Human Network Attacks

by Mr. Timothy L. Thomas
Foreign Military Studies Office, Fort Leavenworth, KS.

This article appeared in

Military Review

September-October 1999

US information warfare (IW) theory consists of some very basic premises: attaining information superiority or dominance, maintaining a quick tempo and decision cycles, integrating efforts whenever possible and working constantly to exploit the information environment. This theory is based on six capabilities: operations security, psychological operations, deception, destruction, electronic warfare and computer network attack.

One of the overriding concerns of the US military is the security of these IW capabilities, especially computer networks. The Pentagon has poured millions of dollars into constructing an infrastructure-protection package aimed at limiting hacker access to manipulate or corrupt our data storage resources in peacetime or wartime. One specific data processor, however, has received far less attention in US thinking. It is the security of the data processor known as the mind, which unfortunately has no innate firewall to protect it from either deceptive or electromagnetic processes. As a result, the mind of the soldier on the battlefield is potentially the most exploitable and unprotected IW capability our military possesses. Soldiers vulnerability to human network attacks (HNA) should be an area of close attention for scientists in the early years of the new millennium.[1]

China and Russia, in addition to studying hardware technology, data processing equipment, computer networks and "system of systems" developments, have focused considerable attention on several nontraditional targets of the information weapon, to include the mind.[2] This attention differs from the US approach for both practical and cultural reasons. Neither China nor Russia have the financial capability or the infrastructure to compete with Western IW technological advancements. However, both countries have a wealth of outstanding mathematicians, philosophers and scientists that can offset this shortcoming through the development of nontraditional approaches, as well as historical and cultural proclivities that draw their focus to this area.

The US Armed Forces, a producer of HNA variants, as demonstrated by psychological operations or nonlethal weapon options, could profit by studying the approaches developed in China and Russia. Examining other approaches to HNA activities would assist in uncovering HNA techniques and vulnerabilities. This article examines China's psychological warfare and knowledge concepts (including the impact of the information age on China's strategic culture) and "new concept" weapons (variants of nonlethal weapons); and Russia's development of information-psychological operations, reflexive control or "intellectual IW" stratagems and human behavior control mechanisms. The latter issue makes Russian thinking on HNA unique. It is clear that to both countries, "gray matter" does matter.

Chinese Nontraditional Practices

> "In military actions, attacking minds_that is the primary mission; attacking fortifications, that is a secondary mission. Psychological war is the main thing. Combat is secondary."[3]
>
> —Third Century Chinese Military Theoretician

China's entry into the information age has proceeded with caution, anticipation and good luck. Caution was used due to the sudden ability of its citizens to communicate with people around the globe, a new phenomenon in Chinese culture, where outside access and information is tightly controlled. Anticipation refers to China's opportunity to quickly catch up with other world powers through the information medium. China has many outstanding mathematicians to speed this process, especially in the development of software. Good luck refers to acquiring Hong Kong at a time when the information revolution was reaching its peak. For purposes of launching a Chinese information-based economy, access to Hong Kong's telecommunications and financial markets is akin to winning the lottery. The market will insert new life into the six or so semiconductor fabrication lines already operating in China. In addition, China's ideological and economic changes have proceeded more slowly than Russia's, ensuring some stability through the 1990s. Russia's population has paid the price for moving too quickly.

A widespread Chinese view is that information technology (IT) has given rise to a new, worldwide military revolution as well. IT is the "core and foundation of this military revolution, because information and knowledge have changed the previous practice of measuring military strength by simply counting the number of armored divisions, air force wings and aircraft carrier battle groups. Nowadays, one must also consider invisible forces, such as computing capabilities, communications capacity and system reliability."[4] A key component of this revolution is information warfare.

In 1995, Dr. Shen Weiguang, known in China as the father of its IW theory, wrote an IW introductory research piece for the Chinese military newspaper *Jiefangjun Bao*. Shen defined information warfare as command and control warfare or *decision control warfare*, where information is the main weapon designed to attack the enemy's cognitive and information systems and influence, contain or change the decisions of enemy policy makers and their consequent hostile actions. The main target of IW is the enemy's cognitive and trust systems, and the goal is to exert control over his actions. The Chinese sometimes refer to this idea as "guidance control." Here the term *cognitive system* refers mainly to information and computer decision-making systems. This thinking is similar, Shen notes, to "electronic beheading" at the beginning of an IW operation.[5]

Four years later, in an article describing the use of NATO IW during the conflict in Kosovo, Wang Baocun described how NATO worked first to behead the command systems of the Yugoslav armed forces. Take away the mind and the body will follow. Wang also noted, however, that the Yugoslav armed forces—the inferior—successfully thwarted NATO attacks—the superior—through the skillful use of three defensive concepts. First, they concealed personnel and armaments to preserve strength (hiding planes in caves or by ring roads; concealed tanks in forests, beside large buildings, or on mountainsides; dispersed the army into each village to mingle with the Albanians; and moved command organs underground). Second, the Yugoslav armed forces successfully used their technical means to avoid detection by not switching on air defense radars, or switching them on infrequently; obtaining the coordinates and operational orbits of reconnaissance satellites; switching off engines, putting equipment close to other heat sources or putting fake heat sources in mock-up tanks; and taking advantage of weak points in electronic surveillance equipment (for example, some systems do not work if a target is stationary). Finally, the Internet was used to communicate the opinions of ordinary citizens to the outside world and to hack or overload NATO E-mail sites.[6] Asymmetric options offset information superiority.

