DRAFT-NOT FOR CITATION-DRAFT-NOT FOR CITATION-DRAFT

COMPARING US, RUSSIAN, AND CHINESE INFORMATION OPERATIONS CONCEPTS

BY

MR. TIMOTHY L. THOMAS
FOREIGN MILITARY STUDIES OFFICE
FORT LEAVENWORTH, KS 66048
FEBRUARY 2004

Disclaimer

The views expressed in this report are those of the author and do not necessarily represent the official policy or position of the Department of the Army, Department of Defense, or the U.S. government.

The Foreign Military Studies Office (FMSO) assesses regional military and security issues through open-source media and direct engagement with foreign military and security specialists to advise army leadership on issues of policy and planning critical to the U.S. Army and the wider military community.

Please forward comments referencing this study to:

FMSO
ATZL-CTL MR. THOMAS
101 MEADE AVENUE
FT LEAVENWORTH KANSAS 66027-2322

COM: (913) 684-5957
DSN: 552-5957
FAX: (913) 684-4701

E-MAIL: THOMAST@LEAVENWORTH.ARMY.MIL

COMPARING US, RUSSIAN, AND CHINESE INFORMATION OPERATIONS CONCEPTS

BY

MR. TIMOTHY L. THOMAS
FOREIGN MILITARY STUDIES OFFICE
FORT LEAVENWORTH, KS 66048
FEBRUARY 2004

Disclaimer

The views expressed in this report are those of the author and do not necessarily represent the official policy or position of the Department of the Army, Department of Defense, or the U.S. government.

The Foreign Military Studies Office (FMSO) assesses regional military and security issues through open-source media and direct engagement with foreign military and security specialists to advise army leadership on issues of policy and planning critical to the U.S. Army and the wider military community.

Please forward comments referencing this study to:

FMSO
ATZL-CTL MR. THOMAS
101 MEADE AVENUE
FT LEAVENWORTH KANSAS 66027-2322

COM: (913) 684-5957
DSN: 552-5957
FAX: (913) 684-4701

E-MAIL: THOMAST@LEAVENWORTH.ARMY.MIL

ABSTRACT

Over the past ten years, Russia and China have developed concepts of information operations (IO) and information superiority (IS) that differ from their US counterpart. Russia divides its IO theory into two aspects: information-technical and information-psychological aspects. With respect to information superiority, the Russians believe the key is to maintain organization. Only when a force becomes disorganized does it lose its ability to maintain information superiority. China IO expert Dai Qingmin defined IO as "a series of operations with an information environment as the basic battlefield condition, with military information and an information system as the direct operational target, and with electronic warfare and a computer network war as the principal forms." China terms its network centric operations as "integrated network-electronic" warfare. China's focus in the area of information superiority is built around stratagems and control, with the latter receiving nearly as much attention as the former. These and other significant differences (to include a critique of US IO) will be highlighted for the symposium's attendees.

INTRODUCTION

Over the past ten years, the United States, Russia and China have developed their own concepts of information war (IW), information operations (IO) and information superiority (IS). It is somewhat easy to ascertain the US approach to these concepts. This is because the US publishes much of its doctrine in an unclassified format as Joint Publications (JP) or Field Manuals (FM). The US does indeed have a JP and FM on IO. Neither Russia nor China publishes such a document and thus the analyst is left to ascertain a plausible description of IW, IO or IS based on reading academic and military (quasi official) views.

The US armed forces expect to publish a new version of JP 3-13, Information Operations, last published in 1998, in 2004 or, at the latest, 2005. The old document emphasized six offensive and eight defensive "assigned and supporting capabilities and activities."[1] The 1998 JP also emphasized the necessity of obtaining and maintaining information superiority during IO. Much emphasis is currently being placed on network-centric operations in US IO theory.

Russia has two aspects to its IO theory: information-technical and information-psychological. Not only are these different from the US's "assigned and supporting capabilities and activities", but Russia also views IS differently. Russian theorists place as much emphasis on "disorganizing" the enemy as they do toward achieving information superiority. In fact, they believe the former produces the latter. Russia currently has not explained its equivalent concept of "network-centric operations" to western audiences. However, Russia is developing the concept of an information weapon to great effect, a term the US military and the State Department do not define.

