CHAPTER 20

Nation-State Cyber Strategies: Examples from China and Russia

Timothy L. Thomas

AN EARLY adopter of cyberspace concepts in the United States was the Air Force, which established a cyberspace command in November 2006. That same year, U.S. policymakers developed the *National Military Strategy for Cyberspace Operations,* which lays out national strategy in the form of ends, ways, and means with the goal of ensuring U.S. military strategic superiority in cyberspace. However, not all nation-states approach the new capabilities of cyberpower in the same way. This chapter describes how China and Russia are implementing cyber doctrine and practice; the challenges each country's cyber strategy presents to current U.S. practices; and what weaknesses those strategies reveal in the U.S. approach.

The cyber strategy of China is focused as much on the use of information warfare (IW) stratagems and reconnaissance of foreign sites as on attacking others' Web sites. Nationalists do most of the hacking that causes disruptions, often during crises in China; whether they are state-directed is not clear.

The cyber strategy of Russia focuses on ensuring information security by managing the flow of information to its citizens, as well as on securing its physical information infrastructure.

This chapter first discusses how China uses what it terms *informationization* (the word *cyber* is not widely used in China but has been noted as a cognate of *informationization*), and the role of informationization in the strategic thought of the People's Liberation Army (PLA). Then, Russia's potential cyber strategy is illuminated through an examination of its cyber terminology and its understanding of the term *strategy*. The chapter concludes with a brief statement of lessons for U.S. cyber strategy.

China

In recent years, Chinese cyber capabilities have become more visible and troubling. China has launched an unknown number of cyber reconnaissance and offensive events with unknown intent against a variety of countries. Episodes reported publicly include espionage conducted in 2005 against U.S. Department of Defense (DOD) computers in operations that Federal investigators code-named Titan Rain.[1] China also reportedly attempted to blind a U.S. satellite using high-powered laser attacks in 2006.[2] Attacks on the U.S. Naval War College's net capability, reportedly originating from China, shut down email and computer systems for several weeks in 2006.[3] When an old Chinese weather satellite was destroyed with an antisatellite missile, a Beijing People's University commentator related this capability both to "the development of missiles" and to "an IW capability."[4] China has also been accused of backing hacker attacks against Japan and Taiwan.[5] These attacks were perceived as retaliation: in the case of Japan, for its anti-Chinese interpretations of history, and in Taiwan, for its claims of independence.

The growing intensity of these cyber attacks demands a closer look at China's cyber philosophy and how it has evolved. Of particular interest is how cyber issues have been embedded into the peacetime strategic activities of the PLA and China's potential use of cyberpower as a preemptive strategy.

Development of Cyber Philosophy

The word *cyber* does not enjoy widespread use in China, which instead generally employs the word *informationization*. However, the latter term may be a cognate for *cyber*. In 2005, the Chinese military translated its own publication, *The Science of Military Strategy,* into English.[6] Chinese translators added a few pages at the back of the book titled "Selected Chinese-English Terms," in which the Chinese word for *information attack* had the alternate translation *cyber attack.* The Chinese word for *informationization* had next to it the alternate translation *cyberization.* Two other related Chinese words were expressed in English as *age of cyber information* and *cyber war*. The main text also dedicated one sentence to the concept of *comprehensive cyberized war*. The editors state that "information production modes keep developing and global integration moves on. Political elements, modes of violence, and even the intension [sic] of war will all be updated. A new pattern of comprehensive cyberized war is going to appear."

In February 2007, *China National Defense News* defined *cyber warfare* broadly as a "struggle between opposing sides making use of network technology and methods to struggle for an information advantage in the fields of politics, economics, military affairs, and technology."[7] Cyber warfare would be "a series of actions like network surveillance, network attack, network defense, and network support by opposing sides using network technology in the area of combat command, weapons control, combat support, logistical support, intelligence reconnaissance, and combat management." Cyber warfare was identified as an important action toward achieving "network control." Control is a vital aspect of China's information operations theory: whoever controls the network can take preemptive actions, either in a propaganda war or in real confrontations such as computer network attacks. Both the cases of Titan Rain and the attacks on the Naval War College are potential examples of confrontational Chinese activities on the Internet, although no U.S. official has confirmed Chinese involvement at a government level.

Cyber technology potentially has advanced Chinese thinking with regard to preemption. Chinese military academics state that those who do not preempt lose the initiative in what may be a very short-lived war; combatants in present- day conflicts, they argue, will find it easier to obtain the objective of war through a single campaign or battle than at any other time in history.[8] The idea of sudden attack has changed. It no longer simply means surprise in the old sense; rather, it means that one side cannot react even if the situation is known, because the other side possesses more advanced technology.

As a result, Chinese analysts argue, preparation and mobilization are more important than ever before.[9] War preparations, to include the recruitment of information talent, must be made in advance, so that a cyber operation, if needed, can be conducted suddenly with the use of all civil-military links.[10] Launching preemptive attacks to gain the initiative includes "striking the enemy's information center of gravity and weakening the combat efficiency of his information systems and cyberized weapons."[11] This allows one to weaken the enemy's information superiority and reduce its holistic combat efficiency.[12]

It appears that the PLA does not expect to go along this path alone. In March 2007, PLA National Party Congress deputy Chen Zuoning declared that the army and civilians together must strengthen state information security cooperation. He suggested they join hands and share resources in the creation of a national cyber information security coordinating institution.[13]

In May 2006, China published its *2006–2020 State Informationization Development Strategy*. Although it is not specifically military, it is in many ways a counterpart to the *National Military Strategy for Cyberspace Operations*. It called for China to:

- provide a nationwide cyber infrastructure[14]
- strengthen capacities for the independent innovation of cyber technologies
- optimize the cyber industry structure
- improve cyber security
- make effective progress in building a cyber-oriented national economy and society
- establish new industrialization models
- build and perfect national policies and systems for the cyberization process
- enhance capabilities to apply cyber technologies among the public
- promote the cyberization of the national economy
- popularize e-government
- establish an advanced Internet culture
- accelerate social cyberization.[15]

To understand China's cyber strategy, it is necessary first to understand how the Chinese definition of *strategy* differs from that of the United States, which defines *strategy* as "a prudent idea or set of ideas for employing the instruments of national power in a synchronized and integrated fashion to achieve theater, national, and/or multinational objectives."[16] The *Chinese Military Encyclopedia* defines *strategy* as "the analytical judgment of such factors as international conditions, hostilities in bilateral politics, military economics, science and technology, and geography as they apply to the preparation and direction of the overall military/war plan." The definition notes that it is "advantageous to study the occurrences and developments in war forecasting/predictions; to formulate strategic policy, strategic principles, and strategic plans; to make warfare preparations; and to put into place directives on the actual principles and methods of warfare."[17] Thus, the major difference is the U.S. concept of a set of ideas for employing the instruments of military power to achieve military objectives versus China's perception of an analytical judgment of factors applicable to a war plan.

