively) easily contained within specific geographically delineated systems, and further such disruption can be minimized with the appropriate back-up mechanisms. There is no reason to suggest that such concentrated failures constitute a widespread threat to society.

Information warfare, propaganda and knowledge

It is worth considering the controlled way in which the Communist Party allows anti-foreign nationalism to erupt, as we saw in the case of the popular demonstrations outside the US embassy in Beijing when the Americans were accused of deliberately targeting the Chinese embassy in Belgrade, and again in the anti-Japan demonstrations of April 2005. Considering that the Chinese government has such a tight grip on internet use in the country, it is interesting that hackers were allowed (a) to access these sites in the first place, and (b) to transfer

[57] Quoted in 'Taiwan has 1000 computer viruses to fight cyber war with China', AFP, 9 Jan. 2000.
[58] 'Hacked China.com', *Taipei Times,* 29 Aug. 1999.

information to them. The examples of Chinese hacking outlined above can be considered the latest manifestation of this anti-foreign nationalism, one that serves the state's purpose. In other words, this is as much an internally as an outwardly directed form of propaganda.

Recent studies suggest that it is relatively easy to disrupt a computer network, thereby affecting perception, knowledge and, ultimately, the information needed for rational decision-making. John Arquilla and David Ronfeldt described this as 'netwar': that is, 'information-related conflict at a grand level between nations or societies. It means trying to disrupt, damage, or modify what a target population knows or thinks about itself and the world around it.'[59] For example, the computer system of the polling organization Gallup was attacked for six hours at the height of the 2000 American presidential primary election. The damage was limited, but a more serious attack could have altered the data stored in the system to present a false picture of the election that might have affected the final result. John Vranesevich, operator of the internet security firm AntiOnline, summarized the possibilities: 'To be able to put out a fake story about Microsoft merging with Apple, for example; just rumours about those kind of stories can send stocks skyrocketing.'[60]

As an economic powerhouse at the centre of an Asian Cold War, Taiwan is particularly vulnerable to such rumours and deception. On 6 August 1999 a Chinese-language website registered in the US (but owned by a Chinese company) posted a false news report that a Taiwanese F-5E fighter had been shot down by the Chinese air force.[61] Taiwan's stock market fell by 2 per cent in a single day. In July 1995 the Chinese military fired M-9 tactical ballistic missiles close to Taiwan. Coinciding with stories of financial corruption surfacing in Taiwan's media, these military tests caused the new Taiwan dollar to slip to a four-year low in mid-August 1995, and the Taipei weighted index fell by 19 per cent (more than 1,000 points) between mid-July and mid-August.[62] In May 1990 Taiwan's media reported that a Chinese submarine was engaged in manoeuvres off the island's southern coast. This was immediately followed by a record 510-point stock market crash. Sources in Beijing denied the story,[63] but it is largely irrelevant whether they were telling the truth or not. What this episode demonstrates is that Taiwan is psychologically weakened by the kind of rumours, stories and information that can be easily generated and circulated by hackers through computer networks. The deliberate planting of rumours of

[59] John Arquilla and David Ronfeldt, 'Cyberwar is coming!', *Comparative Strategy* 12, Spring 1993, pp. 144, 146–7.

[60] 'Gallup hacked, Taiwan cyber-attacked', Yahoo! Asia-News, at http://asia.dailynews.yahoo.com/headline, 7 March 2000.

[61] 'Taiwan cites internet rumours', Associated Press, 7 Aug. 1999.

[62] 'Taiwan: pressure cooker', *Far Eastern Economic Review*, 24 Aug. 1995, p. 16.

[63] 'Pingtong faxian Zhonggong qianting' ('Chinese communist submarines discovered outside Pingtong'), *Shijie Ribao* (*World Daily*), 11 May 1990, p. 32; 'Tai gushi you die' ('Taiwan's stockmarket crashes again'), *Shijie Riabo*, 17 May 1990, p. 1. A similar story surfaced in 1999. Taiwan's Central News Agency reported that China planned to reactivate its submarine fleets. Although the story was denied by China, this did not prevent Taiwan's stock market experiencing a large drop in value. See *United Daily News* (Taipei), 27 Nov. 1999, p. 2.

imminent Chinese military attack would be sufficiently effective to destabilize the island, provoke a massive exodus of capital and people, and increase the pressure on Taipei to capitulate to Beijing's terms. This strategy would be consistent with Beijing's ambition to force a political settlement on Taiwan with minimum violence, as the military destruction of Taiwan would serve only to add to Beijing's economic burden and create a less compliant population in Taiwan. A military victory does not necessarily translate into political victory. In other words, computer-based information warfare—like propaganda—may exert a form of psychological pressure that minimizes the need for military conflict: an assessment that is consistent with Chinese approaches to information warfare that emphasize its value in psychological denial and deception operations.[64]

Conclusion

Information warfare grants militaries the opportunity to realize political objectives without causing the quantity of fatal and non-fatal casualties associated with conventional warfare. However, this does not imply that information warfare will be bloodless. If we accept the possibility that information distributed via connectivity is the foundation of modern society, and that information warfare possesses the capacity to target and massively disrupt whole societies and their infrastructures, then the indirect costs are potentially enormous: electricity grids, power stations, water treatment plants, hospitals, etc. could all be casualties of this 'non-lethal strategy'. Bombs and missiles may not be directly responsible for fatalities in modern or 'virtual' warfare, but the disease and poverty that may result from the disruption to vital social services by computer viruses are killers just as effective.