[1] Joint Pub 3-13, Joint Doctrine for Information Operations, 9 October 1998, p. viii.

China has developed six "forms" (not capabilities or elements like the US but similar in content) for its IO theory: operational security, military deception, psychological war, electronic war (EW), computer network war, and physical destruction. Chinese authors consider “control” to be nearly as important as information superiority. Again, the former results in the latter. China’s focus for attaining information superiority/control is built around the use of stratagems, whereas the US focuses on speed and efficiency. China views network centric operations in a slightly different manner than does the US, calling their nearly equivalent theory "integrated network-electronic" warfare.

This paper develops a comparative view of these theories, and highlights strengths and weaknesses of each. As the comments demonstrate, these concepts may vary radically in the three countries under consideration. At times one can feel as if lost in the Bermuda triangle of IO terminology.

THE UNITED STATES

The definitions of information war (IW) and information operations (IO) have been under constant revision in the US. For comparative purposes some of the more recent definitions are presented here. First, however, an operation and war are defined.

JP 1-02, the Department of Defense Dictionary of Military and Related Terms , defines an operation as Aa military action or the carrying out of a strategic, tactical, service, training, or administrative military mission; the process of carrying on combat, including movement, supply, attack, defense and maneuvers needed to gain the objectives of any battle or campaign.@[2] It would appear, based on an examination of this definition, that IO’s definition should include the terms movement, maneuver and objectives, among other terms.

The 1998 Joint Publication 3-13, Joint Doctrine for Information Operations, and the JP 1-02 (the latter last updated on 5 June 2003) both defined information operations as “actions taken to affect adversary information and information systems, while defending one’s own information and information systems (major capabilities to conduct IO include, but are not limited to, OPSEC, PSYOP, military deception, EW, and physical attack/destruction, and could include computer network attack).” Both publications defined IW as “information operations conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries.”[3] Thus the official definition appears to limit IO to offensive and defensive activities.

Further, the definition’s focus is clearly on the information systems of equipment and not on mental perception or reaction. In fact, the term “information security” as defined in JP 3-13 relates entirely to equipment and systems. The gamut is insufficient to

[2] JP 1-02, the Department of Defense Dictionary of Military and Related Terms , Internet version, last updated 5 June 2003.
[3] Joint Pub 3-13, Joint Doctrine for Information Operations, 9 October 1998, p. I-9, I-11..

clearly define IO given that Army Field Manual 3.0, Operations, touts information superiority as capable of putting disparity in the enemy commander's mind between reality and their perception of reality. The theory talks about influencing the mind of the commander, while the definitions relate to equipment and give scant reference to the mind. Most likely the latter concept will be included in the new version of JP 3-13, giving the manual a boost to the mental aspect of IO.

JP 1-02 *does not define war*. This is rather odd, since we define IW. How can one possibly agree with the definition of IW found in JP 3-13 or JP 1-02, since we don't know what half of the definition means? Perhaps the term invites too much controversy. On the other hand, avoidance of controversy should never be an acceptable price for lack of clarity, an especially troubling condition considering the emphasis we put on the correct determination of an "objective" or a "center of gravity" as an operational or strategic principle.

The latter half of JP 1-02's definition of IW sounds more like the definition of an operation, in that an operation carries on combat to "gain the objectives of any battle or campaign." Further, the definition of war can only be inferred to mean "crisis or conflict" based on the definition of IW in JP 1-02.