The Chinese also dissected the success of the superior coalition forces against the inferior Iraqi forces in the Gulf War. They cited Iraq's economic dependence, inflexible strategies and passive defensive tactics as adding to its inferiority. This led, according to one People's Liberation Army (PLA) officer, to the erroneous conclusion that it is impossible for a weak force to defeat a strong force in a high-technology war. It *is* possible for a weak force to win against high-tech force in war, but this requires bringing the overall function of its operational system into full play, to persevere in defeating the superior with the inferior in crucial battles and, through the integration of the above two aspects, turn the inferior into the superior and finally defeat the enemy.[7]

Information war conducted between China and Taiwan is increasing tension in the area. On 18 August 1999, the *London Times* reported that Taiwanese computer experts were repairing damage from a Chinese hacker attack on the National Assembly, where Chinese flags were planted and a message in Chinese and English noted that "Only one China exists and only one is needed." Taiwanese hackers have targeted China's Securities Regulation Commission and the Science and Technology Bureau, among other targets. At one provincial tax bureau the note that "China should stop playing with fire; we will declare independence should you dare to attack us" was attached to a site as part of a raid. Such declarations indicate that the information age can allow tensions to quickly escalate by direct exchanges of strategic importance that were impossible to make on such a wide scale in the past.[8]

To the Chinese, technology per se is relevant but not sufficient in the long run, especially if viewed from the current inadequate Chinese position regarding IT. One must also create new military theories to complement technological advances and overcome the technological superiority of other nations. Chinese history is rich in the theory of military art, and its analysts can draw from historical examples and stratagems.

Strategic Culture and the Information Age

The world's military theoreticians are intimately familiar with the wisdom and insights contained in the works and stratagems of China's military philosophers. Now, these same stratagems are being reexamined by Chinese theorists for their relevancy to the information age.

The ancient Chinese strategic concept of "not fighting and subduing the enemy" has received particular attention within the context of information-age technologies in China and the West. This concept has found especially fertile ground in political and strategic warfare circles. Even the Chinese game of Wei-chi ("Go" according to many American translations), requiring strategic thinking and foresight (similar to chess in that respect), involves an initial strategy of "not fighting and subduing the enemy."[9] This concept most likely affects modern Chinese political strategists in Beijing as well, prompting moves to control islands in the Spratleys and the takeover of shipping companies in the post-US controlled Panama Canal region in an effort to control flow in and out of the canal. Using information to influence (speed up or impede) financial transactions involved in the Canal negotiations (financial information war), to intercept counterpart negotiating strategies (the electronic warfare aspect) or to deceive a negotiating partner are but a few examples. The latter example is particularly important, since manipulation of human perceptions is an ancient Chinese art and strategic tradition. One report on computer network attacks, for example, noted that a situation could be "shaped" to China's advantage by psychological means, then deception and, finally, dynamic means.

Recent military mobilization moves by China against Taiwan might just be a psychological and deceptive method to uncover an alliance strategy in the region through IW assets that monitor and analyze Taiwanese and its allies' information operations (as well as Western responses to these moves). The game of cat and mouse continues, only now the animals are studied as much for their virtual characteristics as for their real ones.

Upon closer analysis, the "not fighting" theory certainly is not a singular representation of Chinese strategy in the information age but one among many that warrants closer analysis. Another strategy, "absolute flexibility," received much less attention until recently when the book *Unrestricted Warfare* caused a furor in the West. It offers just the opposite view from "not fighting" and the strategic analogy is closer to the concept of "absolute flexibility" or the notion of *quan bian*. This strategy requires one to "respond flexibly . . . and create conditions for victory."[10] The nonmilitary means the authors advance include such IW related concepts as the use of hackers, the mass media and financial information terrorism. The key is the unique alignment and integration of psychological, diplomatic, resource and other warfare techniques, all of which have information aspects. One of the authors, Colonel Qiao Liang, noted that "unrestricted warfare is in the final analysis a way for a weak and small country to cope with `evil,'" as in another old stratagem, "defeating the superior with the inferior." This might involve breaking rules and exploiting loopholes, according to Qiao, and favors nonmilitary means such as soft strikes, magnetic weapons (computer logic bombs), media weapons and electromagnetic energy weapons that do not cause hard destruction.[11] Thus, the "new concept" weapons listed below should be viewed in the light of their potential use as an HNA agent.

