September 15, 2005

“Chinese Information Operations Strategies in a Taiwan Contingency”

Testimony of James C. Mulvenon, Ph.D.
Director, Advanced Studies and Analysis
DGI Center for Intelligence Research and Analysis

Before the U.S.-China Economic and Security Review Commission Hearing
“China’s Military Modernization and the Cross-Strait Balance”

INTRODUCTION

Thank you, Mr. Chairman and the other members of the U.S.-China Economic and Security Review Commission for the opportunity to take part in the hearings you are holding today on the topic of In the minds of the Chinese leadership, the available evidence suggests that the most important political-military challenge and the most likely flashpoint for Sino-US conflict is Taiwan. In seeking to reunify the island with the mainland, however, it is important to note that the PRC has a political strategy with a military component, not a military strategy with a political component. The PRC would prefer to win without fighting, since Beijing's worst case outcome is a failed operation that would result in *de facto* independence for Taiwan. Also, the leadership realizes that attacking Taiwan with kinetic weapons will result in significant international opprobrium and make the native population ungovernable. These assumptions explain why China until recently maintained a "wait and see" attitude towards Taiwan, even though the island elected a President from a party committed previously to independence. From 2000 until late 2003, China eschewed saber-rattling in favor of economic enticement and “united front” cooperation with the Pan-Blue opposition, both of which were believed to be working successfully. In November 2003, in response to perceived provocations by Taiwan President Chen Shui-bian, Beijing once again revived the threat of military force to deter what it saw as further slippage towards independence, dramatically increasing tensions in the U.S., China, Taiwan triangle.

Should the situation deteriorate into direct military conflict, the PLA since 1992 has been hard at work bolstering the hedging options of the leadership, developing advanced campaign doctrines, testing the concepts in increasingly complex training and exercises, and integrating new indigenous and imported weapons systems. At the strategic level, the writings of Chinese military authors suggest that there are two main centers of gravity in a Taiwan scenario. The first of these is the will of the Taiwanese people, which they hope to undermine through exercises, missile attacks, SOF operations, and other operations that have a psyop focus. Based on intelligence from the 1995-1996 exercises, as well as public opinion polling in Taiwan, China appears to have concluded that the Taiwanese people do not have the stomach for conflict and will therefore sue for peace after suffering only a small amount of pain. The second center of gravity is the will and capability of the United States to intervene decisively in a cross-strait conflict. In a strategic sense, China has traditionally believed that its ICBM inventory, which is capable of striking CONUS, will serve as a deterrent to US intervention or at least a brake on escalation. Closer to Taiwan, the PLA has been engaged in an active program of equipment modernization, purchasing niche anti-access, area-denial capabilities such as long-range cruise missiles and submarines to shape the operational calculus of the American carrier battle group commander on station. At the same time, a key lesson learned from analyzing U.S. military operations since DESERT STORM was the vulnerability of the logistics and deployment system.

CENTER OF GRAVITY NUMBER ONE: THE WILL OF THE PEOPLE ON TAIWAN

Chinese strategies to manipulate the national psychology of the populace and leadership on Taiwan involve the full spectrum of information operations, including psychological operations, special operations, computer network operations, and intelligence operations. To this end, Beijing can employ all of the social, economic, political and military tools of Chinese national power, as well as enlist the assistance of private sector players and sympathetic co-conspirators on Taiwan. The goal of these efforts is to shake the widely perceived psychological fragility of the populace, causing the government to prematurely capitulate to political negotiations with the mainland. In a sense, China seeks to use the immaturity of Taiwanese democracy against itself.

Analysis of both Beijing's strategies in this arena as well as Taipei's ability to resist such methods confirms Taiwan's high level vulnerability to Chinese soft coercion, and raises major questions about the island's viability in the opening phase of a PRC coercion campaign, their credibility as an source of intelligence information on the mainland and a keeper of U.S. secrets, and their expected ability to interoperate successfully with U.S. forces in a crisis.

