Information Security Thinking: A Comparison Of U.S., Russian, And Chinese Concepts

by Mr. Timothy L. Thomas, Foreign Military Studies Office, Fort Leavenworth, KS.
July 2001
This article was previously published in
The Science and culture Series
Nuclear Strategy and Peace Technology
International Seminar on Nuclear War and Planetary Emergencies
August 2001
Pages 344-358

Introduction

The advent of the information age forced many nations to reexamine their security procedures. As a result of the new and overwhelming dependence of critical infrastructure on information systems, information security is a priority concern to governments everywhere. However, not every nation has interpreted this concern in the same fashion, nor at the same pace.

Russia, for example, is ahead of everyone. It has produced an Information Security Doctrine that includes the security of the state, society and the individual in its evaluation of information security threats. This paradigm allows Russian security managers to consider information threats to citizens (their cultural, spiritual and psychological well-being) as well as to critical technologies and resources. Perhaps for this reason Russia's military doctrine lists external threats as information-psychological and information-technical issues. China has also been affected by the information age. It is concerned with influential technologies that might be used as a form of virtual deception or influence. The Internet is the focus of most of China's concern, most likely because it offers information that the Chinese government cannot control completely at this time. At the same time, China has an information technology security plan known as Plan 863, and established a Ministry of Information. China has not produced an information security doctrine or related document of which the author is aware. The U.S., while considering psychological operations as a key sub-element of information operations, relegates less attention to the information threat to the minds of its citizens. Rather, U.S. legislation and rights/acts (human rights, freedom of the press, speech, etc.) provide cover for its citizens in this field. The U.S. focuses on critical infrastructure protection instead of technologies and resources as the

Russians. The U.S. seldom uses the term “information security” when discussing cyber-based threats in official documents.

A brief look at how these three nations define information security supports this broad overview. The U.S. published two Presidential Decision Directives (PDDs) to counter information age threats to U.S. systems and its population, PDD-63 and PDD-68. PDD-63 focuses on critical infrastructure protection. The 22 May 1998 PDD-63 White Paper describes the growing vulnerability to U.S. cyber-based systems, and establishes a series of steps to counter this vulnerability. These steps are to be in place by 2003, and include the analysis of foreign cyber/information warfare threats. The directive mentions the term information security only twice, and then only in regard to public outreach programs.[1] PDD-68 coordinates U.S. efforts to promulgate its policies and counteract bad press abroad. This directive created the International Public Information (IPI) group to coordinate the identification of hostile foreign propaganda and deception techniques that target the U.S., according to the group's charter.[2] The focus is hostile information programs that might not be truthful. The directive does not characterize its actions as information security related. To find a U.S. definition of information security, one must turn to the military. Joint Publication 3-13, *Joint Doctrine for Information Operations*, defines information security as “the protection and defense of information and information systems against unauthorized access or modification of information, whether in storage, processing, or transit, and against denial of service to authorized users. Information security includes those measures necessary to detect, document, and counter such threats. Information security is composed of computer security and communications security. Also called INFOSEC.”[3]

Russia has a number of definitions for information security, perhaps because they have thought more about this subject than other nations due to their loss of ideology when the Soviet Union dissolved in 1991. Russia's September 2000 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 May 2000 United Nations resolution, Russia 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." The Russian Academy of Natural Sciences defined the term as “the protection of the information medium of the individual, society and the state from deliberate and accidental threats and effects.”[4] Information security, yet another source adds, is connected with information and its material carriers: the mind of a person and other carriers of information (books, disks, and other forms of “memory”).[5] Thus, differently than the U.S., Russia views both the mind and information systems as integral parts of its concept of information security.

Chinese academician Shen Changxiang, of the Chinese Academy of Engineering, defined information security in the People’s Liberation Army’s (PLA) newspaper of the General Political Department (the *PLA Daily*): “[information security] refers to the prevention of any leakage of information when it is generated, transmitted, used, and stored so that its usefulness, secrecy, integrity, and authenticity can be preserved; and so that the reliability and controllability of the information system can be ensured.”[6] State Council member Shen Weiguang notes that

information warfare (IW) is brain warfare. According to official Chinese sources, the Internet has the capability to manipulate information, the truth, and the moral-psychological state of Chinese citizens. China realizes that the Internet cannot be controlled, and is thus a concern to the government. Thus China appears more like Russia than the U.S. in its understanding of information security, with its emphasis on the mental aspect of information security and its extended use of the term itself.