One of China's most prominent military strategists, Li Bingyan, discussed strategy in terms of the use of information, a crucial component of cyber processes, to influence or control the direction of an opponent's decisionmaking activities.[18] It involves the wisdom, intelligence, and intellect of decisionmakers and how they gain the upper hand in a competitive environment by calculating the future, grasping the situation, making comprehensive plans, and seeking gains while avoiding harm.[19] Li wrote that military strategy should absorb new methodologies, including cybernetics and information theory.[20] If absorbed and understood properly, strategy will be able to take advantage of new conditions. Li thus emphasized the innovative use of information strategies in war.

The best strategy, according to Li, tries to entice the opponent to adopt a strategy that will lead China to the greatest gains. In this sense, risk and opportunity coexist.[21] The fog of war is used to execute, conceal, and develop strategy; strategists hope to know the situation on the other side, while using strategy and concealment to increase the fog affecting the opponent. Planning and designing strategy calls for knowing the enemy, while implementing strategy requires use of information channels to send the information, or misinformation, that one wants the opponent to know or perceive.[22]

To thwart the enemy's plans, friendly forces must analyze the size of the interests and contradictions of the two sides. One should arrange factors and see if one's own interests and objectives can be realized by influencing or destroying the opponent's cognition systems or by changing the opponent's decision-making.[23]

Li described the development of information warfare as a process of escalation. The way that the United States uses battlefield IW, he argued, still relies mainly on data and understanding, seeking to cut off an opponent's flow of information and to assure information flows for its side.

For China, in contrast, Li argued that high-technology warfare requires that Eastern military strategy must shed some old thinking and take into account new features: methods are new; information is abundant; content is vast; summaries are strong; preplanning is detailed; and resolution is quick. This implies that the revolution in military affairs (RMA) is changing the commander's concept of time, space, and strategy. Military theory can now emerge from laboratories, and military strategy can be previewed there.[24]

Li explained how a weak country could fight a technologically superior opponent by using superior knowledge of the other side. Metaphorically, he asked, "How could a mouse hang a bell around a cat's neck?" His answer is that the mouse could "entice the cat to put on the bell himself." In another metaphor, he posed, "How do you make a cat eat a hot pepper?" He suggested three possible ways: "You can stuff it down his throat (the most difficult). You can put the pepper in cheese and make him swallow it. Or you can grind the pepper up and spread it on his back, which makes the cat lick himself and receive the satisfaction of cleaning up the hot pepper."[25] In the last method, the cat is oblivious to the end goal and, said Li, this makes it a useful strategy. One must understand how an opposing side reacts to certain criteria.

Integrating High-tech Cyber Weaponry with Traditional Military Stratagems

One of China's foremost experts on IW is Dai Qingmin, who was director of the PLA Communication Department of the General Staff with responsibility for IW and information operations (IO). Discussing the importance of using RMA-generated information in shaping strategies, he said, "Today we should grasp the historical opportunity afforded by making these transformations in this information age . . . and formulate an effective threat and IW combat capability as soon as possible, thereby gaining the strategic initiative in the military struggles of this new century and even in international struggles."[26]

The topic of developing information warfare or cyber warfare strategies and tactics has taken center stage in China's discussions over the past few years. Dai wrote that "new technologies are likely to find material expression in informationized arms and equipment which will, together with information systems, sound, light, electronics, magnetism, heat, and so on, turn into a carrier of strategies."[27]

Dai's comments imply that China may intend to use packets of electrons as it once used forces. Stratagems such as "kill with a borrowed sword" and "exhaust the enemy at the gate and attack him at your ease" suggest how information operations might, for example, use packets of electrons to help country A destroy country C's information infrastructure after passing the packets through country B, the borrowed sword. Packets of electrons thus serve as the implementers of stratagems.

Dai defined an *information operation* 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 form."[28] Since these operations are a confrontation of forces and arms as well as a trial of strength focusing on knowledge and strategies, Dai recommended a "focus on strategies."

Dai noted that scientific and technological developments have given strategies a new playing field. A strategy may carry different contents under different technological conditions. Thus, there is room for both traditional strategies and for mapping out new strategies using new technological means. Options include new information confrontation strategies.[29] Overall, said Dai:

> [A good strategy may] serve as a type of invisible fighting capacity; may make up inadequate material conditions to a certain extent; may narrow a technological or equipment gap between an army and its enemy; and may make up a shortage of information fighting forces or poor information operational means.[30]

Some specific strategies that Dai suggested include:

- jamming or sabotaging an enemy's information or information system
- sabotaging an enemy's overall information operational structure
- weakening an enemy's information fighting capacity
- dispersing enemy forces, arms, and fire while concentrating one's own
- confusing or diverting an enemy and creating an excellent combat opportunity for oneself
- diverting an enemy's reconnaissance attempt and making sufficient preparations for oneself
- giving an enemy a false impression while simultaneously launching a surprise information attack
- blinding or deafening an enemy with all sorts of false impressions
- confusing an enemy's mind or disrupting an enemy's thinking
- making an enemy believe that what is true is false and what is false is true
- making an enemy come up with a wrong judgment or take a wrong action.[31]

Dai emphasized that future operations must integrate the use of both military and civilian information forces. Information systems are offering more modes for people to take part in IO as well as giving people a chance to serve as a major auxiliary information fighting force.[32]

Dai pointed out that traditional tactics can help shape a strategy before a war so they can sabotage and weaken a superior enemy while protecting or enhancing China's own fighting capacity, serving as a type of invisible fighting capacity, and even helping China to evade combat with a stronger enemy.[33] Dai stated that new developments had created challenges to some traditional strategies while improving conditions for others. He did not specify which strategies he had in mind. However, if defeating strong forces with weak forces in future IW is a goal, then stratagems may suggest useful asymmetric means for China to combat U.S. high technology.[34] In this sense, stratagems would be one of the "magic weapons" that the Chinese stress.

Dai broke with Chinese tradition when he advocated gaining the initiative and seizing information superiority by attacking first. This active offensive strategic emphasis contradicts China's traditional strategy of active defense and indicates new missions for IW/cyber forces. Dai noted that integrated and joint IO, two subjects rarely discussed by other Chinese military

specialists until recently, gives more scope and purpose to a people's war. His support of stratagem-based activities and the writings of other Chinese analysts on the subject should be closely followed by Western analysts.

Information Warfare Strategems

Another important article offered several ways to apply IO stratagems in the information/cyber age.[35] Authors Niu Li, Li Jiangzhou, and Xu Dehui defined *information warfare stratagems* as "schemes and methods devised and used by commanders and commanding bodies to seize and maintain information supremacy on the basis of using clever methods to prevail at a relatively small cost in information warfare."[36] Niu, Li, and Xu compare how East and West view the combination of stratagems and technology in different ways based on their different military and social cultures, not to mention their economic prosperity, and evaluate how this has resulted in different thought processes:

> Traditionally, Oriental people emphasize stratagems, and Occidental people emphasize technology. . . . Occidental soldiers would seek technological means when encountering a difficulty, while Oriental soldiers would seek to use stratagems to make up for technological deficiencies without changing the technological conditions. An Oriental soldier's traditional way of thinking is not conducive to technological development, but can still serve as an effective way of seeking survival in a situation of danger.[37]

A Western proclivity to look for technological fixes has been recognized and critiqued by both Chinese and U.S. analysts. Little has been written or published in the West, however, on IW stratagems. Western audiences have underappreciated the Eastern focus on strategic sophistication and perhaps their importance in general. A proper mix of the two may be required to ensure that all sides of a situation are properly assessed.