Taiwan's vulnerabilities in the critical infrastructure protection arena can be divided into two categories: informational and physical. On the information side, Taiwan is a highly information-dependent society with a relatively low level of information or computer security. Significant disruptions in information systems could have major negative effects on the island, particularly in the economic and financial realms, and increase fear and panic among the population. Past Chinese uses of regional media to send psychological operations messages have also enjoyed success in affecting popular morale and public opinion. For example, an Internet rumor in 1999 that a Chinese Su-27 had shot down a Taiwan aircraft caused the Taipei stock market to drop more than two percent in less than four hours.

On the physical side of the equation, Taiwan's current capability and readiness level is much lower than one might expect for a state under such a direct level of threat, especially when compared with other "national security states" like Israel or South

Korea. Critical infrastructure protection has been a low priority for the government, and Taiwan is acutely vulnerable to Spetnaz-like or fifth column operations, aided significantly by ethnic and linguistic homogeneity and significant cross-border flows, which facilitate entry and access to potential targets. In terms of civilian infrastructure, Taiwan's telecommunications, electric power, and transportation infrastructure are all highly susceptible to sabotage. These weaknesses have been indirectly exposed by periodic natural disasters, such as the September 1999 earthquake and the September 2001 typhoon, when the communications infrastructure effectively collapsed. Taiwan's ports, including Su'ao, Jeelung, and Gaoxiong (the third highest volume container port in the world), are attractive targets. Port charts and ship movements are available on the Internet, and Gaoxiong in particular has two narrow mouths that could easily be blocked with scuttled vessels. Taiwan's highways are a vulnerable bottleneck, particularly given the large number of undefended mountain tunnels and bridges that could be destroyed by SOF units. Finally, the power grid is known to be fragile, marked by numerous single-point failure nodes, and no cross-hatching of sub-grids to form redundancy. The loss of a single tower in the central mountainous region, thanks to a landslide, knocked out ninety percent of the grid a couple of years ago, and delays in construction of a fourth nuclear plan have constrained capacity.

Special operations forces and fifth column are also a major threat for disruption of military command and control and decapitation of the national command authority, as well as providing reconnaissance for initial missile and air strikes and battle damage assessments (BDA) for follow-on strikes. Entry into the country for special operations forces is not a substantial obstacle, thanks to ethnic and linguistic homogeneity and the dramatic increases in cross-strait people flows. Between 1988 and October 2002, for example, more than 828,000 mainlanders visited the island. Moreover, these special forces could also facilitate control of key civilian and military airfields and ports that could be used as points of entry for invading forces. The lack of operational security at key facilities is particularly inexplicable and appalling. Visits to national political and military command centers reveal them to relatively unguarded with poor information security practices, including the use of personal cell phones in supposedly secure areas. The Presidential Palace in downtown Taipei, home to the President and his key staff, has no fenceline and no security checkpoints. Building information, including the location of the President's office, is openly available on the Internet. Given the poor performance of President Chen's personal security detail during the recent assassination attempt on his life, the possibility of elimination of the top leadership through direct action cannot be discounted.