Moreover, the war on terror has brought to the surface a series of new questions that governments, militaries and societies must face to confront the enemy. A suicide bomber may walk into a crowded marketplace in Jerusalem and detonate the explosives strapped around her body, most likely encouraged by local cells of fundamentalists; but it is also possible she received her instructions via a coded email sent from a laptop computer in the mountains of Afghanistan. The military and intelligence communities no longer have exclusive control over information; the proliferation of technology has empowered those with even minimal computer competence, as both the 'hacker' and the 'blogger' cultures demonstrate.

In other words, we can return to the framework of critical security and suggest that the collapse of space and time, the shift of attention from the state to civil society, and the increasing capacity for anonymity mean that computer-based information warfare will play a progressively more important role in facilitating conventional methods of potentially lethal activity.

[64] Kate Farris, 'Chinese views of information warfare', *Defense Intelligence Journal* 10: 1, 2001, p. 38.

In addition, we must recognize that information warfare is not a modern phenomenon. The history of propaganda and psychological operations is centuries old, and the sword has always fought against the mind. This article suggests that while computer-based information warfare allows for a more precise and therefore potentially more effective form of propaganda than print media, radio and television, it is also an instrument *of* propaganda, and that in the case-study presented the threat of information warfare across the Taiwan Strait is limited and exaggerated. There is no doubt that both sides are actively preparing offensive and defensive capabilities, but it is unlikely that either will deploy its information warfare arsenal without first deciding to launch a conventional attack. The academic, political and military communities throughout the world agree that such a conventional attack is not impossible, but they remain divided on the probability of conflict. In the meantime, information warfare continues to play a pivotal role in cross-Strait propaganda, as demonstrated by the 'hacking' of computer systems that takes place in the aftermath of a downturn in China–Taiwan relations, and by the planting of rumours and stories that can have a dramatic and detrimental effect on the social psychology of the other side. (Taiwan's Ministry of National Defense claims that there are over 300 Chinese agencies disseminating false information in Taiwan to spread panic and destabilize the stock market, but the accuracy of these allegations is difficult to establish.)

We must accept that a revolution in military affairs has taken place within the People's Liberation Army, and the priorities identified within the PLA for research and investment do acknowledge the implementation of high-tech military strategies.[65] However, the consensus among observers is that these are designed to drive China's long-term ambition to be a major world player in military affairs, rather than to present a realistic threat to Taiwan. In other words, the expressed commitment to the development of information warfare capacity consolidates the projection of strength to the regional and international community, with little regard for actual capabilities.[66]

Both Taiwan and China are mistaken to believe that computer-based information warfare will provide the architecture for any cross-Strait military confrontation. While Beijing calculates the possibility of intervention by the American military, Taiwan faces a formidable military machine across the Taiwan Strait,[67] a PLA that is fundamentally different from the organization created by Mao to fight a 'people's war': 'Today, the PLA is more combat-capable, multilayered, and integrated. Its conventional forces are more streamlined, lethal, mobile, versatile, better co-ordinated, and have a greater operational

[65] Richard Bitzinger, 'Going places or running in place? China's efforts to leverage advanced technologies in military use', in Susan M. Puska, ed., *People's Liberation Army after next* (Carlisle, PA: Strategic Studies Institute, 2000), p. 14.

[66] O'Hanlon, 'Why China cannot conquer Taiwan'.

[67] 'The backbone of the PLA's missile forces opposite Taiwan are the Dongfeng-11 and Dongfeng-15 SRBMs. They are expected to be augmented in coming years with conventionally armed Dongfeng-21/25 medium-range ballistic missiles. China is also expected to develop cruise missiles for land attack to boost its ability to strike Taiwan': Lague, 'Chen launches his missile vote', p. 26.

reach … [T]he downsized Chinese forces have retained their quantitative superiority … Barring US intervention, the PLA could overwhelm Taiwan's modernizing army.'[68] Yet Major-General Chen Wen-chien described information security as the 'top priority task of the military'.[69] Clearly, China is winning the information war; propaganda about its capacity to inflict heavy damage on Taiwan through its application of information technology is sufficiently intimidating to push Taiwan towards perceiving its inferiority in this area. Reinforced by the reality of 600 missiles located in Fujian province and pointing at the island, this propaganda exerts substantial psychological pressure on Taiwan and its inhabitants.

In assessing information warfare the imponderables are many. The discourse nurtures the propaganda strategies—and it is propaganda that has characterized the cross-Strait conflict since 1949—but the promise of information warfare remains, as yet, unfulfilled. Risk estimates 'always move between paranoia and carelessness, without ever being precise. The relevant studies and analyses are therefore full of terms like "capability", "possibility" or "could".'[70] The militaries on both sides of the Taiwan Strait have yet to move beyond this level of discourse.

[68] Chong-Pin Lin, 'Red fist: China's army in transition', *International Defense Review* 28, Feb. 1995, p. 34.
[69] 'Taiwan's first information warfare group enters service', *Taipei Times*, 3 Jan. 2001.
[70] Bendrath, 'The cyberwar debate', pp. 80–103.