Niu, Li, and Xu argue that clever stratagems can help China make up for its deficiencies in high-technology–based weaponry. Stratagems may combine human qualitative thinking with computer-assisted quantitative calculations. One goal, for example, may be to cause enemy commanders to make mistakes by influencing their cognitive elements and system of beliefs. The idea is to force enemy commanders to develop decisions in the direction desired by the Chinese side, as suggested earlier by the scenario of the cat and the bell.[38]

Stratagems must be devised to be compatible with the characteristics of different networks, and they must be used by a system capable of ensuring information acquisition, transmission, and processing. They must control the entire process in a targeted manner, which requires an understanding of how an information contest develops over different stages and times. Chinese authors place emphasis on attacking first; this indicates that, in the information age, an active offense may be more important than an active defense.[39]

In the acquisition or preparation phase, stratagems might be devised to interfere with, damage, or destroy listening and antilistening, camouflage and anticamouflage, reconnaissance and antireconnaissance, or stealth and antistealth devices, among other items. Perhaps this is the current stage of development of China's cyber philosophy. Stratagems may be included in information flows to block channels of communication while keeping friendly flows of information secure. Some of the methods of influencing information flows are to carry out interference and anti-interference, deciphering and antideciphering, and destruction and

antidestruction efforts. The processing phase requires stratagems that, in addition to the transmission task, include misleading and antimisleading efforts targeting the enemy's information processing system, to cause the enemy to make decisionmaking errors.[40]

Stratagems can be used to intimidate, employ perception management, and create fictitious objects (such as fake networks and equipment in an information system) as part of a deception plan whose intent is to hide true reality. The intellectual battle is now more important than contests in bravery, the authors note, and wide-ranging knowledge and superior wisdom, boldness, and scheming ability are required.[41]

A stratagem can be as simple as misleading the enemy by pretending to follow his wishes. If one knows the enemy's intentions, the enemy can be led into a trap:

> A contest in information warfare stratagem is usually conducted in a non- contact manner, and contains efforts to create cognitive errors on the part of the enemy and to influence the contents, process, and direction of thinking on the part of the enemy's commanders and relevant personnel for information warfare; the purpose is to make enemy commanders make wrong decisions or even stop fighting, so as to achieve the objectives of information warfare without fighting.[42]

The effectiveness of this strategy would need to be evaluated based on the enemy's perceived awareness of the strategy's intent and subsequent response. Niu, Li, and Xu noted that "there are many ways of seizing information supremacy and the initiative in IW, and the use of stratagems is one of the most efficient ways." They suggest 10 specific stratagems that can be applied to IW.[43] *Thought-directing.* Direct others' thinking toward the wrong decision by attacking cognitive and belief systems and force commanders to make errors. Use schemes with regard to enemy doubts and exploit information relays between enemy units and departments.

Intimidation through momentum-building. Generate psychological pressure via intimidation by signaling inevitable victory, concentrating forces, and coordinating information networks. This is achieved by creating a situation favorable to China and unfavorable to the enemy. Intimidation is to be achieved via momentum- building: enhancing one's own position, situation, and posture while blocking the flow of information to the enemy.

Information-based capability demonstrations. Intimidate by demonstrating capabilities in actions that should not appear to be intentional. The right time, occasion, and modality must be chosen to make information believable to the enemy. One's own true strength should not be revealed, and one should be unpredictable, using both true and false information.

Prevailing over the enemy with extraordinary means. Adopt active and effective measures to generate surprise, and use decisive technical equipment and means of information warfare. Develop and hide information warfare "killer weapons."

Using fictitious objects to hide the true picture. Hide true reality by creating a fictitious reality. Simulate combat forces using high-tech means, to include the creation of nonexistent objects, such as fictitious networks or information systems, as well as fictitious strategic and operational objectives.

All-encompassing deception. Apply deceptive schemes simultaneously or consecutively according to strategic or operational intentions. Actions taken should be coordinated to ensure the enemy will have no suspicion.

Prevailing over the enemy with all-around strength. Use all means of information warfare to maintain supremacy, including electronic soft attacks by use of reconnaissance

satellite systems and the like, hard attacks such as informationized precision guidance weapons or strategic bombings, and command, control, communications, and information battlefield control and management.

Going with the flow. Mislead the enemy by pretending to follow his wishes. Pretend to "go with the flow" by exploiting one's knowledge of an enemy's intentions and the detection of enemy moves in order to lead the enemy into a trap.

Releasing viruses to muddy the flows. Release viruses to contaminate information flows. Using viruses, the authors note, is an important combat operation. A virus attack is "a technical act, which will have to be based on the use of stratagems in order to play an important role in IW." Stratagems should be used to create a favorable time for releasing viruses. It is important not only to seize opportunities but also to create opportunities and to "attack first."

Controlling the time element. Control of the time element is crucial. Information inducement, deception, concealment, and containment operations will help achieve the desired amount of control.[44]

The goal of the use of stratagems, write Niu, Li, and Xu, is to force an opponent to refrain from deciding to launch information attacks in order to achieve objectives without direct fighting; to create cognitive errors in the enemy; to influence the content, process, and direction of thinking on the part of enemy commanders; and to create a multidimensional threat with which the enemy must contend.[45]

China is already a cyber competitor of the United States. Hopefully, it will not become a cyber enemy. However, China is making significant strides in tying its cyber capabilities to its strategic concepts and is taking a more active (some would say threatening) posture. The Chinese use a different cyber vocabulary and different definitions, analyses, and institutions for the study of cyber-related strategic issues than the United States. China's definition of strategy encompasses basic and applied theory as well as the objective and subjective aspects of strategy and discusses ways to apply stratagems familiar from traditional Chinese military thought in new ways to shape information warfare. China's Academy of Military Science (a comparable institution does not exist in the United States) studies the science of information operations (an academic discipline that does not exist in the United States); and the University of Information Security proposed by Shen Weiguang (China's father of information warfare) will study cyber issues and strategy. An updated version of Mao Tse Tung's people's war strategy includes cyber techniques and procedures. China seeks to develop cyber countermeasures, both technical and cognitive, to Western cyber strengths. China frequently practices information-related mobilization exercises.

It is important for the United States to continue to examine how China is developing and applying its cyber-related strategic concepts and to prepare to adapt to them or develop countermeasures to them. Of particular concern is the Chinese movement in the direction of a preemptive strategy. Discussing strategic guidance, the editors of *The Science of Military Strategy* stated that information operations are directly linked to the gain or loss of the initiative in war and thus "priority should be given to the attack and combining the attack with the defense."[46]

China's extensive computer reconnaissance in the United States and other countries should cause other nation-states to take note. Cyber issues such as these should be seen in light of the ancient dictum that "a victorious army first wins and then seeks battle." It is possible that China's cyber strategy is already preparing to preempt U.S. systems if Beijing perceives a need to do so. More importantly, China's ability to hide the form of its attack will

make it difficult to recognize a preemptive action as it unfolds.