Unrestricted Warfare indicates that "not fighting" is not necessarily the ideal to follow in the information age. "Not fighting" gained notoriety in the West primarily because it was the principal slogan used by IW proponents to promote their theories. "Not fighting" was the basis for the clean IW rules that the West hoped to play by in the information age_no casualties, just a victory from a stand-off position. Perhaps this is why the publication of *Unrestricted War* caused such an uproar. It indicated that conflict might actually be preferred in some cases in the information age, depending on priorities set by Chinese leaders. As Qiao noted, "the stronger side is never the first to break the rules and use irregular methods."

IW's Relation to Psychological Operations

The PLA has not published a great deal on the subject of psychological operations. What it has published does not seem to be strikingly different from Western theory except that there is more emphasis on peacetime psychological operations. In fact, there is even some agreement among Chinese and Russian psychologists about the growing importance of both countering and conducting peacetime information-psychological defensive and offensive operations. These operations set the stage for wartime IW and by Chinese estimates can sap the morale of the soldier by a factor of several times greater than in previous wars due to the power and manipulative ability of IT. Failure to confront this information-psychological invasion is more serious than military backwardness in other areas, according to some Chinese analysts.[12] In the Gulf War, only after reducing combat morale among some 40 to 60 percent of the Iraqi forces did the multinational forces decide to attack, in the Chinese view.

Technological developments have made it possible to subject all people, from ordinary citizens to heads of state, to a complex information offensive. Simulated and reproduced voices, fabricated provocative speeches delivered by virtual heads of state, and projected images of actual life situations can affect troops psychologically.[13] In the area of psychological warfare, author Liu Ping stressed that China recognizes special information media, such as language, texts, images and sound, as future enemy weapons capable of exerting a "multilevel operational effect" instead of simply a political or economic one. The target remains the enemy's decision-making processes, both human (the mind's soft data processor) and material (hardware data processing). The main task is to overwhelm opposing forces through the use of terror tactics, thereby upsetting their psychological stability. Psychological war usually starts in peacetime and, if war erupts, will run throughout its course.[14]

Liu noted that psychological warfare is now planned at the highest levels of the armed forces or state leadership. The equipment of psychological warfare supports this idea, since "facts" can now be fabricated in a much more realistic form (real time on radio or TV) using high-tech voice and image recording and editing equipment. Perhaps even more important, the means of psychological warfare are now more diversified, and its striking force has increased.

Today, simulation, stealth and various types of camouflage technologies allow for the "mixing of the spurious with the genuine" and can cause errors in the enemy's decision-making. More important is acoustic technology because it creates deafening noises, such as explosions, whizzing sounds, rumblings and heartrending screams, to upset psychological stability. Liu notes that other countries' psychological warfare offensives will attempt to penetrate the mind of PLA soldiers or key decision makers to throw them into a psychological maze or cause psychological disorders or panic.[15] This psychological warfare organization bears closer scrutiny as it develops. As a result, the following was recommended to counter enemy IW techniques:

"It is necessary to set up an organization for psychological warfare; form a theoretical system for modern psychological warfare with the characteristics of our army; promulgate a training program for psychological warfare and regulations for psychological warfare operations and standardize the training and combat of the whole army; set up specialized psychological warfare units; and strive to raise our army's capabilities in psychological warfare."[16]

Knowledge Warfare

One Chinese analyst has noted that the human must be able to comprehend what happens when two systems collide, such as two command and control systems or an electronic warfare (EW) system and a counter EW system. The human must be able not only to control or manipulate such interactions and their consequences but to comprehend what has happened and why.[17] If the human can master this interaction, then he employs "knowledge warfare," which the Chinese believe rivals information warfare in importance. While the latter is data, the former is how to use the data to one's advantage. Even though knowledge is invisible, it can be transformed into combat power and affect combat effectiveness. This concept will not be fully realized until after the first full-scale confrontation between highly technical combatants. Then, for the side that has not taken knowledge warfare into consideration, it will be too late. Simulations cannot provide true understanding of such confrontations.