This paper briefly examines the information security policies of the three countries noted. There are both narrow and broad approaches to the subject, and situational context, culture, and history are the real forces that differentiate national approaches. An understanding of each country's concerns and their paradigm for interpreting information security can potentially alleviate misunderstanding in future international discussions among nations over this concept.

U.S. Views on Information Security

With regard to information technology and critical infrastructure protection, PDD-63 demonstrated that the U.S. is very interested in establishing an "infrastructure to protect the infrastructure." The document builds on the recommendations from the October 1997 President's Commission on Critical Infrastructure Protection. PDD-63 opens by describing the growing potential vulnerability to America's cyber infrastructure, and then states the President's intent, the national goal, and the public-private partnership to reduce these vulnerabilities. Next general guidelines are issued, and then a structure and organization to meet the challenge are introduced (which included lead agencies for sector liaison, lead agencies for special functions, interagency coordination, and the appointment of a National Infrastructure Assurance Council). Tasks included:

- Vulnerability analysis
- Remedial plan
- Warning
- Response
- Reconstitution
- Education and awareness
- Research and development
- Intelligence
- International cooperation
- ; Legislative and budgetary requirements[7]

A National Coordinator for Security, Infrastructure Protection, and Counter-Terrorism is responsible for coordinating the implementation of the directive. This person will also chair the Critical Infrastructure Coordination Group (CICG). Further, the President authorized the FBI to create a National Infrastructure Protection Center (NIPC). This organization shall serve as a national critical infrastructure threat assessment, warning, vulnerability, and law enforcement investigation and response entity. Finally, the national coordinator will encourage the creation of a private sector information sharing and analysis center (ISAC). The center would be the mechanism for gathering, analyzing, appropriately sanitizing and disseminating private sector information to both industry and the NIPC, and could transmit NIPC information the other

way.[8] However, throughout the PDD-63 White Paper, only twice (and not in the main section) is the term "information security" used.

U.S. civilian agencies seldom use the term "information security." For example, in a computer search of Congressional committees and bills produced by the 107th Congress, there are four hits for the term "information security": the Computer Security Enhancement Act of 2001; the FBI Reform Commission Act of 2001; the E-Government Act of 2001; and the bill "To revise, codify, and enact without substantive change certain general and permanent laws, related to public buildings, property, and works, as title 40, United States Code, 'Public…". None of these address psychological security or manipulating the emotions or logic of individuals via information. Searches for the terms information-psychological security, and psychological security in the 50 bills of the 107th Congress resulted in zero hits.

Again, one has to turn to the military to find the use of the term "information security." The U.S. General Accounting Office report of March 2001 (GAO-01-341) is titled "Information Security: Challenges to Improving DOD's Incident Response Capabilities." The contents of this document demonstrate that, to the authors of this report anyway, information security is a computer and information system related problem. No reference is made to the individual, just to technical systems. The definition from the Joint Publication noted above emphasized the computer security and communications security aspects of information security.

PDD-68, mentioned above, discusses the requirement to identify hostile propaganda and deception targeted against the U.S.. However, PDD-68 apparently does not address information security. The actual document has still not been released. Even though the U.S. does not mention information security in terms of mental activity, other western nations do. Sweden, for example, has a psychological defense department that aims to uphold for every Swedish citizen a constitutional right to correct, clear and complete information on what is happening in society and in the world at large, especially in times of stress or crisis, or in times of particular importance.[9]

Most Americans realize that the issue of the influence of information on the minds of Americans is covered by different terminology than "information security." Advertising agencies are forbidden to persuade citizens using certain technology such as the infamous "25th frame effect" demonstrated in the 1950s at one theater. The mind reportedly can process 24 frames of film a second, and a 25th frame becomes a subliminal message. The movie theater in question sold popcorn and drinks by inserting this extra frame. This was ruled unconstitutional and other restrictions on media advertising are written into U.S. law to protect human rights and privacy. Thus American citizens are protected from "mind attacks" by different segments of legal code using different terminology.