Russia

Russia, like China, has been accused of conducting cyber activities against foreign states. The main U.S. accusation was a series of incidents between 1998 and 2000 that came to be known as Moonlight Maze. These intrusions were reportedly traced to a mainframe in Russia. Moscow denied any involvement, and the actual state sponsor (if any) or origin of the attack apparently remains unknown.[47]

More recently, a 3-week wave of cyber attacks against Estonia reportedly originated primarily from Russia. This attack came at a time when Estonia and Russia were in dispute over the planned Estonian removal of a Soviet war memorial from Tallinn. The main targets of the attacks were the Estonian presidency and parliament, government ministries, political parties, three of the country's six news organizations, two of the biggest banks, and firms specializing in communications.[48] European Union and North Atlantic Treaty Organization (NATO) officials did not accuse Russia formally. Estonian officials, however, identified specific Russian Internet addresses, including some from Russian state institutions.

Russia denied any involvement. Kremlin spokesman Dmitry Peskov stated that in "no way could the state be involved in terrorism."[49] Direct Russian responsibility for the attack became even more questionable when Estonia arrested one of its own citizens (an ethnic Russian) and charged him with complicity in the attack. It was reported that he was simply angry over the war memorial issue.[50]

In response to the attack on Estonia, NATO stated its intention to establish a Cyber-Security Center in Estonia.[51] The agreement for such a center was signed on May 14, 2008. The center will develop standards and key directions for NATO's cyber protection system and carry out expert analyses of suspected cyber attacks.[52]

In light of these episodes and in the absence of any formal charges, Russia's complicity remains uncertain. But that is not to say that Russia does not have a national cyber-related strategy. On February 7, 2008, President Vladimir Putin signed a document titled, "The Strategy of Information Society Development in Russia." When briefing the strategy in early April 2008, Vladimir M. Vasilyev, deputy director of the Department of Information Society Strategy of the Ministry for Information Technologies and Communications, used the term *cyber* several times in his charts that explained the strategy.[53] Developments such as these indicate that Russia's cyber and information strategy deserve examination for the direction they are headed and for basic content. Perhaps more than any other country, Russia is alarmed over the cognitive aspects of cyber issues as much as their technical aspects, which make its strategy of further interest.

In Russia, *military strategy* has been defined as a system of scientific knowledge about the objective laws of war as armed combat to achieve certain class interests.[54] Military strategy prepares for and wages war and conducts various forms of strategic operations.[55] Strategy organizes, directs, and guides the deployment of forces during war, proceeding from and serving the needs of policy.[56]

Officially, Russia does not use the word *cyber*. In unclassified publications on information warfare and information operations, the term seldom appears, and then only when referring to other countries. Instead, like the Chinese, Russian military and civilian communities prefer the term *informationization*.[57]

A related term is *electronification*. In a plan called "Electronic Russia," the Ministry of Information and Communications is studying the formation of an information society and its electronification to address the Moscow region's information security plan and other issues.[58] The purpose is to thwart aggression against Russian systems by criminals, terrorists, or nation-states.

Concerns regarding criminal use of cyber actions are illustrated by comments of the First Deputy Head of the Russian Interior Ministry, Konstantin Machabeli, who stated in October 2006 that Russia had the ability to combat high-tech crime but that there was no law that would regulate it. He described cyber terrorism as "the use of the Internet aimed at recruiting new members of terrorist organizations and spreading information that calls for interethnic strife and racial intolerance."[59]

However, use of the term *cyber*, while not widespread, is growing in colloquial speech and even in some military journals. A November 2006 journal article noted that:

> In recent years certain socio-economic, scientific-technical, and cultural prerequisites have formed in our country for the development of an information society and its essential attribute—cyberspace. The latter has today essentially become a new front for global confrontation and all of humanity has become a target for a possible cyber attack.[60]

Russia recognizes that informationization topics greatly influence the modes and methods of the conduct of war. For example, virtual simulations influence what strategy a Russian commander might take. In 1995, General Vladimir Slipchenko stated that the Russian General Staff Academy was no longer doing force-on-force simulations but rather system-on-system simulations, to include cyber and other information-related systems.[61] This suggests that cyber issues influence strategic planning from its earliest stages in Russia.

Reflexive Control, Stratagems, and Perception Management

Russia views the cognitive aspect of cyber issues as more important than do most other nations. Some Russian policymakers feel that the disintegration of the Soviet Union was due to a cognitive attack or deliberate information operation. Many Russian books discuss the "Third World War" as a war of information in which the West conquered the Soviet Union.

While the Chinese use stratagems to alter the reasoning of decisionmakers, the Russian preference is for a concept known as *reflexive control*, a process in which the controlling actor conveys to the target various motives and reasons that cause the latter to reach the decision sought by the controlling actor.[62] The decision itself must be made independently. In this sense, reflexive control is very much like the stratagem concept employed by the Chinese. A *reflex* involves the specific process of imitating the enemy's reasoning or possible behavior and causing it to make a decision unfavorable to itself:

> In fact, the enemy comes up with a decision based on the idea of the situation which he has formed, to include the disposition of our troops and installations and the command element's intentions known to him. Such an idea is shaped above all by intelligence and other factors, which rest on a stable set of concepts, knowledge, ideas and, finally, experience. This set usually is called the "filter," which helps a commander separate necessary from useless

information, true data from false, and so on.[63]

The chief task of reflexive control is to locate the weak link of the opponent's filter and to exploit it. Accordingly, during a serious conflict, the two opposing actors (countries) analyze their own ideas and those of the perceived enemy and then attempt to influence one another. A reflex refers to the creation of certain model behavior in the system it seeks to control (the objective system). It takes into account the fact that the objective system has a model of the situation and assumes that it will also attempt to influence the controlling organ or system. Reflexive control exploits moral, psychological, and other factors, as well as the personal characteristics of commanders. (Thus, biographical data, habits, and psychological deficiencies could be used in deception operations.[64]) In a war in which reflexive control is being employed, the side with the highest degree of reflex (the side best able to imitate the other side's thoughts or predict its behavior) will have the best chances of winning. The degree of reflex depends on many factors, the most important of which are analytical capability, general erudition and experience, and the scope of knowledge about the enemy. Military author Sergei Leonenko added that, in the past, stratagems were the principal tool of reflexive control, but today camouflage and deception (*maskirovka*) have replaced stratagems; however, this conclusion is not universally accepted.