Analyst Wu Jianguo, speaking at a Chinese conference devoted to studying knowledge warfare, stated that "knowledge confrontations are the focus of military confrontations and the hallmark of an army's strength is its *intellectual* combat capability." Soldiers must depend on their ability to apply knowledge and innovate. The information engagement will not be between the soldier and the battlefield as some expect but rather it will test the soldier's mastery over the network and his ability to prevent the enemy from paralyzing it.[18] The knowledge confrontation system will have the most decisive significance in the era of smart warfare where, according to Wu, it will be more important than the firepower, mechanical, electronic and even information confrontations. It is the subsystem that requires top priority in development and should become the core mission of military education, training and war preparation in China. Wu recommends the establishment of a coordinating department for the entire military and national security systems to synergize all forms of knowledge-based confrontations.[19] As one Chinese analyst noted about knowledge:

"New information technologies are permeating and functioning in all spheres of society in an all-pervasive way, making information and knowledge important resources and wealth. If we say knowledge equals wealth in economic life, then in the military field it equals victory. With the advent of an era of intellectual militaries, changes in the military field will lead to dazzling military changes as if "thousands upon thousands of pear trees blossomed overnight in the wake of a spring wind."[20]

There is also a desire in the Chinese military to manipulate information, a tendency much stronger in the Russian nontraditional approach. Chinese analyst Wang Zhi, for example, noted that warfare is changing from "organizing around the weapon system" to "organizing around information." Processes are under development to prevent an enemy from using information correctly or to paralyze him, leading to mistakes in recognizing or responding to a situation or in decision making.[21]

New Concept Weapons

Chinese writings have not emphasized psychotronic weapons or suggestive influences, as have the Russians. Rather, they have focused on the impact of what they term "new-concept weapons," such as infrasound weapons, lasers, microwave and particle-beam weapons and incoherent light sources.[22] Speaking to foreign participants, analyst Wang Zhi added ultraviolet radiation, anti-environment (earthquakes, for example) and biological weapons to this list. These innovations will allow decision makers to select and adjust the intensity of war according to their needs.[23] One needs simply to "turn up the volume" if a technique is not working.

Infrasound weapons use sound waves with frequencies lower than 20 Hz to cause cardiac, respiratory, digestive and central nervous system malfunctions, disorientation and emotional disorders. The journal *People's Military Surgeon* noted that such a weapon has already been developed and tested, and that infrasound waves generated by the device are adjustable to cause controllable amounts of disorientation, nausea, vomiting and incontinence.[24] The journal also describes the use of microwave weapons to cause electronic interference, lasers to disable equipment and incoherent light sources and super-high frequency weapons, with the latter capable of interfering with the functioning of the human nervous system and capable of causing unbearable noise and whistling sounds.[25] The *People's Military Surgeon* article ended on the ominous note:

"Weapons generating interference and causing blindness have become practical to use. Foreign armed forces already have corresponding prevention and protection measures, standard, and diagnostic techniques, and have conducted further research . . . [and] microwave electronic interference equipment is already widely utilized. Therefore, medical protection against microwaves are already being developed."[26]

The Chinese military apparently believes these devices will be used in future war since its doctors are investigating treatment for injuries caused by special types of high-tech or new-concept weapons.[27]

Russian Nontraditional Practices

> "The image is fragmented and introduced in pieces into `normal' frames by an unnoticeable element and the subconscious mind instantly `reads' the pieces as the encoded image."[28]

—Russian Medical Journal, September 1998

Russia entered the 1990s in an entirely different context than the Chinese. The country has been fragmented, with the former republics receiving their independence from the center. The concepts of Perestroika and Glasnost' have upset the ideological prism through which Russians viewed the world. Some believe this has led to a spiritual vacuum, while others think this has led to a disregard for state interests, to money-laundering schemes and the growth of criminal structures, among other phenomena. Russia's economic troubles have been well documented. At the same time, the country has embraced the information revolution. Now it is much easier to contact ordinary citizens through the Internet than in China. Russia is also faster at adapting to information innovations and applying them to industry. The problem remains finding the money to do so.

However, like China, Russia has felt that it is the object of information-psychological aggression from abroad and has attempted to establish some legal and doctrinal criteria for thwarting such attacks. The country has a draft information security doctrine, a Duma subcommittee devoted to information security issues and a security service that increasingly is patrolling and regulating cyberspace. Russian authorities consider citizens extremely vulnerable to outside influences and information weapons. Some blame the West for using these means to accelerate the Warsaw Pact's disintegration.

Russian Major S.V. Markov, writing in the journal *Bezapasnost'* (Security), defined an information weapon as "a specially selected piece of information capable of causing changes in the information processes of information systems (physical, biological, social) according to the intent of the entity using the weapon."[29]

Thus, an information weapon could be a virus, incorrect commands or disinformation, among other things. The information weapon can be used to destroy, distort or steal data files; to mine or obtain the desired information from the files after penetrating defense systems/firewalls; to limit or prevent access to systems and files by authorized users; to introduce disorganization or disorder into the operation of technical equipment; and to completely disable telecommunication networks, computer systems and all the advanced technology that supports society and the operation of the state.[30] Such information weapons can be used at the strategic, operational and tactical levels.