In November 2003 the US Army released its new and updated version of FM 100-6, Information Operations, now called FM 3-13. It defined information operations as

> The employment of the core capabilities of electronic warfare, computer network operations, psychological operations, military deception, and operations security, in concert with specified supporting and related capabilities, to affect or defend information and information systems, and to influence decision-making.[4]

In this case, the US Army is stating that it foresees five core capabilities, but retained the wording for "supporting and related capabilities." IO, the manual asserts, encompasses attacking adversary C2 and protecting friendly C2. The proper combination of the two produces IS at decisive points. More important, however, is the assertion in the manual that IO allows commanders to mass the effects of the information element of combat power. IO and automated information systems and communications allow for staff processes to be shortened, and decision cycles to be compressed. This increases operational tempo.[5]

Attaining IS remains the goal of IO, as this condition allows commanders to seize, retain, and exploit the initiative. This can only be accomplished, of course, if the core capabilities of the US are superior to those of the opposing side not only in the technological sense but also in the manner in which the data obtained is analyzed and used. Seeing the battlefield first is not enough. Commanders must be trained in how to take advantage of such situations not to mention how to analyze the information presented to them. As is often the case (witness subjects such as the operational art of

[4] FM 3-13, Information Operations: Doctrine, Tactics, Techniques, and Procedures, November 2003, p. 13.
[5] Ibid., pp. v, vi.

taking down a huge city, or post-conflict termination plans and measures) our commanders often are not taught how to use the information at their fingertips, or what information to request. There currently are no courses at military educational institutions addressing these concerns.

What is covered in depth in reading material is the purely business aspect of the subject of IO, and some of that material is misleading. For example, in the past three months Defense News has carried the following article titles: "C4ISR Tops R&D Spending Lists"; "Network-Centric Warfare Hot Topic at DSEi"; "Pentagon Eyes IO Support Plan" (don't be fooled here—the article is about IO as "attempts to influence the minds of adversaries," which doesn't square with our definitions); "One Network, Several Security Levels"; "UAVs Shifted Role in Iraq Operations"; and "Information-Sharing Program Improves U.S. Base Security." The attainment of IS may be short lived if analysis is not properly conducted. If not attained, it cannot support at times and places neither a commander's intent nor his concept of operations.[6] Interestingly, the new FM 3-13 did not define information war, indicating a renewed emphasis on IO alone. However Army Field Manual 3.0, noted above and also a relatively new publication, listed 11 "elements" of IW. Thus it is easy to see that even today, after some ten or so years, there is still much discussion about what IO is or is not in the US armed forces.

RUSSIA

IW and IO have been defined in several ways by Russian authors. Without an authoritative publication like a JP or an FM, it is nearly impossible to get an official definition of either term, however. The 1986 Soviet Encyclopedia defined an operation as "an aggregate of battles, engagements, strikes and maneuvers, coordinated and interlinked in objective, tasks, place and time, by various force organizations, conducted simultaneously and sequentially according to a common concept and plan, to accomplish missions in a theater of operations, a strategic or operational sector, or within a specified period of time; a form of military operation." War was defined in the military encyclopedia as "a sociopolitical phenomenon, continuation of politics by violent means... Armed struggle comprises the specific content of war."

In the 2003 book An Introduction to the Formal Theory of Information War, Russian IW expert S. P. Rastorguyev discussed the concept of IW. It is worth examining Rastorguyev's concepts because he was commissioned a few years earlier to write a book called Information War for the Security Council of the Russian Federation. He thus appears to be a very influential IW theorist.

Rastorguyev defined IW as "a battle between states involving the use of exclusively information weapons in the sphere of information models." The final objective of an information weapon's effect is the knowledge of a specific information system and the purposeful use of that knowledge to distort the model of the victim's world. He adds that there is no important difference between the terms IW, information struggle and information battle. Rastorguyev defined an information operation as "a

[6] Ibid.

sequence of actions to use an information weapon to achieve an assigned task." An information weapon, according to Rastorguyev, is

> A means directed at activating (or blocking) information system processes in which the subject using the weapons has an interest. An information weapon can be any technical, biological, or social means or system that is used for the purposeful production, processing, transmitting, presenting or blocking of data and or processes that work with the data.[7]