In his writings, Leonenko integrated information technologies and reflexive control theory. He noted that the use of computers could hinder the use of reflexive control by making it easier to process data and calculate options, allowing an opponent to see through a reflexive control measure by an opposing force because the computer's speed and accuracy in processing information could detect it. On the other hand, in some cases, this may actually improve the chances for successful reflexive control, since a computer lacks the intuitive reasoning of a human being.[65]

Computer technology could increase the effectiveness of reflexive control by offering new methods. Writing in 1995 from a military perspective, Leonenko defined reflexive control as:

> consist[ing] of transmitting motives and grounds from the controlling entity to the controlled system that stimulate the desired decision. The goal of RC [reflexive control] is to prompt the enemy to make a decision unfavorable to him. Naturally, one must have an idea about how he thinks.[66]

Leonenko assessed the new opportunities afforded by the use of computer (cyber) technology:

> In present conditions, there is a need to act not only against people but also against technical reconnaissance assets and especially weapons guidance systems, which are impassive in assessing what is occurring and do not perceive to what a person reacts.[67]

If an IW or IO operation system cannot perceive what a person reacts to and is unable to assess what is occurring, does this mean that it provides only insignificant data? Or does it mean that there are two layers of data to reflexively control? The first layer consists of the "eyes, nose, and ears" of sensors, satellites, and radars. The second layer is the "brain software" of humans, which gathers, processes, and produces knowledge from the information or makes decisions based on it. But what happens if the "eyes, ears, and nose" are manipulated? How does that affect the input into decisions and knowledge? Using such principles (perhaps from

studying Russian actions), Yugoslav forces in the Balkans fooled NATO sensors over Kosovo into shooting at fake targets.

In the end, some decisions are left to computers and are made automatically without human intervention. To Leonenko, this indicates that we live in a much more frightening environment than we may have thought: decisions may be made by machines that are "incapable of assessing what is occurring and do not perceive what a person reacts to." Leonenko noted that "how the enemy thinks" is shaped by combat intelligence and a collective image set made up of concepts, knowledge, ideas, and experience.

Leonenko's definition of reflexive control contains many of the elements of another term, the *information weapon*, defined by Sergei Markov as a "specially selected piece of information capable of causing changes in the information processes of information systems (physical, biological, social, etc., in this case, decision-making information) in accordance with the intent of the entity using the weapon."[68] Accordingly, it causes change in the information processes of an opponent by persuading it to make decisions according to the design of the controller, and it affords the information weapon a methodology for controlling an opponent. So defined, the information weapon, like reflexive control, can be applied in the modeling and decisionmaking contexts of various types of conflicts. It can also be used in social processes and systems.

The concept of reflexive control is influencing approaches to various branches of knowledge in Russia, including philosophy, sociology, psychology, pedagogy, and problems of artificial intelligence and computer science in general, as well as military affairs, intelligence, counterintelligence, and a number of other areas.[69]

Definitions of Information Warfare and Information Operations

No Russian definitions of IW and IO utilize the term *cyber*, although several discuss informationization. In general, Russian military theorists view information-related topics in two categories: information-technical and information-psychological. Russia does not separate information-related topics into the same kinds of categories that the United States and China do, such as psychological operations, computer network operations, operational security, deception, and the like.

The technical aspect is of greatest interest in most countries, but the psychological aspect is the area of most attention in Russia. A Russian book titled *Secret Weapons of Information War* stated that the primary threat to a nation's security in the 21st century is to its psychophysical security. Threats may take the form of psychological, suggestive, or "technotronic" effects (such as computer games, virtual reality, acoustical and video equipment, computer technology, and lasers and other effects).[70]

In 2002, Russian information warfare expert S.P. Rastorguyev defined *IW* as "a battle between states involving the use of exclusively information weapons in the sphere of information models." An *information operation* was defined as a "sequence of actions to use an information weapon to achieve an assigned task."[71]

An article in the Russian navy publication *Morskoy Sbornik* in October 2003 defined the two parts of IW further. The "information-psychological" part consisted of the mass media, the Internet, computer network attacks, leaflets, and religious propaganda. The "information-technical" part consisted of deception; misinformation; radio-electronic intelligence, attack, deception, and defense; counterintelligence; cryptology; and steganography.[72]

In October 2005, Konstantin Nikolskiy defined the principal object and meaning of IW to consist of "a disorganization of the structure of society and distortion of public consciousness, as a result of which society loses moral- psychological and scientific-technological potential and thereby is deprived of the capability to wage armed warfare." He defined information threats as "ideological-religious, scientific-technological, and emotional-psychological." He argued for viewing the world as an aggregate of specific properties of systems.[73]

The Initial Russian Policy on Information Security

In contrast to the Chinese approach, the Russian focus has been on the development of a state information security doctrine, international information security laws, and the "Electronic Russia" program, and on the study of U.S. cyber programs. The Russian strategic concept appears to focus on protecting the state from "harmful" information and from the effects of informationization while simultaneously focusing on international laws limiting the use and development of "information weapons," a term often used in Russia.

Russian authorities closely follow cyber developments in the United States. Pavel Shumilo described the U.S. cyberspace concept as the establishment of a national system to counter cybernetic security threats, and noted that other U.S. priorities were:

- a national program to prevent threats and decrease vulnerability in cyber-space
- the development of a conscious awareness among the population of cyber threats
- ensuring the security of the government's infrastructure in cyberspace
- cooperation in the sphere of international cybernetic security.[74]

Shumilo declared the U.S. approach, as he described it, to be similar to that of the Russian Federation's Information Security Doctrine.

Russia's Information Security Doctrine in 2000

The Information Security Doctrine was first developed in 2000, years before publication of the first official U.S. cyberspace document. It presented the purposes, objectives, principles, and basic directions of Russia's information security policy. Its 11 sections cover, first, the national interests of the Russian Federation in the information sphere, including observance of constitutional liberties of man and citizen, information backing for Russian Federation policy, development of information technology and industry, and protection of information resources from unsanctioned access.

The second section examines types of threats to Russia's information security. These include constitutional rights in spiritual life, information support for state policy, the development of the information industry, and the security of information. Third, it identifies external and internal sources of threats to Russia's information security. Fourth, it outlines the state of information security in the Russian Federation and objectives supporting it, discussing tension between the need for the free exchange of information and the need for restrictions on dissemination of some information.

General methods of information security of the Russian Federation—legal, organizational-technical, and economic—are outlined in the information security doctrine. The

document next discusses features of information security: economics, domestic policy, foreign policy, science and technology, spiritual life, information and telecommunications systems, defense, law enforcement, and emergency situations. Goals of international cooperation in the field of information security include such issues as a ban on information weapons, support for information exchanges, coordination of law enforcement activities, and prevention of unsanctioned access to confidential information.

Another topic of Russia's information security doctrine is a description of two provisions of state policy on information security: guidelines for federal institutions of state power and for balancing the interests of the individual, society, and the state in the information sphere. Priority measures in implementing information security are identified, including mechanisms to implement the rule of law and increase the efficiency of state leadership, and programs to provide access to archives of information resources, training, and harmonizing standards in the field of computerization and information security. The functions of the system of information security are discussed. Finally, organizational elements of Russia's information security system are described; these include the president, Federation Council of the Federal Assembly, the State Duma of the Federal Assembly, the government of the Russian Federation, the Security Council, and other federal executive authorities, presidential commissions, judiciary institutions, public associations, and citizens.[75]

Russia's Information Security Doctrine defines *information security* as "the state of protection of its national interests in the information sphere defined by the totality of balanced interests of the individual, society, and the state." Just a few months earlier, in a resolution to the United Nations, Russia had defined information security somewhat differently as the "protection of the basic interests of the individual, society, and the State in the information sphere, including the information and telecommunications infrastructure and information per se with respect to its characteristics, such as integrity, objectivity, availability, and confidentiality."