Finally, there is substantial open source evidence to suggest that China is winning the intelligence war across the strait, raising serious doubts about the purity of Taiwanese intelligence proffered to the U.S., the safety of advanced military technologies transferred to the island, and the ability of official Taiwan interlocutors to safeguard shared U.S. secrets about intelligence collection or joint warplanning. In the last five years, a steady series of leaked stories have appeared in the Taiwan and other regional media, describing either the rounding up of Taiwanese agent networks on the mainland or the unmasking of high-ranking Taiwanese agents in the military, with similar successes a rarity on the Taiwan side, despite significant political incentive to publicize such discoveries. Reported examples since only early 2003 include the arrest of the president of the PLA Air Force Command Academy, Major-Genera Liu Guangzhi, his former deputy, Major-General Li Suolin, and ten of their subordinates; the arrest of 24 Taiwanese and 19 mainlanders in late 2003; the arrest of Chang Hsu-min, 27, and his 24-year-old girlfriend Yu Shi-ping; the arrest of Xu Jianchi; the arrest of Ma Peiming in February 2003; and the arrest and conviction to life imprisonment of Petty officer first class Liu Yueh-lung for passing naval communications codes to the PRC. Farther back, high-profile intelligence losses include the discovery, arrest and execution of General Logistics Department Lieutenant-General Liu Liankun and Senior Colonel Shao Zhengzhong as a result of Taiwanese government intelligence disclosures about the fact that warheads on Chinese missiles fired near the island in 1996 were unarmed, the arrest and sentencing of Hainan Province deputy head Lin Kecheng and nine others in 1999 for providing economic, political and other kinds of intelligence to the Taiwan Military Intelligence Bureau, and the arrest and imprisonment of a local official in Nanchong, Sichuan named Wang Ping for allegedly also working for the MIB. In addition, retired senior Taiwan intelligence officials, including National Security Bureau personnel chief Pan Hsi-hsien and at least one former J-2, continue to travel to and often residence in China despite Taiwan regulations barring such movement for three years after retirement. At the same time, Taiwan and international media is regularly filled with leaks about sensitive U.S.-Taiwan military interactions or weapons transfers, sourced to either legislators or standing Taiwan government officials. Examples include disclosures about possible deployment of an Integrated Underwater Surveillance System (IUSS) north and south of the island to detect Chinese submarines, the provision of early warning data on Chinese missile attack from the Defense Support Program (DSP) satellite constellation, and the alleged SIGINT cooperation between the National Security Agency and Taiwan on Yangming Mountain. All of these possible compromises raise serious concerns about future technology or information sharing with Taiwan.

CENTER OF GRAVITY NUMBER TWO: U.S. MILITARY INTERVENTION

Strategies for Attacking U.S. Logistics

When Chinese strategists contemplate how to affect U.S. deployments, they confront the limitations of their current conventional force, which does not have range sufficient to interdict U.S. facilities or assets beyond the Japanese home islands. Nuclear options, while theoretically available, are nonetheless far too escalatory to be used so early in the conflict. Theater missile systems, which are possibly moving to a mixture of conventional and nuclear warheads, could be used against Japan or Guam, but uncertainties about the nature of a given warhead would likely generate responses similar to the nuclear scenario.

According to the predictable cadre of “true believers,” both of the centers of gravity identified above can be attacked using computer network operations. In the first case, the Chinese IO community believes that CNO will play a useful psychological role in undermining the will of the Taiwanese people by attacking infrastructure and economic vitality. In the second case, the Chinese IO community envisions computer network effectively deterring or delaying US intervention and cause pain sufficient to compel Taipei to capitulate before the US arrives. The remainder of this section outlines how these IO theorists propose operationalizing such a strategy.

General IO and Computer Network Attack Analysis

Before examining this scenario in detail, it is first necessary to provide some background regarding Chinese views of information operations in general, and computer network operations in particular. At the strategic level, contemporary writers view IO and CNO as a useful supplements to conventional warfighting capability, and powerful asymmetric options for "overcoming the superior with the inferior.” According to one PRC author, "computer network attack is one of the most effective means for a weak military to fight a strong one.” Yet another important theme in Chinese writings on CNO is the use of computer network attack as the spearpoint of deterrence. Emphasizing the potential role of CNA in this type of signaling, a PRC strategist writes that "We must send a message to the enemy through computer network attack, forcing the enemy to give up without fighting.” Computer network attack is particularly attractive to the PLA, since it has a longer range than their conventional power projection assets. This allows the PLA to "reach out and touch" the U.S., even in the continental United States. "Thanks to computers," one strategist writes, " long-distance surveillance and accurate, powerful and long-distance attacks are now available to our military.” Yet computer network attack is also believed to enjoy a high degree of “plausible deniability,” rendering it a possible tool of strategic denial and deception. As one source notes, "An information war is inexpensive, as the enemy country can receive a paralyzing blow through the Internet, and the party on the receiving end will not be able to tell whether it is a child's prank or an attack from an enemy.”