The use of an information weapon assumes that the following have been developed: (1) an analysis of the means and mechanisms for activating within an enemy system the self-destruction, self-control, and self-limitation programs installed in that system (2) development of a specific information weapon and (3) use of an information weapon against a given objective within the framework of the information operation under consideration. An information weapon must: be used on an objective with maximum speed as compared to another type of weapon; cause the necessary damage to the objective within the allotted time period; be sufficiently cheap and simple to produce, as compared to another type of weapon of the same action class; and be capable of mass production.[8]

Rastorguyev added that information weapons are the most significant weapons of the modern era for four reasons: they offer a much cheaper production of data due to the emergence of information technologies; they provide automated means for obtaining knowledge from data that has been created; they provide a great reduction in the cost and time for delivering information to practically any point on the planet due to the development of telecommunication assets; and they offer a great increase in the effectiveness of the impact of information. The latter is due to the emergence of sophisticated theories in the areas of programming for computers and neuro-linguistic programming for social systems, to include many methods and means for exerting an information-psychological effect.[9] Thus Rastorguyev discusses both the information-technical and information-psychological aspects of IO.

Breaking the subject of information war and information operations into two components, information-technical and information psychological, and not into elements as the US armed forces does, started several years ago. For example, threats in both Russia's April 2000 military doctrine, and in a year 2000 issue of the Russian defense complex journal Information Security, were listed as information-technical and information-psychological aspects of IO. In the latter journal, the information-technical confrontation was divided into technical intelligence devices, means and measures for protecting information, super high-frequency weapons, ultrasonic weapons, radio-electronic countermeasures, electromagnetic impulse weapons, and special software and hardware. Information-psychological aspects included the mass media, non-lethal weapons, psychotronic tools, and special pharmaceuticals.

---

[7] S. P. Rastorguyev, An Introduction to the Formal Theory of Information Warfare, Moscow 2003, p. 6, 7.
[8] Ibid., pp. 7, 8.
[9] Ibid., p 9.

An October 2003 brochure "Urgent Tasks of the Development of the Russian Federation Armed Forces" also stated that information operations (IO) were a threat to the Russian Federation and its allies. IO was said to contain two aspects, information-technical and information-psychological operations. In the last issue of the military's authoritative journal Military Thought in 2003, author S. A. Bogdanov stated that the goals of contemporary armed struggle were obtainable by military, economic, and "information-technical and information-psychological" measures.

Perhaps the most recent article reflecting this breakdown into two major components was that of Captain First Rank (Reserve) R. Bikkenin. Writing in Morskoy Sbornik (Naval Journal) in October 2003, Bikkenin first pointed out that many players conduct information conflict at different levels. At the strategic level, various ministries and departments are involved, and in wartime two or more fronts or fleets may perform strategic missions. At the operational level, fronts, fleets, army, flotilla, and corps are involved. At the tactical level of information conflict, formations, units, single ships and army subunits are involved.[10] Bikkenin noted that information conflict has become a kind of military art, wherein offensive and defensive actions are used to influence the intellect of civilians and servicemen. Information weapons are involved (a term which the US military and State Department, as noted above, refuse to define), and are defined by Bikkenin as:

> a means of eliminating, distorting or stealing information for the purpose of obtaining necessary data after penetrating the security system; blocking of access to information by its legitimate users; and in the final account, disorganization of all means of society's life support, including the enemy military infrastructure.[11]

Bikkenin thus uses disorganization instead of information superiority as part of his definition.

He then lists the fundamental components of information conflict as information-technical and information-psychological, just as did Russia's military doctrine and the brochure on "Urgent Tasks." However, Bikkenin somewhat altered the subcomponents of these two aspects from past definitions. Under the former he listed the main targets of attack and defense as electronic assets, above all communications and telecommunications systems, and the Internet. Other aspects of the information-technical component of information conflict included disinformation, maskirovka, intelligence, the science of cryptology, and steganography. Bikkenin pointed out that several new cryptographic algorithms have become widespread, particularly the RSA-algorithm, and the El Gamal algorithm.[12]

---

[10] R. Bikkenin, "Information Conflict in the Military Sphere: Basic Elements and Concepts," Morskoy Sbornik, No 10, 2003, pp 38-40 as translated and downloaded from the FBIS web site on 6 February 2004.
[11] Ibid.
[12] Ibid.