The U.S. has not had to consider the human aspect of cyber-based operations nor the loss of an ideology as some nations have faced. In the affected countries consideration was given to the "information-psychological security" factor as a result to a much greater degree than in the U.S., which did not lose its democratic ideology. Russia lost an ideology and is working hard to ensure that Russian culture, identity, and spirit do not also disappear along with it.

Russian Views on Information Security

The approved Russian Federation's information security document represents the purposes, objectives, principles, and basic directions of Russia's information security thought. The document is divided into eleven sections. They are:

- National interests of the Russian Federation in the information sphere (observance of constitutional and individual liberties, information backing for Russian Federation policy, development of information technology and industry, and protecting information resources from unsanctioned access)
- Types of threats to Russia's information security (to constitutional rights in spiritual life, to information backing for state policy, to the development of the information industry, and to the security of information—the same as national interests!!)
- Sources of threats to Russia's information security (external and internal)
- The state of information security in the Russian Federation and objectives supporting it (tension between the need for the free exchange of information and the need to retain individual regulated restrictions on its dissemination)
- General methods of information security of the Russian Federation (legal, organizational-technical, economic)
- Features of information security (economics, domestic policy, foreign policy, science and technology, spiritual life, information and telecommunication systems, defense, law enforcement, and emergency situations)
- International cooperation in the field of information security (banning information weapons, supporting information exchanges, coordinating law enforcement activities, preventing unsanctioned access to confidential information)
- Provisions of state policy of information security (guidelines for federal institutions of state power and institutions, based on a balance of interests of the individual, society, and the state in the information sphere)
- Priority measures in implementing information security (mechanisms to implement the rule of law, an increase in the efficiency of state leadership, programs providing access to archives of information resources, a system of training, and harmonizing standards in the field of computerization and information security)
- Functions of the system of information security (summary of above points, 17 in all)
- Elements of the organizational basis of Russia's information security system (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).

The security doctrine's sections are further subdivided into three or four recognizable areas. First, there are some general principles associated with the section. Then the external and internal threats to that section's principles are listed, and this is followed by a list of measures to be taken to offset these threats. A look at the section on "subjects of the information security of the Russian Federation in the sphere of defense" follows to examine this methodology.

There are four general subject areas listed under this section. These are the information infrastructure of the central elements (the branches of the armed forces and scientific research institutions of the Ministry of Defense) of military command and control; the information resources of defense complex enterprises and research institutions; software and hardware of automated command and control systems; and information resources, communication systems, and the information infrastructure of other forces and military components and elements.

External threats to the Defense Ministry make up the next section. They include the intelligence activities of foreign states; information and technical pressure (electronic warfare, computer network penetration, etc.) by probable enemies; sabotage and subversive activities by the security services of foreign states using information and psychological pressure; and the activity of foreign political, economic, and military entities directed against the defense interests of the Russian Federation. Internal threats include the violation of established procedures for collecting, processing, storing, and transmitting information within MoD; premeditated actions and personal mistakes with special information and telecommunications systems, or with the latter's unreliable operation; information and propaganda activities that undermine armed forces prestige; unresolved questions about protecting intellectual property of enterprises; and unresolved questions regarding social protection of servicemen and their families.

The final section of the defense discussion outlines the main ways to improve the system of information security for the armed forces including the systematic detection of threats and their sources; structuring the goals and objectives of information security; certifying general and special software and information-protection facilities in automated military control and communications systems; the 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 in light of the Russian military doctrine's views on information security, the 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 probably enemy.

Interestingly, this discussion of the information security dimension of the defense sphere varies from the military doctrine of the Russian Federation. The latter states quite specifically that information-psychological and information-technical matters are the two external threats to Russia, and disruptive plans or technologies are the greatest internal threats. That these two important terms are not used in the information security doctrine is probably due to the fact that military people advised but did not write it. However, the two sections on the spiritual and cultural sphere, and the section on the scientific research sphere cover the military's information-psychological and information-technical concerns from the military doctrine. While not citing information-psychological activities directly, several sections imply this is a concern. For example, under constitutional rights, it notes that a threat is the unlawful use of special techniques influencing the individual, group, and social consciousness, as well as the disorganization of the system of cultural values. Under foreign policy concerns, an internal threat is the propaganda activities of political forces, public associations, the news media, and individuals who distort the strategy and tactics of the foreign policy of the Russian Federation. An important spiritual concern is the prevention of unlawful information and psychological

influences on the mass consciousness of society and the uncontrolled commercialization of culture and sciences. Thus, information security in Russian is focused on both the mind and on technical systems. The impression is that internal threats are more real and consequential than external threats.