It is important to note that Chinese CNA doctrine focuses on disruption and paralysis, not destruction. Philosophically and historically, the evolving doctrine draws inspiration from Mao Zedong' theory of "protracted war," in which he argued that "we must as far as possible seal up the enemies' eyes and ears, and make them become blind and deaf, and we must as far as possible confuse the minds of their commanders and turn them into madmen, using this to achieve our own victory." In the modem age, one authoritative source states: “computer warfare targets computers - the core of weapons systems and C4I systems - in order to paralyze the enemy.” The goal of this paralyzing attack is to inflict a "mortal blow" [zhiming daji], though this does not necessarily refer to defeat. Instead, Chinese analysts often speak of using these attacks to deter the enemy, or to raise the costs of conflict to an unacceptable level. Specifically, computer network attacks on non-military targets are designed to "...shake war resoluteness, destroy war potential and win the upper hand in war," thus undermining the political will of the population for participation in military conflict.

At an operational level, the emerging Chinese IO strategy has five key features. First, Chinese authors emphasize defense as the top priority, and chastise American theorists for their "fetish of the offensive." In interviews, analysts assert their belief that the US is already carrying out extensive computer network exploit activities against Chinese servers. As a result, CND must be the highest priority in peacetime, and only after that problem is solved can they consider "tactical counteroffensives." Second, IW is viewed as an unconventional warfare weapon to be used in the opening phase of the conflict, not a battlefield force multiplier that can be employed during every phase of the war. PLA analysts believe that a bolt from the blue at the beginning is necessary, because the enemy may simply unplug the network, denying them access to the target set, or patch the relevant vulnerabilities, thus obviating all prior intelligence preparation of the battlefield. Third, IW is seen as a tool to permit China to fight and win an information campaign, precluding the need for conventional military action. Fourth, China's enemies, in particular the United States, are seen as "information dependent," while China is not. This latter point is an interesting misperception, given that the current Chinese C4I modernization is paradoxically making them more vulnerable to US methods.

Perhaps most significant, computer network attack is characterized as a preemption weapon to be used under the rubric of the rising Chinese strategy of *xianfa zhiren*, or "gaining mastery before the enemy has struck." Preemption [xianfa zhiren] is a core concept of emerging Chinese military doctrine. One author recommends that an effective strategy by which the weaker party can overcome its more powerful enemy is "to take advantage of serious gaps in the deployment of forces by the enemy with a high tech edge by launching a preemptive strike during the early phase of the war or in the preparations leading to the offensive." Confirming earlier analysis of Chinese views of U.S. operational vulnerabilities in the deployment phase, the reason for striking is that the "enemy is most vulnerable during the early phase of the war." In terms of specific targets, the author asserts that "we should zero in on the hubs and other crucial links in the system that moves enemy troops as well as the war-making machine, such as harbors, airports, means of transportation, battlefield installations, and the communications, command and control and information systems." If these targets are not attacked or the attack fails, the "high-tech equipped enemy" will amass troops and deploy hardware swiftly to the war zone, where it will carry out "large-scale airstrikes in an attempt to weaken...China's combat capability." More recent and authoritative sources expand on this view. "In order to control information power," one source states, "there must also be preemption.. .information offensives mainly rely on distant battle and stealth in order to be effective, and are best used as a surprise...Therefore, it is clear that whoever strikes first has the advantage.” "The best defense is offense," according to the authors of *Information Operations.* "We must launch preemptive attacks to disrupt and destroy enemy computer systems."

Specific Targeting Analysis of Network Attacks Against Logistics

There are two macro-level targets for Chinese computer network operations: military network information and military information stored on networks. Computer network attack seeks to use the former to degrade the latter. Like US doctrine, Chinese CNA targeting therefore focuses specifically on "enemy C2 centers," especially "enemy information systems." Of these information systems, PLA writings and interviews suggest that logistics computer systems are a top military target. According to one PLA source, "we must zero in on the...crucial links in the system that move enemy troops... such as information systems." Another source writes, “we must attack system information accuracy, timeliness of information, and reliability of information.” In addition to logistics computer systems, another key military target for Chinese CNA is military reliance on civilian communications systems.