In the case of the latter aspect, information-psychological, Bikkenin focused attention on the civilian population and servicemen. This IO aspect includes the use of the mass media (press, radio, and television), leaflets, religious propaganda, and computer networks, especially the Internet, according to Bikkenin. Thus if Bikkenin's views are widely held, the Internet is now considered both an information-technical and information-psychological aspect of IW.[13] Of greatest surprise, however, was the introduction by Bikkenin of the religious propaganda aspect of IW. This addition is indicative of the influence that the Chechen conflict has had on Russia's society and armed forces. Russia's elite is clearly concerned about the impact of religious extremism on local conflicts, especially the effect of Wahhabism to coerce local residents to fight for their cause.

With regard to the information-technical aspect of IW, a 1999 article by then Russian Defense Minister Igor Sergeyev highlighted the influence of the information age on Russia's military-technical policy. He listed the following as priorities for the Russian military in the coming years:

- guided and electromagnetic energy weapons
- cyberweapons
- stealth unmanned combat platforms
- and all weather reconnaissance and accurate long-range weapons[14]

The Russian military journal Military Parade offers the analyst an updated perspective on how the military has focused on implementing Sergeyev's plan. For example, Issue One of 2003 had articles on drones and UAVs (a series begun in Issue Four of 2002), communication devices, radars with electronic beam control, laser information technologies for military and dual-use applications, modernizing tanks and infantry fighting vehicles with information technologies (thereby improving their combat potential), high-precision cruise missiles, digital mapping technologies, automatic control systems, and smart guidance systems. The issue also had an article on "High-Precision Weapon Systems Development Trends and their Role in Modern Armed Conflicts." All this in just one issue!

Issue Five of 2003 also contained several articles of interest from an information-technical viewpoint, and several stood out. These articles were about information technologies as tools of troop and weapon control, military satellite communications equipment, helmet-mounted vision systems, the Akveduk communications system, and high-precision anti-ship missiles belonging to the Navy.

The ongoing conflict in Chechnya has offered examples of both the information-psychological and the information-technical aspects of information conflict. Russian author V. V. Panchenkov explained the information-psychological defeat of the Russian

[13] Ibid.
[14] Igor Sergeyev, "The Main Factors which Determine Russia's Military-Technical Policy on the Eve of the 21st Century," Krasnaya Zvezda, 9 December 1999, as translated and downloaded from the FBIS web site on 6 February 2004.

armed forces in the first (1994-1996) Chechen conflict; and measures to correct the situation in the second (1999-present) conflict. In the first conflict, the Russian media were not under state control and were often financed by Chechens, and Russia's Defense Ministry did not provide journalists with official information that the Russian public needed. As General of the Army Makhmut Gareyev noted, no army can operate successfully if …it is being morally beaten down by its own compatriots and the media."[15] Information-psychological influence on the illegal armed formations was ineffective, Panchenkov added.

For the second conflict, information centers were established in two republics that are neighbors to Chechnya, the republics of Dagestan and North Ossetia. Journalists were supplies with videos and briefing material, and escorted to specific locations by Russia's official representatives. In this way, the information centers were able to better control information produced about the conflict.[16]

Panchenkov also noted the use of new measures to help establish the information-technical aspect of IW. At the start of the second conflict in Chechnya, he noted that

> During 1999 more than 150 control points and radio-electronic facilities operating in the interests of the illegal armed formations were found. By the end of September 77 of them had been destroyed by fire engagement, including 22 of the 38 radio broadcasting stations. The power was cut off from 18 radio-electronic facilities. Some 90% of the base stations (to include retransmitters) for radio relay, cellular, and other types of communications were either seized or put out of commission.[17]

CHINA

When examining Chinese IW materials for the past decade, it becomes clear how serious a role IW is playing in the transformation of the People's Liberation Army (PLA) from a mechanized to an informationized force. For example, on 6 August 2003 Defense Minister Cao Gangchuan told a meeting of municipal governments, the PLA General Staff, and the Beijing Military Region that the defense buildup was aimed at gaining victory in IW. This IW directed effort also has the complete support of the Central Military Commission (CMC) and its Chairman, Jiang Zemin, formerly China's President. Jiang's son Mianheng, by the way, was reported to be the nominee who would serve as an advisor for the 38th Group Army's digitization program. He will be responsible for digitizing weapons and command systems of the unit.