The information security doctrine uses the term "information-protection" quite often, and this term is the one item that the state could put on a par with the military's information-psychological and information-technical issues. Another area of obvious emphasis is the formation of a legal base for information security. The laws on "State Secrecy," "Information, Computerization, and Information Protection," "Participation in International Information exchange," and "Essentials of Legislation of the Russian Federation on the Archive Collection of the Russian Federation and Archives" are specifically mentioned. Legal issues are one of three methods of information security mentioned in the doctrine, with organizational-technical and economic the other two. The threat of information weapons to Russia's information infrastructure and the threat of foreign governments using information warfare techniques against Russia were also mentioned. Special concern focused on the inadequate development of telecommunication systems, the integrity of information resources, space-based reconnaissance, and electronic-warfare facilities.

On an international level, the doctrine is designed to do several things. These include:

- Banning the development, proliferation, and use of information weapons
- Supporting the security of international information exchanges, including the integrity of information during its transmission by national telecommunication channels
- Coordinating the activities of these law enforcement agencies of countries that are part of the world community to prevent computer crime
- Preventing unsanctioned access to confidential information in international banking telecommunication networks and world trade information-support systems as well as information of international law-enforcement organizations fighting transnational organized crime, international terrorism, illicit trade in arms and fissionable materials, and in the distribution of narcotics and mind-altering substances, and the trade of human beings.

Near its end the doctrine notes 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." While this sounds pleasant enough, Russian citizens are concerned over the interpretation of this notion. Some citizens fear the fact the government was concerned about two issues: conveying RELIABLE information to the Russian and international community, and NOT ALLOWING propaganda that promoted the incitement of social, racial, national, or religious hatred and animosity. Measured against the government's handling of the Kursk incident and the war in Chechnya, the idea of reliable government information is questionable at best. The government considers the "information war" conducted by the press for public opinion as 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 swung the pendulum far past reason in these two cases. The doctrine states 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 needs of citizens, society, and the state for the free exchange of information, and the necessary restrictions on the dissemination of information."

The last paragraph of the document states that

> 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.

Over the next few years more attention should be directed to these more recent documents. The first meeting to start the process was the 23 October conference on information security. Anatoliy Streltsov, deputy head of the Information Security Department (which has six members) of the staff of the Russian Security Council, said that the doctrine might promote a dialogue between the authorities and the press. The conference hoped to create a data bank for shaping state policy in the sphere of the mass media and the formation of the most effective basis for cooperation between the press services of ministries and agencies, on the one hand, and the mass media on the other.[10]

Chinese Views on Information Security

The issue of information security appeared to become an important subject in China in early 2000. A series of articles on the subject appeared in the press throughout the year. Even though not directly addressed in the definition above of information security, the content of the articles showed that Chinese analysts consider the information security aspect of the mind more so than does the U.S. but less so than the Russians. For example, some Chinese analysts feel that the U.S. wants to use the Internet to shape the world's values in accord with those of the U.S. in order to maintain political, economic, military, and information benefits.[11]

It was also of interest that many Chinese information security articles are published by military journals. The military cites problems due to a neglect of safeguards, backward technology, and a lack of comprehensive rules and regulations.[12] The first Chinese all-army forum held in late October 2000 set forth management rules and accelerated building an effective protection system for information security technology. There are now more than 1,000 computer networks of various kinds for the PLA to manage.[13]

The military identified the "three shifts" required to ensure the security of network information. These shifts are from maintaining secrets to maintaining secrets and building firewalls, from merely emphasizing conventional security work to emphasizing the security of information, and from stressing administrative management to stressing both administrative management and prevention technology. Educators are trying to help officers renew their concept of security and establish building a "firewall" in everyone's head. The armed forces are trying to train a group of

"network guards" with high-tech expertise. This process has been accelerated through the establishment of an all-army center for information security examination, appraisal, and recognition.[14]

Chinese information theorists believe that the modern fight is centered on the "right of controlling information," making information security one of the "commanding heights" for winning a war. "The right of controlling information" is synonymous with having an advantage in warfare. This makes the information confrontation an important operational component of modern war with information security and confidentiality the main battleground. Obtaining and counter-obtaining, control and anti-control, and destroying and counter-destroying will become an important operational mode in future warfare, as will developing the strategies and tactics of information security work.