These concepts, combined with the earlier analysis of the PLA view that the main US weakness is the deployment phase, lead PLA IO theorists to conclude that US dependence on computer systems, particularly logistics systems, is a weak link that could potentially be exploited through computer network attack. Specifically, Chinese authors highlight DoD’s need to use the civilian backbone and unclassified computer networks (i.e., NIPRNET) as an "Achilles Heel." There is also recognition of the fact that operations in the Pacific are especially reliant on precisely coordinated transportation, communications, and logistics networks, given the “tyranny of distance” in the theater. PLA strategists believe that a disruptive computer network attack against these systems or affiliated civilian systems could potentially delay or degrade U.S. force deployment to the region while allowing the PRC to maintain a degree of plausible deniability.

The Chinese are right to highlight the NIPRNET as an attractive and accessible target, unlike its classified counterparts. It is attractive because it contains and transmits critical deployment information in the all-important TPFDL (time-phased force deployment list), which is valuable for both intelligence-gathering about US military operations but also a lucrative target for disruptive attacks. In terms of accessibility, it is relatively easy to gather data about the NIRPNET from open sources, at least before 9/11. Moreover, the very nature of system is the source of its vulnerabilities, since it has to be unclassified and connected to the greater global network, albeit through protected gateways. To migrate all of the NIPRNET to a secure, air-gapped network would likely tax the resources and bandwidth of DOD's military networks.

DoD’s classified networks, on the other hand, are an attractive but less accessible target for the Chinese. On the one hand, these networks would be an intelligence gold mine, and is likely a priority computer network exploit target. On the other hand, they are a less attractive computer network attack target, however, thanks to the difficulty of penetrating its defenses. Any overall Chinese military strategy predicated on a high degree of success in penetrating these networks during crisis or war is a high-risk venture, and increases the chances of failure of the overall effort to an unacceptable level. Moreover, internal PRC writings on information warfare show no confidence in the PRC's ability to get inside network-centric warfare aboard deployed ships or other self-contained operational units. Instead, the literature is focused on preventing the units from deploying in the first place, and thereafter breaking the C4I linkages between the ships and their headquarters.

Chinese CNE or CNA operations against logistics networks could have a detrimental impact on US logistics support to operations. PRC computer network exploit activities directed against US military logistics networks could reveal force deployment information, such as the names of ships deployed, readiness status of various units, timing and destination of deployments, and rendezvous schedules. This is especially important for the Chinese in times of crisis, since the PRC in peacetime utilizes US military web sites and newspapers as a principal source for deployment information. An article in October 2001 in *People's Daily,* for example, explicitly cited US Navy web sites for information about the origins, destination and purpose of two carrier battle groups exercising in the South China Sea. Since the quantity and quality of deployment information on open websites has been dramatically reduced after 9/11, the intelligence benefits (necessity?) of exploiting the NIPRNET have become even more paramount. Computer network attack could also delay re-supply to the theater by misdirecting stores, fuel, and munitions, corrupting or deleting inventory files, and thereby hindering mission capability.

The advantages to this strategy are numerous: (1) it is available to the PLA in the near-term; (2) it does not require the PLA to be able to attack/invade Taiwan with air/sea assets; (3) it has a reasonable level of deniability, provided that the attack is sophisticated enough to prevent tracing; (4) it exploits perceived US casualty aversion, over-attention to force protection, the tyranny of distance in the Pacific, and US dependence on information systems; and (5) it could achieve the desired operational and psychological effects: deterrence of US response or degrading of deployments.

CONCLUSIONS: IS THE SCENARIO REALISTIC?

Chinese IO theorists assert that computer networks attacks against unclassified computer systems or affiliated civilian systems, combined with a coordinated campaign of short-range ballistic missile attacks, "fifth column," and IW attacks against Taiwanese critical infrastructure, could quickly force Taiwan to capitulate to Beijing. This strategy exploits serious vulnerabilities, particularly with regards to Taiwanese critical infrastructure and U.S. military reliance on the NIPRNET, but is also partially predicated on a set of misunderstandings, misperceptions, and exaggerations of both U.S. logistics operations and the efficacy of PLA information operations. This final section assesses the balance of these perceptions and misperceptions, concluding with an evaluation of the cost-benefit calculus for the PLA in undertaking such an effort.