China adheres to an IW theory closer in detail to that of the United States. China has six core "forms" or subdivisions of IW, and not just two as Russia nor 11 elements as US FM 3.0 advertises. China's IW and IO definitions have also changed through the

[15] V. V. Panchenkov, "Lessons from the Information War in the North Caucasus," Vooruzhenie, Politika, Konversiia, No 4 2002, downloaded from the FBIS web site on 5 February 2004.
[16] Ibid.
[17] Ibid.

years. One Chinese IW expert noted a few years ago that "IW occurs all the time, in peace and war. It is part of the ideological struggle. An IO only occurs in wartime."[18] In 2002, the PLA's IW General Staff proponent, General Dai Qingmin, listed six forms of IW in the authoritative Chinese journal China Military Thought: operational security, deception, computer network attack, electronic warfare, intelligence, and physical destruction. Two of these forms stand out: electronic warfare and computer network warfare. China's concept of "integrated network-electronic warfare (INEW)", similar in content to the US concept of network-centric warfare, refers to a series of combat operation actions with integrated use of EW and CNW measures on the informationized battlefield designed to disrupt the normal operation of the enemy's battlefield network information systems, and protect one's own. The objective of INEW is to seize battlefield information superiority, according to Dai.[19]

Dai had earlier defined information operations as "a series of operations with an information environment as the basic battlefield condition, with military information and an information system as the direct operational target, and with electronic warfare and a computer network war as the principal forms."[20] In the same article he contended that contention for "information control" might become a focus of future war. Belligerents in a future war will contend for information superiority, but Dai maintained that information control was needed to create conditions for maintaining the initiative and winning final victory.[21]

Dai listed three characteristics of information supremacy: it is an integrated combat posture that can greatly affect the war as a whole; it allows freedom of movement in the information dimension, is conducted in three areas (electromagnetic space, computer network space, decision-makers cognition and belief system) and two levels (attack against information systems, attack against human's cognition and belief system); and it influences events in the information dimension so as to affect events in the physical dimension.[22]

A review of China's open source literature reveals that China intends to use IW in one of three ways, depending on the geopolitical situation confronting its leaders: as a tool of war, as a way to achieve victory without war, or as a means to enhance stability through the promotion of new military theories. These different methods will present a continual guessing game to the Western mind as it tries to ascertain the actual IW strength of the PLA: is the PLA "appearing weak when strong" or is it trying to "appear strong when weak?"

---

[18] Author's discussion with Chinese IW expert, January 2001.
[19] Dai Qingmin, "On Integrating Network Warfare and Electronic Warfare," China Military Science, Feb 2002, pp 112-117 as translated and downloaded from the FBIS web site.
[20] Dai Qingmin, "Innovating and Developing Views on Information Operations," China Military Science, August 2000, pp 72-77 as translated and downloaded from the FBIS web site.
[21] Ibid.
[22] Dai Qingmin, "On Seizing Information Supremacy," China Military Science, April 2003, pp 9-17, as translated and downloaded from the FBIS web site.

Several specific issues stand out in the open source analysis of IW, IO, and IS theory that probably will carry over into the next ten years of PLA development. These items are:

- Joint offensive IW has become a closely studied subject by the Chinese leadership, and is considered an important aspect for the attainment of victory in the information age.
- Psychological warfare will have an elevated role in future war.
- In nearly every training exercise a "blue IW based army" has superiority in technology which forces a "red IW deficient army" to rely on backup systems or the employment of counter tactics, which might indicate that the PLA expects to absorb a first IW strike.

Joint, offensive IW.