Russian IW modelers try to foresee the application and utility of information weapons. They study an information model of the psyche of a person and then attempt to simulate the interaction between people, social groups and other factors. The formation of methods to ensure moral-psychological stability is important to Russian modelers. They want to counter the influence of information weapons that aim to suppress the will to resist, "zombify" the psyche through manipulation and reconfigured thinking, reprogram human behavior and demoralize and psychologically degrade people.[31]

IW and Information-Psychological Operations

With the elevation of the information-psychological factor to such prominence in discussions of information weapons, the psychological factor has become a prime consideration in many current IW definitions. The various national security agencies in Russia look at the concept from their own contextual situation. The definition of the Foreign Intelligence Service, for example, differs from that of the Federal Agency for Government Communications and Information. This article uses a military definition. An officer from Russia's General Staff Academy defined information war as a technical/psychological activity:

"Information warfare is a way of *resolving a conflict* between opposing sides. The goal is for one side to gain and hold an information advantage over the other. This is achieved by exerting a specific information/psychological and information/technical influence on a *nation's decision-making system, on the nation's populous and on its information resource structures*, as well as defeating the enemy's control system and his information resource structures with the help of additional means, such as nuclear assets, weapons and electronic assets."[32]

Information-psychological security, defined as "the condition and use of information to guarantee the functional reliability of the psyche and consciousness of a person in peacetime or wartime," must remain a goal of commanders in the field.[33] A system of information-psychological security is important because:

"In the past half century the potential for working on the consciousness, psyche or morale of a person, society or the composition of an armed force has grown dramatically. One of the main reasons is the considerable success achieved by many countries in their systematic research in the areas of psychology, psychotronics, parapsychology, other new psychophysical phenomenon, bioenergy, biology and psy-choenergy in the fields of security and defense."[34]

While Western analysts place less credence in these latter issues, it is nevertheless important to recognize the attention and assets Russia directs to them. Some Russian military analysts have warned that the country is and will be the object of information-psychological strikes, aggression, expansion and pressure. A recommendation was made by one officer to construct an information-psychological counteraction (IPC) program.[35]

In fact, the information-psychological factor is so important to the Russian military that it considers the information-psychological operation as an independent form of military activity. A military activity is defined by the Russian military as "an activity conducted in the form of engagements, battles, operations, strikes and systematic combat actions." The term usually refers to operations on a strategic scale. Thus, the military is looking for ways to construct or win information-psychological engagements, battles and operations. These operations may include the normal leaflets and loudspeakers but could extend to atypical responses. Traditional IW uses, such as planned engagements of the enemy's information systems on the battlefield, might join nontraditional uses, such as striking at the enemy's perception of reality or attempting to control behavior or break the mental stability of combatants through the use of high-tech (holograms, satellite destruction) or nonlethal (acoustic or electromagnetic) means. Conversely, the goal of defensive information-psychological operations would be to protect the military collective and operations from such activities and counter any negative enemy action aimed at the psyche of the soldier.

One of the leading proponents of this idea is General Major E.G. Korotchenko, deputy chief of the chair for military art at the General Staff Academy. Korotchenko views information methods and techniques as nontraditional forms of power wielding. The main goal of IW against Russia in the information-psychological sense, Korotchenko believes is "to capture the consciousness of the population of the Russian Federation, to undermine the moral and fighting potential of the armed forces and set the stage for political, economic and military penetration."[36] Agents of this activity are considered to be the foreign mass media and the "activities" of tourists, foreign intelligence agents and certain busi-nessmen, advisers and journalists. This characterization implies the peacetime use of IW and Korto-chenko includes foreign agents' use of either special psychotropic or possibly even psychotronic means.[37]

Russian theorists have gone so far as to attempt to mathematically calculate the morale-psychological stability of the modern soldier and figure this component into their assessment of success or failure in engagements and battles. Some scientists are working on a mathematical model to calculate under what conditions the spirit of the soldier becomes a mass multiplier (an idea based on Leo Tolstoy's description of the spirit of the fighting man in *War and Peace*).[38] Other scientists are studying the moral-psychological impact of certain information actions, such as cutting access to a soldier's global positioning system (GPS).