Chinese Strategies Against U.S. Logistics Systems and Operations

The Chinese are correct to point to the NIPRNET as a potential vulnerability, but would such an attack actually produce the desired effect? First, there is the issue of the "ready" carrier battle group at Yokusuka, which is only a few days steam away from

Taiwan. Though extended re-supply might be degraded, the group’s arrival time would not be heavily affected by attacks on the NIPRNET, undermining a strategic goal of the attacks in the first place. In response, PLA analysts point to times in the last several years when there was no ready carrier in the Pacific because it was “gapped” in the Mediterranean or in the Persian Gulf. More recently, PLA analysts took note of the DOD's formal revision of its strategy from 2 MTWs to 1 MTW. In both cases, they could envision scenarios in which US forces would require seven or more days to arrive near Taiwan, potentially providing China with a "window of opportunity" to carry out rapid coercive operations against Taiwan.

Second, there is the issue of Chinese characterizations of the U.S. logistics system itself. The Chinese tend to overemphasize the U.S. reliance on computers. The writings of some Chinese strategists indicate that they believe the U.S. system cannot function effectively without these computer networks. Moreover, PRC strategists generally underestimate the capacity of the system to use paper, pencil, fax and phone if necessary. In fact, interviews with current logistics personnel suggest that downtime on these systems is a regular occurrence, forcing US logistics personnel to periodically employ non-computerized solutions. At the same time, there is also evidence that U.S. logistics systems are moving toward increasing automation, which would increase the potential impact of an attack against the NIPRNET.

Third, Chinese analysis seems predicated on questionable assumptions about American casualty aversion, particularly the notion that U.S. forces would not deploy to a Taiwan contingency until all of the assets were in place. If logistics delays meant that some part of the force protection package would not be available, they assume, then U.S. forces would wait until they arrived before intervening in the conflict. This is a debatable assumption, particularly given the precedence of the two CVBG deployment in 1996 and Washington’s considerable interests in the maintenance of peace and stability in the Strait.

Could the Chinese Actually Do It? In terms of courses of action, interviews and classified writings reveal interest in the full spectrum of computer network attack tools, including hacking, viruses, physical attack, insider sabotage, and electromagnetic attack. One of the most difficult challenges of this type of analysis is measuring China’s actual computer network attack capability. In rough terms, a computer network attack capability requires four things, three of which are easy to obtain and one of which is harder. The easy three are a computer, an Internet connection, and hacker tools, thousands of which can be downloaded from enthusiast sites around the globe. The more difficult piece of the puzzle to acquire is the operator himself, the computer hacker. While individuals of this ilk are abundant in China’s urban centers, they are also correctly perceived to be a social group unlikely to relish military or governmental service.

The answer may be found in the rise of “patriotic hacking” by increasingly sophisticated, nationalistic hacker groups. As demonstrated by the "hacker wars" that followed former Taiwan President Lee Teng-hui's announcement of "special state-to-state relations," the US bombing of the Chinese Embassy in Yugoslavia, and the EP-3 crisis, patriotic hacking appears to have become a permanent feature of Chinese foreign and security policy crises in recent years. One the one hand, the emergence of this trend presents the PRC military and political leadership with serious command and control problems. Specifically, uncontrolled hacking by irregulars against the US and Taiwan could potentially undermine a PRC political-military coercive diplomacy strategy vis-a-vis Taiwan and the United States during a crisis. Unlike traditional military instruments such as missiles, many of the levers of computer network operations by "unofficial means" are beyond the control of the Chinese government. This could negate the intended impact of strategic pausing and other political signals during a crisis. Yet at the same time patriotic hacking offers several new opportunities for the PRC. First, it increases plausible deniability for official Chinese CNA/CNE. Second, it has the potential to create a large, if unsophisticated set of operators who could engage in disruption activities against US and Taiwan networks. One classified PLA document obtained by Taiwan intelligence emphasizes the use of the "unofficial power of IW" and highlights the role of non-state actors in achieving state coercion goals.