Information security in the defense sphere was highlighted in the doctrine.

The sphere involves:

- the information infrastructure of the central elements of military command and control, and the elements of military command and control of the branches of the armed forces and the scientific research institutions of the Ministry of Defense
- the information resources of enterprises of the defense complex and research institutions
- the software and hardware of automatic systems of command and control of the forces and weapons, arms, and military equipment furnished with computerization facilities
- information resources, communications systems, and the information infrastructure of other forces and military components and elements.[76]

External threats to the Ministry of Defense (MOD) are spelled out in the next part of the section. They include the intelligence activities of foreign states; information and technical pressure (electronic warfare, computer network penetration, and so forth) by probable enemies; sabotage and subversive activities of the security services of foreign states, including information and psychological pressure; and activities of foreign political, economic, or military entities directed against the interests of the Russian Federation in the defense sphere. Internal threats included the violation of established procedure for collecting, processing, storing, and transmitting information within the MOD; premeditated actions and individual mistakes with special

information and telecommunications systems, or unreliability in their operation; information and propaganda activities that undermine the prestige of the armed forces; unresolved questions of protecting intellectual property of enterprises; and unresolved questions regarding social protection of servicemen and their families.[77]

Ways to improve the system of information security for the armed forces included the systematic detection of threats and their sources, and structuring the goals and objectives of information security; certification of general and special software and information protection facilities in automated military control and communications systems; improvement of facilities and software designed to protect information; improvement in the structure of functional arms in the system of information security; training of specialists in the field of information security; and—most important, it seems, in light of the Russian military doctrine's views on information security—refinement of the modes and methods of strategic and operational concealment, reconnaissance, and electronic warfare, and the methods and means of active countermeasures against the information and propaganda and psychological operations of a probable enemy.[78]

The discussion of the defense sphere in the information security document varies in many ways from the general military doctrine of the Russian Federation. The latter is quite specific that information-psychological and information- technical matters are the two greatest informationization (cyber-related) external threats to Russia, and that disruptive plans or technologies are the greatest internal threats. The terms *information-technical* and *information-psychological* are not used in the information security doctrine, perhaps because military people did not write it. However, its sections on the spiritual and cultural sphere and the scientific research sphere do cover the gist of the military's concerns in information-psychological and information-technical realms. While not citing information-psychological issues explicitly, several sections implied that they were a concern. For example, under constitutional rights, it was noted that one threat was the unlawful use of special techniques of influencing individual, group, or social consciousness, and the disruption of cultural values. Under foreign policy concerns, one internal threat was identified as propaganda activities of political forces, public associations, the news media, or individuals who would distort or disrupt the strategy and tactics of the foreign policy activity of the Russian Federation. An important spiritual sphere of concern in the information security doctrine was the prevention of unlawful information or psychological influences on the mass consciousness of society, and another was the uncontrolled commercialization of culture and sciences.

The doctrine declared that the "implementation of the guarantees of the constitutional rights and liberties of man and citizen concerning activity in the information sphere is the most important objective of the state in the field of information security."[79] While this sounds reassuring enough, Russian citizens are concerned over the interpretation of this notion. Some citizens fear the government's ability to convey reliable information to the Russian and international community, since they fear that what is "reliable" information would be determined by the state. The record of the government's handling of information on the *Kursk* incident and the war in Chechnya causes some to question the idea of reliable government information. The government considers the "information war," conducted by the press for public opinion, to be a very important aspect of keeping the emotions and loyalties of its people in check during crises. All governments do this to a certain degree, but the Russian government appears to have gone quite far, especially in these two cases.

The doctrine stated near its conclusion that a basic function of the system of information security of the Russian Federation is "the determination and maintenance of a balance

between the need of the citizens, society, and the state for the free exchange of information, and the necessary restrictions on the dissemination of information."[80] The last paragraph of the document stated:

> The implementation of the priority measures in support of the information security of the Russian Federation enumerated in this doctrine presupposes the drafting of the corresponding federal program. Certain provisions of this doctrine may be made more specific with reference to particular spheres of the activity of society and the state in the appropriate documents approved by the President of the Russian Federation.[81]

Little was written about the Information Security Doctrine after 2000. One of the first doctrine-related articles to appear was generated by an October 23, 2000, conference on information security. Anatoliy Streltsov, deputy head of the six-member Information Security Department of the staff of the Russian Security Council, said that the doctrine might promote a dialogue between the authorities and the press. The conference wanted to create a data bank for shaping state policy in the sphere of the mass media and the formation of an effective basis for cooperation between the press services of ministries and agencies, on the one hand, and the mass media on the other.[82]

In another report, First Deputy of the Security Council Vladislav Sherstyuk, who helped draft the doctrine, claimed that it would not be used to restrict independent media or control television channels, but asserted that the state must supervise all media, state or private.[83] The Speaker of the Upper House of the Federation Council, Yegor Stroyev, stated that the doctrine did not contradict freedom of speech but was aimed at "consolidating the Russian state as a whole."[84] Anatoly Streltsov noted that the components of the doctrine provide for the constitutional rights and freedoms of citizens to obtain and use information, while providing for Russia's spiritual renewal, the development of moral values, patriotic and humanistic traditions, and cultural and scientific potential. The doctrine's components also provide information support to Russia's state policy, notifying the Russian and international public about state policy and offering citizens access to open state information. Most important, according to Streltsov, is that the doctrine would improve an individual's information security, since in 2000:

> [t]he doctrine drafters believe that the level of Russia's information security does not fully comply with the needs of society and the state. The constitutional rights of citizens to the inviolability of private life, personal and family secrecy, and secrecy of correspondence do not have sufficient legal, organizational and technical backing. The protection of information about individuals, which is collected by federal and municipal institutions, is inferior.[85]

Thus, the doctrine was presented as having the best of intentions, according to the official spokesmen.