It is evident that reserve, militia, PLA, and civilian forces will conduct joint operations in the future and join hands against any intervening IW force. This integration is already underway, as signified by the proposed establishment of a cyber security force. Qu Yanwen, a security specialist, has proposed that a cyber security force (CSF) be composed of members of the PLA, the Ministry of State Security and Public Security, and technical specialists. Currently Chinese political, economic and military security is in danger due to the nascent stage of development of China's networks, according to some reports. Weaknesses exist in financial security; cyber attacks against information networks of key organizations; computer-based fund raising operations and scams; information control affecting the stability of the public order; and military information security.[23] Within the PLA, the Shijiazhuang Army Command College, the Navy Command Academy, the Air Force Command Academy, and the Second Artillery Corps Command Academy met in July to work out an overall joint teaching program for the three armed forces. They are trying to share information resources, and exchange experiences via the Internet, among other issues.[24]

To demonstrate the emphasis on offensive IW, one need look no further than the militia. Guangzhou City's militia has, for the past few years, focused on the requirements of the information battlefield. It was decided to organize a battalion headquarters (set up as a provincial telecommunications company, and two companies: a computer network warfare company and an electronic warfare company). The computer network company has two platoons, a network defense platoon and a network attack platoon, and the electronic warfare company has two platoons, one devoted to reconnaissance and the other to deception. However, there is no training outline to follow, since this unit is a newly emerging force. A draft "Training Plan for Militia Information Technology Elements" was developed from discussions with staffs of the Guangzhou Military Region.

---

[23] Takungpao News, http:www.takungpao.com/news/2003-11-30/MW-203198.htm, Naval News http:..jczs.sina.com.cn/2003-11-30/167226.thml, 30 November 2003.
[24] http:www.pladaily.com.cn/gb/pladaily/2003/07/31/20030731001027, from FBIS document CPP 20030811000030.

This year's training research included the topics of protecting one's own network security, searching for enemy network stations, and attacking enemy networks.[25]

Thus, with this level of attention devoted to the militia, it is no wonder that the PLA has developed its own IW brigades that conduct offensive and defensive operations against one another. In March, 2003 military representatives attending the National People's Congress (NPC) noted that IW units would soon be activated. These units had "already developed electronic jamming/bombardment weapons" capable of paralyzing all enemy electronic systems including the Internet and military command systems, and more advanced than the US. Several trial units were already established, and a large portion of the budget would go to developing IW units.[26] On 4 November Jiang Zemin, asked the armed forces to build IW units to win in IW. New types of soldiers with new military theories are needed to do this, he added.[27]

Increased emphasis on PSYWAR.

The theory of psychological warfare has tremendous significance and value to China. Chinese theorists are attempting to develop an updated ideology and strategy of psychological warfare — one that will focus on intimidation and on exploiting the differences between Eastern and Western mentalities. The PLA intends to establish a command structure for psychological warfare, as well as create special units that will attempt to overcome Chinese inferiority in high-tech weapons.[28] More important, Chinese theorists appear to believe that because modern psychological warfare can help ensure stability and shape national-security thinking, the concept is more applicable in peace than in war.[29]

In offering a recommendation for future psychological-warfare forces in China, Major General Xu asks Chinese leaders to:

- Develop a psychological-warfare system that integrates specialized and non-specialized personnel, and that emphasizes China's special characteristics.
- Establish a psychological-warfare coordination agency at the national level to provide guidance and coordination for national psychological-warfare actions.
- Establish a psychological-warfare command agency, under the unified leadership of the Central Military Commission and the party committee.
- Establish several types of psychological-warfare scientific research agencies in order to guide both national and military work.
- Establish a specialized psychological-warfare corps that would form a consolidated and effective psychological attack force.
- Develop a modernized basis for psychological-warfare material and technical equipment.

---

[25] Ye Youcai, Zhou Wenrui, "Building a High-quality Militia Information Technology Element," Guofang, 15 September 2003 p. 45 as translated and downloaded from the FBIS web site on 15 September 2003.
[26] Mingpao News, 12 March 2003.
[27] The Sun Daily News <http://the-sun.com.hk/channels/news/20031105/20031105012934.html>, 5 November 2003.
[28] Ibid.
[29] Xu Hezhen, "Focus on Psychological War."