PLA deputies to the National People's Congress called for legislation on information security, and pointed out a few hidden dangers--technological traps and weak preventative measures. Deputies called for a national defense information security law, and concentration of effort to speed up the development of information security technology in China.[15] On 23 October 2000, the Chinese State council recommended that the 18th meeting of the 9th National People's Congress consider a final daft of related regulations on maintaining network and information security. It appears that the issue is receiving top-level consideration, and that a policy may be forthcoming in the coming year.[16]

Shen Changxiang wrote the most authoritative article available to this author on the subject of information security. He noted that the main threats to China's cyber-information system included (1) its being tampered with, altered, stolen or sabotaged by viruses, or by hackers taking advantage of the Internet to intrude into the system to collect and transmit sensitive information (2) using computers' CPUs, or pre-installed information collection and sabotage programs in the computer's operating system, data managing system, and application system (3) and monitoring and intercepting information, using the Computer's electromagnetic leaks and its peripheral equipment. Whoever excels in preserving information security; controls information and wins the information war in future conflicts. In IW, the difference between a developed country and an undeveloped country will be far smaller than if it were a conventional war. This requires that China draw up an information security strategy and information defense system.[17]

In the civilian sector, information security is as important a topic as it is in the military sector. In June of 2001 the weekly general affairs journal of China's official news agency Xinhua, *Liaowang*, stated that information security issues are now of the utmost importance. For example, the Internet is linked to vital national infrastructures as well as to the education, health, and minds of citizens. This makes the control of the Internet's information security aspect twice as important as it was in the past. In addition, it is estimated that over 33% of the U.S. economic growth is from the information industry. The U.S. has control over the Internet and online resources. *Liaowang* estimated that America has 70% of the world's web sites, 94 of the top 100 most visited web sites, accounts for nearly one half of the world's total number of cybercitizens, and conducts nearly 90% of the world's Internet business. It also controls 80% of the world's

computer systems and software markets. The Internet has also produced new information security issues such as simply controlling the amount of information available.[18]

The most visible expression of a Chinese information security "plan" was offered in the June 2000 issue of the Internet website Guojia Gao Jishu Yanjiu Fazhan Jihua (HTRDP) 863. This website is sponsored by the China Office for the High Technology Research and Development Plan, an institution under the State commission for Science and Technology. The web site offered a guide to help China focus on making technical breakthroughs regarding typical information security issues and tasks in politics, the economy, and culture. The guide is based on decisions from the "Emergency Information Security Technology Plan" formulated by a specialist group researching information security strategy for National Plan 863. The goals of the plan are: effectively alleviate information security issues for party and government network systems and financial network systems; effectively control the wanton propagation of illegal and deleterious information in mutually connected networks; and raise China's information security technology to a new level.[19]

There are several information security issues affecting China. First, China must correct flaws in its information security management system. There is no clear division of labor on information security management among various functional departments, and it is difficult to adapt the present management model to a networked era. Second, there is an inadequate legal system in place to handle information security issues. Critical laws designed to protect the information infrastructure have not been formulated, and the construction of a legal system lags far behind what is required. Third, more research is required in the area of core information security technologies and products. China is limited by its microelectronics industry, which is of a lower quality and standard. Many cryptographic, digital signature, identity authentication, firewall and monitoring system requirements are not fulfilled as a result. Finally, there are many hidden information security dangers associated with China's financial system. The use of lower-grade PCs and the lack of information security methods in supervisory management still make people nervous.[20]

Qiushi magazine warned that China must develop an information security system that is strong and adaptable, independent of foreign control, and must combat superstition, rumors, slander, pornography and hackers that corrupt people's minds and threaten national security. Of particular concern is the Internet as a subversive tool. The U.S.'s over reliance on technology causes it to forget that the last line of defense in information security remains people. China must also enhance the use of positive propaganda on the Net, and strive to run a number of web sites that attract people. China must also build up its information security infrastructure including network control centers, appraisal and certification centers, and virus prevention centers. This will help accelerate the promotion of China's information security sector.[21]