For these reasons, some Western analysts have been tempted to assert that the patriotic hackers are “controlled” by Beijing. Among the arguments marshaled to support this thesis is the fact that consistently harsh punishments are meted out to individuals in China committing relatively minor computer crimes, while patriotic hackers appear to suffer no sanction for their brazen contravention of Chinese law. Other analysts begin from the specious premise that since the Chinese government “owns” the Internet in China, therefore patriotic hackers must work for the state. Still others correctly point to the fact that a number of these groups, such as Xfocus and NSFocus, appear to be morphing into “white-hat” hackers (i.e., becoming professional information security professionals), often developing relationships with companies associated with the Ministry of Public Security or the ministry itself. Yet interviews with hackers and officials strongly suggest that the groups truly are independent actors, more correctly labeled “state-tolerated” or “state-encouraged.” They are tolerated because are “useful idiots” for the regime, but they are also careful not to pursue domestic hacking activities that might threaten “internal stability” and thereby activate the repression apparatus.

Indeed, most of the groups have issued constitutions or other organizing documents that specifically prohibit members from attacking Chinese web sites or networks.

Even if it is true that patriotic hacker groups are not controlled by the state, Beijing is still worried about the possible effect of their behavior in a crisis with the United States and/or Taiwan. Analysis of several recent "hacker wars" over the last two years suggests an evolving mechanism for shaping the activities of "patriotic hackers.” In August 1999, after the conclusion of the cross-strait hacker skirmish that erupted in the wake of Taiwan President Li Teng-hui's declaration that the island's relationship to the mainland was a "state-to-state relationship," a *Liberation Army Daily* article lauded the "patriotic hackers" and encouraged other hackers to join-in during the next crisis with Taiwan. In April 2001, *Guangzhou Daily* reprinted without attribution a *Wired* article on the impending outbreak of a "hacker war" between Chinese and American hackers, which many hackers saw as a sign of government backing. A media-generated hacker war thereafter ensued, with Chinese and American hackers defacing hundreds, if not thousands, of web sites. In May 2001, however, an authoritative *People's Daily* article rebuked both Western and Chinese hackers, calling activities by both sides "illegal." This signaled to the hackers that the state had withdrawn its sanction of their activities, and hacker activity quickly tapered off in response to the warning.

A year later, patriotic hacker chat rooms were filled with discussion and planning for a “first anniversary” hacker war. In late April 2002, on the eve of the proposed conflict, *People’s Daily* published another unsigned editorial on the subject, decrying the loose talk about a hacker war and warning of serious consequences. Participants in the hacker chat rooms quickly recognized the signal, and the plans for a new hacker war were abandoned. In neither case could this dynamic be called control, but instead reflects the population’s keen sensitivity to the subtle messages in government propaganda, which continues to successfully create a Leninist climate of self-deterrence and self-censorship that is more powerful than active state repression. As some groups move into “white-hat” positions, however, the relationship might actually transition from a ruler-ruled dynamic to a partnership motivated by reasons ranging from nationalism to naked self-interest.

A final issue related to measuring capability involves the assessment of a group or country’s ability to generate new attack tools or exploits. Outside analysts, many of whom are programmers themselves, tend to reify countries like Russia that abound with highly talented programmers, and look down upon countries or individuals that simply use off-the-shelf “script kiddie” tools like distributed denial of service (DDOS) programs. DDOS is admittedly a blunt instrument, but a fixation on finding more sophisticated attacks, which reflects the widely-held but logically tenuous assumption that statesponsorship correlates with sophistication, may be counterproductive. Instead, analysts should employ a simple “means-ends” test. In the Chinese case, DDOS, despite its relatively simplicity, looks like the right tool for the right mission. From the Chinese point of view, for example, hammering the NIPRNET and forcing it to be taken down for repairs would be considered an operational success, since it could potentially delay or degrade U.S. logistics deployments to Taiwan.

In conclusion, therefore, a strategy to disrupt U.S. logistics systems with computer network attack seems well-matched to U.S. vulnerabilities and Chinese capabilities, though the final operational impact of the effort may be undermined by important Chinese misperceptions about political will and the nature of U.S. logistics operations.