Reflexive Control: an Information Weapon Subset

The Soviet Union had a propaganda machine second to none. One of its most intriguing methods for managing information and getting people (or an opponent) to perform a certain action was described by the theory of reflexive control (RC). In a military context, it can be viewed as a means for providing one military commander with the ability to indirectly maintain control over his opposing commander's decision process.[39] Reflexive control involves creating a pattern or providing partial information that causes an enemy to react in a predetermined fashion without realizing that he is being manipulated. Its aim above all else is to influence command and control systems and decision makers. Colonel S. Leonenko stressed the importance of using RC against systems in the IW age:

> "Under present conditions a need arises to act not only on people, but also on technical reconnaissance assets and especially weapon guidance systems, which are impassive in assessing what is occurring and do not perceive what a person reacts to."[40]

Thus, a system may be easier to deceive than a person. Colonel Leonenko further noted that under today's conditions the importance of the commander's personality in deciding what RC action to use is somewhat diminished, since collective decision making has become the standard way of doing business. In Leonenko's opinion, in addition to the increased potential for being fooled, computers hamper RC by making it easier to process data and calculate options. That is, computers' speed and accuracy make it easier for an opponent to "see through" an RC attempt by an opposing force if the information is processed correctly.[41]

Other aspects of RC are under scrutiny as well, including the strategic use of these concepts within IO/IW theory. One instructor at the General Staff Academy of the Russian Federation, General N.I. Turko, made a direct link between IW/IO and reflexive control, noting that "The most dangerous manifestation of the tendency to rely on military power relates **not so** much to the direct use of the means of armed combat as to the possible results of the use of reflexive control by the opposing side via developments in the theory and practice of information war."[42]

To Turko, the information weapon (RC) is more important than firepower in achieving objectives. His understanding is likely based on the belief that the use of the information weapons during the Cold War, such as the Strategic Defense Initiative or SDI, did more to defeat the Soviet Union and bring about its financial exhaustion and demise than any real weapons' use. Turko has also listed RC as a method for achieving geopolitical superiority and as a mechanism in arms control negotiations.[43] In this regard RC would be used to influence a state's information resource and thereby its decision-making process by formulating certain information or disinformation.

Russian military theorist S.A. Komov has written that RC is a form of "intellectual" IW. He offered the following eleven types of intellectual IW for use against systems, people, alliances or forces in the field:

Distraction—during preparatory stages of combat operations, creating a real or imaginary threat against one of the most vital enemy places such as flanks and rear, forcing him to reevaluate his decisions to operate on this or that axis.

Overload—often manifested by sending the enemy a large amount of conflicting information.

Paralysis—creating the belief of a specific threat to a vital interest or weak spot.

Exhaustion—cause the enemy to carry out useless operations, thereby entering combat with expended resources.

Deception—during preparatory stages of combat operations, force the enemy to reallocate forces to a threatened spot.

Divisive techniques—cause the enemy to believe he must operate in opposition to coalition interests.

Pacification—through a peaceful attitude and approach cause the enemy to lose vigilance.

Deterrence—create the impression of superiority.

Provocation—force enemy action advantageous to your side.

Suggestion—offer information that affects the enemy legally, morally, ideologically or in other areas.

Pressure—offer information that encourages society to discredit its own government.[44]

Finally, there is a direct connection between RC and information-psychological security from the Russian point of view. For example, in the journal *Problemy informatsionno-psikhologicheskoy* *bezopasnosti*, the well-respected RC theorist Dr. Vladimir Lepsky describes reflexive mechanisms for manipulating the conscience and behavior.

From the X-Files

The Russian armed forces are studying a host of unusual subjects, almost all of which center on how information or electronic waves affect the mind. For example, a recent book offered an extensive set of algorithms designed to implant "suggestive influences" or what the author called "psycho viruses" into a person's mind. This officially sanctioned book was commissioned by the Security Committee of the State Duma. The leader of a Security Committee subset, the Information Security Committee of the State Duma, co-authored a book on *Psychotronic Weapons* as well.

This latter subject has been one of intense military interest over the past several years. An article that appeared in the armed forces journal *Orientier* a few years ago was titled "Can a Ruler make `Zombies' Out of the World?" with a subtitle reading "It is completely possible that humanity is standing on the verge of psychotronic war." The article described many of the "psy" weapons available for use, such as VHF generators, lasers, X-ray equipment, ultrasound and radio waves. A psychotronic generator, for example, was described as a device that produces powerful electromagnetic emanations.[45]

The Ministry of Defense reportedly has a special unit known as 10003. According to the newspaper *Novaya Gazeta-Ponedelnik* (clearly not a mainstream newspaper and therefore suspect), this unit studies mysticism and the occult, primarily to understand the essence of mind control (for use in recruiting and other situations).[46] In other words, the Russians are exhaustively exploring what makes the mind tick and how to manage it.

It is important to note that many, if not all, of the "X-file" subjects listed here are highly suspect in the West. Even the newspapers in which such articles appear must be viewed with caution. Whether these ideas work or not is not the point. The issue is they form one of the elements of the Russian understanding of IW.

In their search to offset Western supremacy in the IW arena, Russian and Chinese theorists are exploring nontraditional, asymmetric approaches. One is to utilize the capabilities of psychological operations and deception to fool one's cognitive processes, especially the case in China, on the strategic level. Another is to control the mind and to affect the nervous system. This effort involves HNA methods designed to upset the data-processing capability of the human nervous system. In China these efforts are referred to as "new concept" weapons and in Russia as psychotronic war. Similar efforts with nonlethal weapons have produced some results in the West.