Other Views

On October 5, 2000, Sherstyuk took part in an Internet chat with citizens from all over the country. He defined information security as the state of protection of national interests in the information sphere, dictated by the aggregated balance of interests of the individual,

society, and the state. Asked if the doctrine threatens freedom of the press, he replied:

> The state doesn't plan to control the independent mass media, let alone, as some journalists say, establish complete and comprehensive control over the television airwaves and infringe on freedom of mass information. You won't find such provisions in the Doctrine; they simply aren't there. You will agree that controlling the mass media and strengthening the state mass media is not one and the same thing.[86]

A participant in the Internet discussion asked if the balance between the individual, society, and the state was upset by this emphasis on the state, and also whether the doctrine signaled Russia's admission that it had lost the "information war" in Chechnya and the Balkans.[87]

Sherstyuk's reply to these questions was abrupt and unconvincing. He said it would be improper to talk about Russian defeat in "information wars" since there are no precise criteria for such defeats and victories. (Actually, the perceived requirement to publish an information security doctrine is arguably an indication of Russian defeat in this sphere.) Sherstyuk's denials notwithstanding, many Russian leaders and analysts have openly referred to the "information defeat" at the hands of the Chechens. Sherstyuk's answer was that fears about a disturbance of the balance of interests among the individual, society, and the state are simply groundless; however, many Russians were raising concerns about this very idea.[88]

June 2006 Military Policy Proposal

By 2006, Russian analysts were stating that the military policy of the Russian Federation needed to be updated, due to concern over the development, manufacture, introduction, preparation, and deployment of information weapons and the resulting endangerment of military security. Issues included restraining foreign states from deploying the means and methods of IW against Russia, promoting and developing international information security concepts with friendly states (including within the United Nations and other regional organizations, such as in Geneva or in accord with the Okinawa or Tunisia accords on the development of an information society), and arranging for equitable and reliable information exchanges based on the norms and principles of international law.[89] Another concern was that because "hundreds of millions of people have never been harnessed by the uniform world-wide electronic information space," they were "unprotected against the 'mass effect weapon' attack." Concern about critically important infrastructure systems was also mentioned, as "the triggering of production-induced, energy-oriented, financial catastrophes [would] creat[e] chaos and panic aimed at bringing the indomitable enemy [meaning Russia], after all, to its knees."[90]

Russian cyber strategy has accepted that the task of preserving internal stability in Russia is a priority. Books and articles claim that the death blow to the Soviet Union came, not from NATO conventional forces, but from an imperialist "information war" that Russia lost. By 2000, therefore, Russian state specialists had written the country's first information security doctrine (perhaps the first of any nation in the world), focused on laws and regulations and the information security of individuals as much as on the information security of industry.

This does not mean that Russia avoids attacking or conducting reconnaissance of foreign sites. Russia's fingerprints seemed to be all over both the Moonlight Maze incident and the cyber attacks on Estonia, even if conclusive proof of Russian involvement was not found.

Russian nationalist hackers, as in China, may be behind many of the reconnaissance or offensive attacks on foreign sites.

For Russian information warfare specialists, the use of information weapons is a key component of success. This effort is aimed as much at disrupting an adversary's information as it is at obtaining information supremacy. Targets of disorganization are not only weapons and decisionmakers on the field of battle but also the minds of average citizens. An article in *Morskoy Sbornik* listed, as aspects of the information-psychological aspect of information warfare, theories of the mass media, the Internet, computer network attacks, leaflets, and religious propaganda.[91] It is rare indeed to find computer network attacks listed more for their psychological than their technical impact, but this is the case in Russia.

With its talented corps of mathematicians, Russia is expected to remain a strong cyber power for the coming years. Of interest will be to see whether Russia's cyber plans are oriented more toward the information-psychological or the information-technical direction as it conducts future missions. Nation-states should expect to encounter Russia's electronic presence on the virtual battlefield, in plain sight or disguised by reflexive control principles.

Russia has also been aggressive in pushing an international understanding of informationization/cyber issues. They are active participants in discussions to define cyber-related (information/cyber aggression, information/cyber territory, cyber strategy, and so on) issues in the United Nations and among other international organizations such as the Shanghai Cooperation Organization. In this manner, Russia is leading the drive to shape the world's opinions regarding information-technology issues.

Lessons for U.S. Cyber Strategy

If U.S. cyber strategists expect to continue to lead the way in the cyber age, then they cannot afford to ignore the methods that other nation-states are using to advance their agendas or to implement cyber-age concepts. They must learn from these methods as well, both their offensive and defensive techniques. These methods reflect characteristics and approaches that differ, sometimes dramatically, from U.S. approaches. Chinese efforts to move packets of electrons through wires in accordance with 5,000-year-old stratagems come immediately to mind, as do Russian attempts to use international organizations to shape the world's understanding of cyber technology. Without close study of these and the approaches of other nation-states to cyber issues, it would be akin to playing a game of basketball in which your focus was solely on your team's offensive and defensive philosophy while disregarding your opponent's skill set and strategy. This can only result in defeat. Sun Tzu recognized this important aspect of potential conflict years ago, noting, "Know the enemy and know yourself and you will never fail in battle." Of particular importance in both the Chinese and Russian cases is their emphasis on cognitive aspects of cyber issues, an aspect to which the United States pays less attention than these nations.

A lack of agreement on international cyber terminology could also result in misunderstanding. One nation's understanding of cyber warfare could differ greatly from another's due to cultural or organizational differences. U.S. cyber strategists must continue to attempt to overcome this potential weakness in their assessment of the international environment, its actors, and the interpretations of events by these actors. The coming years could be ones of understanding or of tension and unanticipated circumstances. Hopefully, nation-states will work for the former and not leave our world to chance and at the mercy of the latter.

[1] Nathan Thornburgh, "The Invasion of the Chinese Cyberspies," *Time*, August 29, 2005, available at <www.time.com/time/magazine/article/0,9171,1098961,00.html>.
[2] Vago Muradian, "China Tried to Blind U.S. Sats with Laser," *Defense News*, September 25, 2006, 1.
[3] Josh Rogin, "Network Attack Disables Naval War College," *Federal Computer Week*, November 30, 2006, available at <www.fcw.com/online/news/96957-1.html>.
[4] Anthony Kuhn, National Public Radio, January 19, 2007, interview with Beijing People's University commentator.
[5] "Chinese Hackers Attack Taiwan Military Computers," *Taipei P'ing-kuo Jih-pao* (Internet version), May 15, 2006, Open Source Center Report no. CPP20060516310002.
[6] Peng Guangqian and Yao Youzhi, eds., *The Science of Military Strategy* (Beijing: Military Science Publishing House, Academy of Military Science of the Chinese People's Liberation Army), 2005.
[7] Pu Duanhua, "Network Control: New Access Control Concerning Outcome of Future War," *China National Defense News*, February 8, 2007.
[8] Peng and Yao.
[9] Ibid., 418–419. 10.
[10] Ibid., 345.
[11] Ibid.
[12] Ibid.
[13] Yang Zurong, "Military Deputy Appeals to Army-Civilian Joint Efforts to Guard 'Information Border'," *Jiefangjun Bao*, March 7, 2007, 4, Open Source Center Report no. CPP20070307710014.
[14] The word *cyber* was used in place of the term *informationization* here based on a glossary in *The Science of Military Strategy* where it was noted that the two words are cognates.
[15] Report on Chinese Military, Science and Technology Developments, May 1–15, 2006, Open Source Center Report No. CPP20060612478001, Department of Defense, in English, June 7, 2006.
[16] Joint Publication 1–02, *Department of Defense Dictionary of Military Terms* (Washington, DC: The Joint Staff, April 12, 2001, as amended through March 4, 2008).
[17] *Chinese Military Encyclopedia*, vol. 3 (Beijing: Military Science Publishing House, July 1997), 699.
[18] Li Bingyan, "Applying Military Strategy in the Age of the New Revolution in Military Affairs," in *The Chinese Revolution in Military Affairs*, ed. Shen Weiguang (Beijing: New China Press, 2004), 2–31.
[19] Ibid.
[20] Ibid. He also listed dispersion theory, function theory, intelligence theory, optimality theory, homology theory, and fuzzy theory.
[21] Ibid.
[22] Ibid.
[23] Ibid.
[24] Ibid.
[25] Ibid.
[26] Dai Qingmin, "Discourse on Armed Forces Informationization Building and Information Warfare Building," in Shen, 39–47. The chapter also appeared as an article in *China Military Science*, 2002.
[27] Dai Qingmin, "Innovating and Developing Views on Information Operations," *Zhongguo Junshi Kexue* (China Military Science), no. 4, August 2000, 72–77, Foreign Broadcast Information Service, document no. CPP2000911000150.
[28] Ibid.
[29] Ibid.
[30] Ibid.
[31] Ibid.
[32] Ibid.
[33] Ibid.
[34] Ibid.
[35] Niu Li, Li Jiangzhou, and Xu Dehui, "Planning and Application of Strategies of Information Operations in High-Tech Local War," *Zhongguo Junshi Kexue* (China Military Science), no. 4 (2000), 115–122, Foreign Broadcast Information Service document no. CPP 20010112000141. The authors of this article teach at an unidentified communications and command institute in China.