State Council member Shen Weiguang, reportedly China's first information warfare analyst, wrote that China needed a national information security commission to strengthen centralized leadership over information warfare research. Such a commission should assume total responsibility for China's information security and provide an information security and information warfare studies institute at the highest level. Soldiers no longer have a patent on war. There now are information invasion, information firepower surveillance, information deterrence,

and information pollution problems to contend with in information space. China must establish information security standards and rules of conduct, and issue information security assessments and inspection standards according to Shen.[22]

Conclusions

The purpose of this article was to examine the U.S., Russian, and Chinese understanding of information security. The examination shows that in both definitions and in discussion, Russia and China differ markedly in their idea of information security than does the U.S.. Russia and China are worried about ways to influence the mind and emotions of its citizens. The U.S., on the other hand, treats the mind as a separate issue governed by different terms: human rights, perception management, and so on.

The U.S. does not use the same lexicon in its documents (seldom if ever using "information security" in conjunction with the logic of its citizens), and has been affected by a different situational context.

Governed by such different paradigms, it is easy to fathom how discussion and understanding of the term "information security" in the U.N. could prove to be very difficult. However, with just minor compromises, common ground can be found. It is important to do so now. A decade ago, cloning and stem-cell research were futuristic problems for scientists but today they are problems scientists must learn to control. The speed of development of information technology implies that a futuristic concept such as the electronic manipulation of the mind may be closer than we want to believe. If that happens, the idea of information security will take on a whole new dimension. It is wise to prepare now for the future and develop some universal procedures for scientists to consider.

---

[1] White Paper, The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63, 22 May 1998, downloaded from the Internet.

[2] "International Public Information Presidential Decision Directive PDD 68, 30 April 1999, downloaded from the web site of the Federation of American Scientists on 3 July 2001.

[3] Joint Publication 3-13, *Joint Doctrine for Information Operations*, 9 October 1998, p. GL-7.

[4] Mubin Abdurakhmanov and Dmitry Barishpolets, "From the Dictionary 'Geopolitics and National Security,'" *Military News Bulletin*, Vol. Vii, No 10, October 1998, p. 13.

[5] V.I. Parfenov, "Protecting Information: Terms and Definitions," *Questions of Protecting Information*, No. 3-4, 1997, p. 1 of an insert.

[6] Shen Changxiang, "Information Security—an Important Contemporary Issue," *Jiefangjun Bao*, 4 April 2001, p 11 as translated and downloaded from the FBIS web site on 4 April 2001.

[7] White Paper, 22 May 1998.

[8] Ibid.

[9] See http://www.psycdef.se/english

[10] ITAR-TASS, "Conference on Information Security, Mass Media held in Russia," 23 October 2000.

[11] PLA Daily News, 9 November, 2000.

[12] "Security Means Ensuring 'Winning the War,'" *Jiefangjun Bao*, 27 October 2000 p. 1 as translated and downloaded from the FBIS web site on 27 October 2000.

[13] Li Xuanqing and Liu Mingxue, "PLA's Security Work Emphasis Shifted to Building of Information Security," *Jiefangjun Bao*, 27 October 2000 as translated and downloaded from the FBIS web site on 27 October 2000.

[14] Ibid.

[15] No author, title, *Jiefnagjun Bao*, 12 March 2000, p. 4 as translated and downloaded from the FBIS home page on 14 March 2000.

[16] PLA Daily News, 9 November 2000.

[17] Ibid., Shen.

[18] Yang Guangliang, "Paying Attention to Information Security," *Liaowang*, No 23, pp. 37, 38, 4 June 2001 as translated and downloaded from the FBIS web site on 12 June 2001.

[19] "PRC High Technollogy Research Development Plan, http://www.863.org.cn, 6 June 2000 as translated and downloaded from the FBIS web page on 25 October 2000.

[20] Ibid.

[21] He Dejin, "Raise Network Security Awareness and Build Information Protection Systems," *Quishi*, 1 November.

[22] Shen Weiguang, *The Third World War—Total Information War*, 2000 as translated and downloaded from the FBIS web page.