The Chinese approach to date, based on open-source materials, approximates efforts in the West (perhaps by design) in the psychological operations and deception fields. Chinese thinking in the HNA arena will be supplemented and integrated with the rich Chinese traditions in military art that impart a distinctive flavor to their strategic culture that is different from most Western theories. Russia's approach is more direct in exploring capabilities to corrupt or manipulate mathematical algorithms that control software packages and human behavior.

The ability to study the mind for all its strengths and weaknesses has always been a Chinese and Eastern culture strength. Russia also has had a strong capability in operational thinking in the military field and became most adept at using propaganda to the fullest extent during the days of communism. Adapting these capabilities to the data-processing capabilities of the mind is a new but logical extension of these tendencies. The West should absorb what is said about these matters in Russia and China, just as these countries have done with our debates over hardware. There is much to be learned from both countries.

---

[1] HNA is my term to describe the impact of human, computer or nonlethal generated attacks, such as deception or electromagnetic effects, on the human nervous or cognitive systems. It is neither a Chinese nor a Russian term, merely a descriptor.

[2] For two traditional discussions of Chinese and Russian IW thinking by this author, see "Behind the Great Firewall of China: A Look at RMA and IW Thinking from 1996-1998"; and "Dialectical versus Empirical Thinking: Ten Key Elements of the Russian Understanding of Information Operations," both located on the Foreign Military Studies Office web page, found at <http://fmso.leavenworth.army.mil/fsmo.htm>

[3] Sergei Modestov, "Kutay gotovitsya k informatsionnym voynam" (China is Preparing for Information War), *Nezavisimoe voennoe obozrenie* (*Independent Military Review*), No 13, 1998, 2.

[4] Hai Lung and Chang Feng, "Chinese Military Studies Information Warfare," *Kuang Chiao Ching*, 16 January 1996, 22-23 as translated in FBIS-CHI-96-035, 21 February 1996, 33-34.

[5] Shen Weiguang, "Focus of Contemporary World Military Revolution_Introduction to Research in Information Warfare," *Jiefangjun Bao*, 7 November 1995, 6 as translated in FBIS-CHI-95-239, 13 December 1995, 23- 25.

[6] Wang Baocun, "Information Warfare in the Kosovo Conflict," Beijing *Jiefangjun Bao*, 25 May 1999, as downloaded from the FBIS web site on 28 June 1999.

[7] Shen Kuiguan, "Dialectics of Defeating the Superior with the Inferior," *Chinese Views of Future Warfare*, revised edition, edited by Michael Pillsbury, National Defense University Press, Washington, DC, 1998, 216-217.

[8] David Watts, *London Times*, 18 August 1999, as downloaded from the Internet.

[9] George Capen, "Wei-chi: The Game of War," *Proceedings*, August 1999, 60. This game focuses on territorial expansion, attacking and defending. Territorial expansion occurs in peacetime, according to the rules of the game.

10. Alastair I. Johnston, *Cultural Realism*, Princeton Academic Press, 1995, 102. Johnston's outstanding book should be reinterpreted through the lens of the information age in order to get at the heart of the Chinese use of information technologies as strategic tools or methods today.

11. Sha Lin, "Two Senior Colonels and `No-Limit' Warfare," Beijing Zhongguo Qingnian Bao, 28 June 1999, 5. The author has taken the liberty to use the term unrestricted in place of no-limit, as it has been translated in other places. The article was translated and downloaded from the FBIS web page on 28 July 1999.

12. Miao Jinyuan, "Information Psychological Offensive," *Jiefangjun Bao*, 9 July 1996, 6 as reported in FBIS-CHI-96-168, 9 July 1996.

13. Ibid.

14. Liu Ping, "Some Remarks on Future Psychological Warfare," *Jiefangjun Bao*, 18 August 1998, 6 as translated and downloaded from the FBIS web page, 31 August 1998.

15. Ibid.

16. Ibid.

17. Ibid.

18. Zhang Guoyu, "Symposium on the Challenge of the Knowledge Revolution for the Military," *Beijing Jiefangiun Bao* 5 January 1999, 6 as translated and downloaded from the FBIS web page.

19. Ibid.

20. Wang Yongyin, "Intellectualization: Inevitable Trend of Future Military Development," *Jiefangjun Bao*, 20 April 1999, 6 as translated and downloaded from the FBIS web page on 10 May 1999.

21. Wang Zhi, "Lessons Learned from the Historical RMA," talk presented in Beijing in November 1998.

22. "New Concept Weapons and its Medical-Related Problems," *Beijing Renmin Junyi*, No 9, September 1997, 507, 508.