[36] Ibid.
[37] Ibid.
[38] Ibid.
[39] Ibid.
[40] Ibid.
[41] Ibid.
[42] Ibid.
[43] Ibid. The Chinese use the phrase *thought directing* in this article in the way a U.S. analyst might use *perception management*.
[44] Ibid.
[45] Ibid.
[46] Peng and Yao.
[47] See, for example, "Moonlight Maze," *Wikipedia*, available at <http://en.wikipedia.org/ wiki/Moonlight-Maze>.
[48] Ian Traynor, "Russia Accused of Unleashing Cyberwar to Disable Estonia," *The Guardian*, May 17, 2007, available at <www.guardian.co.uk/russia/article/0,,2081438,00.html>.
[49] Patrick Jackson, "The Cyber Pirates Hitting Estonia," *BBC News*, May 17, 2007, available at <http://news.bbc.co.uk/2/hi/europe/6665195.stm>.
[50] Kevin Poulsen, "We Traced the Cyberwar—It's Coming from Inside the Country!" *Wired*, available at <http://blog.wired.com/27bstroke6/2008/01/we-traced-the-c.html>.
[51] *Moscow Interfax*, May 17, 2007, Open Source Center document no. CEP 20070517950094.
[52] *Moscow Interfax*, May 14, 2008, Open Source Center document no. CEP 20080514950059.
[53] The author of this chapter was present for Mr. Vasilyev's briefing.
[54] V.D. Sokolovskiy, *Soviet Military Strategy* (New York: Crane, Russak, and Company, Inc.), 1963.
[55] S.N. Mikhalev, *Military Strategy: Preparation and Conduct of New and Latter-Day Wars* (Moscow: Kuchkovo Polye, 2003), 22, 23, quoting A.A. Danilevich's 1992 definition of strategy.
[56] S.F. Akhromeev, *Military Encyclopedic Dictionary* (Moscow: Military Publishing House, 1986), 711, 712.
[57] A Russian information operations specialist confirmed this use of *informationization* in place of *cyber* to this author in an October 2006 interview in Moscow.
[58] S.V. Belking and S.N. Navolokin, "Conceptual Foundations of the Moscow Oblast's Information Security," *Nauchno-Tekhnicheskaya Informatsiya. Seriya 1. Organizatsiya I Metodika Informatsionnoy Raboty*, no. 3, 2005, Open Source Center translation.
[59] *ITAR-TASS*, "Russian Interior Ministry Calls for Legislation to Combat Cyber Terrorism," October 19, 2006, Open Source Center document no. CEP 20061019950025.
[60] Pavel Shumilo, "A Cyber Attack on Humanity Is in Progress," *Armeyskiy Sbornik*, November 30, 2006, Open Source Center translation no. CEP 20070502322005.
[61] Author's discussion with Major General (retired) Vladimir Slipchenko in Moscow.
[62] S. Leonenko, "*Refleksivnoe upravlenie protivnikom* (Reflexive control of the enemy)," *Armeyskiy Sbornik*, no. 8 (1995), 28.
[63] Ibid.
[64] Ibid., 29–30.
[65] Ibid., 29.
[66] Ibid., 28. This is akin to how British and American perception management theorists view the purpose of deception.
[67] Ibid.
[68] S.V. Markov, "*O nekotoryk podkhodakh k opredeleniyu sushchnosti informatsionnogo oruzhiya* (Several approaches to the determination of the essence of the information weapon)," *Bezopasnost* no. 1–2, (1996), 53.
[69] Vladimir E. Lepsky, *Refleksivnoe upravlenie v polisubektnikh i mnogoagentnikh sistemakh* (Reflexive control in multi-object and multi-agent systems)," copy of an unpublished manuscript provided by Lepsky to this author, 2.
[70] V.F. Prokof'ev, *Secret Weapons of Information War* (Moscow: Sinteg), 2003.
[71] S.P. Rastorguyev, *An Introduction to the Formal Theory of Information War* (Moscow: Vuzovskaya Kniga, 2002). In an earlier book (*Information War* [Moscow: Radio and Communication, 1998]), Rastorguyev discussed the use of algorithms to put "psycho viruses" into people's heads. His focus over the years has been on

computer methods to accomplish both information-technical and information-psychological goals.
[72] R. Bikkenin, "Information Conflict in the Military Sphere: Basic Elements and Concepts," *Morskoy Sbornik*, no. 10 (October 2003), 38–40.
[73] Konstantin Nikolsky, "When They Shoot with Words," *Krasnaya Zvezda*, October 19, 2005, 2.
[74] Pavel Shumilo, "A Cyber Attack on Humanity Is in Progress," *Armeyskiy Sbornik*, November 2006, Open Source Center document no. CEP 20070502322005.
[75] *Information Security Doctrine*, Russian Federation Security Council (Internet version), September 13, 2000, Open Source Center translation.
[76] Ibid.
[77] Ibid.
[78] Ibid.
[79] Ibid.
[80] Ibid.
[81] Ibid.
[82] ITAR-TASS, "Conference on Information Security, Mass Media Held in Russia," October 23, 2000.
[83] "Russia Calls for International Information Security System," *Interfax*, October 12, 2000.
[84] Lyudmila Yermakova, ITAR-TASS, September 12, 2000, Foreign Broadcast Information Service.
[85] Mikhail Shevtsov, ITAR-TASS, September 12, 2000, Foreign Broadcast Information Service.
[86] V.P. Sherstyuk's responses to questions from Internet users, October 5, 2000, Foreign Broadcast Information Service.
[87] Ibid.
[88] Ibid.
[89] I.N. Dylevskii, S.A. Komov, S.V. Korotkov, S.N. Rodionov, and A.V. Fyodorov, "Russian Federation Military Policy for the Provision of International Information Security," *Military Thought*, June 30, 2006.
[90] Ibid.
[91] Bikkenin.