• Form a people's psychological-warfare mentality by developing psychological-warfare education for the masses and for all commanders in the military.[30]

"Blue" versus "Red"

There were numerous training exercises in which a "blue IW based army" force confronted a "red IW deficient army." In the ensuing "battle" the red force had to rely on backup systems or the employment of counter tactics. In nearly every instance these counters included counter reconnaissance and counter interference. The impression left with the reader is that the PLA expects to absorb a first IW strike like a fighter on the ropes, and then counter after the opponent has taken his best shot. Perhaps for this reason control is deemed so important, for pure information superiority is not obtainable at the outset of a conflict from a PLA perspective. It will be attainable only after forcing the opposing side to expend some of its resources.

In conclusion, Chinese military theorists apparently believe they have found a willing, relatively cheap, and malleable ally in IW, an ally that can enable China to catch up with the West in both strategic military and international status. Success in these areas could lead China to play an important strategic deterrent role (or potential troublemaker) in the Asia-Pacific region in the future and to gradually emerge into an economic competitor worthy of close scrutiny. China sees a strategic opportunity to leap frog the age of mechanization and move directly into the age of information, a move full of positive aspects for the Chinese military.

CONCLUSIONS

Electrons and information technologies are the supplemental formations of 21st century armed forces that support the traditional forces of the US, Russia, and China. Electrons require that the focus or concentration of effort be on operational effectiveness, manipulation, and speed as well as the principle of concentrating military strength. The West should examine Russian and Chinese approaches for new areas of emphasis. Such areas include new criteria for figuring correlation of forces, the new emphasis on cognitive factors, especially psychological, and the offsets to IS (disorganization and control), among other issues. While it was easy to measure the intent of steel in the form of a tank it will be much more difficult to measure the intent of an electron, and to conduct the consequence management assessments for electronic activities.

Hopefully, all countries engaged in the development of IW forces will learn to talk and negotiate with one another, perhaps through the establishment of an IW hotline between governments. Since it will be more difficult to know who or what is attacking a nation in the age of information, communications will become even more important and vital to our national security than they were in the past. Everyone will know immediately if a nuclear device is detonated but not everyone will know as quickly if an electronic attack is launched on, say, a nuclear power station. The former will bring death and destruction while the latter may only produce darkness. In the information age it is

[30] Ibid.

possible to mask attacks and make them appear to come from someplace other than the attacks origination. The hotline will enable clarifications of attack status, and allow nations to correspond and sort out what has happened, thereby reducing misunderstanding over a very serious issue. In fact, such a hotline should be collocated with the current nuclear hotline.

Thus, for the U.S. military, a force focused on information superiority, dominant maneuver, digitalization, and information assurance, a study of Russian and Chinese IW methods would be not only advisable but also required. Such a study might uncover inherent IW weaknesses in the U.S. system when analyzed through the thought process of another ideological prism or framework. The absolute worse mistake that America can make is to use its own process for uncovering vulnerabilities exclusively, since there are other problem-solving schemes (the dialectic) available. It is worth the time of the U.S. analytical community to analyze IW strategies and tactics from all points of view, not just the empirical U.S. approach. China and Russia have been able to learn from the mistakes of others, and may soon become IW forces with which to reckon as they bypass major mechanized age stumbling blocks. IW has allowed both countries to skip over some technological developments, to use discoveries in the West to save time and money or to, as the Chinese say, "borrow a ladder to climb the tree."[31] As the Chinese have said, losers in IW will not just be those with backward technology. They will also be those who lack command thinking and the ability to apply strategies.

[31] Wang Jianghuai and Lin Dong, "Viewing Our Army's Quality Building from the Perspective of What Information Warfare Demands," Beijing Jiefangjun Bao, 3 March 1998, p. 6 as translated and downloaded from the FBIS web site on 16 March 1998.