23. Ibid., Zhi.

24. The monthly journal *Beijing Renmin Junyi* of the PLA General Logistics Department Health Department carries many technical articles on military medicine.

25. Ibid., "New Concept…"

26. Ibid.

[27] Rui Yaocheng, Wei Shuiyi, and Chen Shengxin, "Progress in Military Pharmacological Research, Application," *Zhongguo Yaoxue Zazhi*, Vol 32, 662-667 as translated and downloaded from the FBIS web page, 23 September 1998.

[28] Translation of FBIS that was downloaded from their web page.

[29] S.V. Markov, "O nekotoryk podkhodakh k opredeleniyu sushchnosti informatsionnogo oruzhiya (Several approaches to the determination of the essence of the information weapon)," *Bezopasnost'* (*Security*), No. 1-2, 1996, 53.

[30] Ibid., 56.

[31] Ibid., 59.

[32] Discussion with a Russian officer in Moscow, May 1995. An *information resource* as used here refers to: information and transmitters of information, the method or technology of obtaining, conveying, gathering, accumulating, processing, storing and using that information; the infrastructure, including, information centers, the means for automating information processes, switchboard communications and data transfer networks; the programming-mathematical means for managing information; the administrative and organizational bodies that manage information processes, scientific personnel, creators of data bases and knowledge, as well as personnel who service the means of informatization.

[33] Markov, 47.

[34] Markov, 45.

[35] Ye. G. Korotchenko, "Information-Psychological Warfare in Modern Conditions," *Military Thought*, English edition, 1/96, 25.

[36] Ibid., 22.

[37] Ibid., 23. Psychotronics is defined as "an inter-disciplinary area of scientific knowledge, which, mediated by consciousness and by perceptual processes, investigates distant (noncontiguous) interactions among living organisms and the environment. It studies the energy and information phenomena of such interactions." See V.D. Ts'gankov and V.N. Lopatin, *Psikhotronnoe Oruzhie i Bezopasnost' Rossii*, Moscow 1999, 16, 17.A psycho-physical (psychotronic) weapon is defined as "a technically generated means designed to exert an information and/or energy influence on the functions of the human psyche and on the physiological functioning of human organs and systems. It belongs to the category of non-lethal weapons." See M.I. Abdurakhmanov, V.A. Barishpolets, V.L. Manilov, V.S. Pirumov, Geopolitika I Natsional'naya Bezopasnost', Moscow 1998, 144.

[38] V.I. Tsymbal, "Kolichestvenno-kachestvennyi analiz vliyaniya informatsion-nykh sredstv na khod i iskhod vooruzhennoi bor'by (Qualitative-Quantitative Analysis of the Influence of Information Means on the Course and Outcome of Armed Conflict)," report at the conference on

"Analiz Sistem Na Poroge XXI Veka: Teoriya i Praktika (Systems Analysis on the Verge of the 21st Century: Theory and Practice), conference proceedings, Moscow, 1997, 281.

39. Clifford Reid, "Reflexive Control in Soviet Military Planning," in *Soviet Strategic Deception*, edited by Brian Daily and Patrick Parker, Lexington Books, 294.

40. S. Leonenko, "O Refleksivnoe upravlenie protivnikom (On Reflexive Control of the Enemy)," *Armeyskiy sbornik* (*Army Journal*), No. 8, 1995, 28. For more on technology and Infosphere attacks, see my article "Infosphere Threats," beginning on page 46 of this issue.

41. Leonenko, 29. On the other hand, computer processing may actually improve the chances for RC's being accepted since a computer may not have the intuitive capability of a human.

42. A. A. Proxhozhev and N.I. Turko, "Osnovy informatsionnoy voyny" (The Basics of Information Warfare), report at the conference on "Systems Analysis on the Threshold of the 21st Century: Theory and Practice," Moscow February 1996, 251.

43. N.I. Turko and S.A. Modestov, "Refleksivnoe upravlenie razvitiem strategicheskikh sil gosudarstva kak mekhanizm sovremennoy geopolitiki (Reflexive Control in the Development of Strategic Forces of States as a Mechanism of Modern Geopolitics)," report at the conference on "Systems Analysis on the Threshold of the 21st Century: Theory and Practice," Moscow February 1996, 366.

44. S. A. Komov, "About Methods and Forms of Conducting Information Warfare," *Military Thought*, July-August 1997, 18-22.

45. I. Chernishev, "Poluchat li poveliteli `zombi' vlast' nad mirom?" (Can a Ruler Make `Zombies' Out of the World?) *Orientier*, February 1997, 58-62.

46. Roman Shleynov, "Armed Evil Forces: The Dubious Experiments of the Ministry of Defense," *Novaya Gazeta-Ponedelnik*, 26 October-1 November 1998, No. 42, 1 and 5 as translated in FBIS, 11 November 1998.
