The Negative Impact of the Internet and Its Solutions

By Ru Guangrong, Chinese Information Center for Defense Science and Technology

The Chinese Defense Science and Technology Information Monthly

Issue 121, 5th Issue of 1998

The advent of the Internet has been one of the most exciting major events in the second half of the 20th century. The ancient dream of "a scholar knows all things happening in the world without venturing outdoors" has finally become a reality. Since 1993, the Internet started to take off. At present, the Internet has spread to more than 180 countries and regions, connecting more than 600,000 domestic networks of various types, hooking up more than 20 million computers available to 120 million users (2% of the entire global population). Within the Internet are the information treasures shared by all human civilizations.

The reason why the Internet seems all-powerful is because it has two characteristics no other mechanisms possess: first, the Internet contains the biggest resource of information in the entire world; second, it enables people to obtain an interactive mechanism to instantly communicate with each other.

Once connected with the Internet, everyone can enjoy the unparalleled richness of global information resources including textual, audio, graphic information. The information on the Internet is so rich that no one can tell what is really out there. Furthermore, the Internet information resources are constantly expanding at a great speed—one can only make a rough estimate. The types of information on the Internet are also wide-ranging, from scientific research, education, public policy, legal regulations to commerce, arts, entertainment etc. to include everything. For all those connected with the Internet, they can quickly put onto the Internet all they want announced or all they think others should know about.

The Internet not only has an inexhaustible amount of information as vast as the ocean, but also has its interactive mechanisms—net to net, net to people, and people to people communications—that makes the Internet seem able to take on any task: entertainment, interpersonal exchanges, education, health and medicine, information gathering, securities and investment, trade and settlement of commercial goods, even online voting, etc. All these seemed ever so remote and unrealistic only yesterday.

The exchange and sharing of information among all peoples has ushered in an omnipotent status in Internet applications. As long as people develop certain desires, the information to satisfy such desires will quickly and continuously appear on the Internet.

And such information will gradually satisfy people's desires for their material as well as spiritual demands.

With the knowledge economy gradually ascending to a dominant status and the gradual formation of an information society, to characterize the Internet as "omnipotent" may not be overstating.

In the last four years, our country has seized the rare opportunity of developing computer networks. By the middle of July 1998, our country has 570,000 computers connected with the Internet, with a total of 1.175 million users. In order to speed up the applications of information technology in operations, command, and communications, our military has also established many computer networks, some of which are connected with the Internet, making use for our military of what was originally designed to serve the U.S. military and U.S. scientific research.

However, due to its innate transnational, decentralized, open and unregulated nature, the Internet as a free, open and anarchic device has brought various countries great risks as well as opportunities. While it provides enormous convenience and stimulates the economy to further develop, the Internet has also brought us negative impact that cannot be ignored.

The Negative Impact of the Internet

1. The Political Influence of Reactionary Nature

    a. The Internet explicitly propagates and implicitly spreads western democratic values. These views are mainly spread through some governmental organizations or government-sponsored groups in the West. They select some typical stories that reflect western democracy and wrapped them up in attractive packages. Then they put these stories in visual and/or audio format and give them to people with great appeal and attractiveness. Most of those who have visited these websites come off praising the beauty of western democracy.

    b. The Internet degrades and repudiates those countries, political parties, and governments that have different ideologies from those of the West. Some websites provides free forums, allowing everyone to express one-sided views and cite examples that serve to demonstrate the backwardness of China; other websites underestimate the abilities of Asian governments (including the Chinese government) to control political situations and economic development; some so-called "June 4th Elites," and "pro-democracy fighters," have also utilized the Internet to profusely attack our socialist system, spread anti-Party and anti-government views, even launch ad hominen attacks on our national leaders. They take advantage of our nation's systemic reforms and the increasing social instability to disseminate views such as "national salvation through democracy" and "human rights as a supreme principle" etc. They also exploit popular sentiment of disenchantment resulting from unsatisfactory work and frustration in personal lives to agitate the populace. A website for "Central Collection of

Political Gossip With Regard to the Chinese Communist Party," for example, has become a hotbed for rumormongers.

c. The Internet can be used as a tool to harm national sovereignty and interfere with other countries' internal affairs. In some websites, when agencies and organizations of some foreign governments publish data, they treat areas such as Taiwan and Tibet as independent countries. The website of the U.S. National Geographic Society once published a map of Asia, which flagrantly excludes the South China Sea and Taiwan from our territories. Another example, some websites have published views supporting Taiwanese and Tibetan independence and providing some so-called "historical evidence." This has clearly interfered with our internal affairs. The politically intended websites all have certain level of deceptiveness, influencing people to accept their views subconsciously, albeit with some doubt at first, thus shaking people's firm stance of ideological correctness.

2. Cultural Invasion

a. The Internet advocates western life-styles. These websites display various aspects of western society and life, and the overwhelming majority of them have positive portrayals of the western life-style. It makes people believe that the West seems to be countries of absolute freedom and paradise for individual achievement where private life is without obstacles and external inferences. Partial information such as this is particularly appealing to our youths whose life philosophy and worldview have yet to mature. Many of these youths aspire with great diligence to go abroad just to "change a way of living."

b. The Internet helps dominant cultures impact and homogenize cultures in an inferior position. Because the Internet overwhelmingly is a culture of the English language, it further strengthens throughout the globe the culture based upon the English language. In comparison, cultures based upon the Chinese, the French and other languages have been weakened. Because of the introduction of the Internet, some under-developed countries have made themselves vulnerable to foreign dominant cultures, busy defending themselves. This situation has become so bad that scholars in some developing countries are concerned about their indigenous cultures being homogenized and have provided proposals to counter "cultural invasion" on different fronts.

c. The Internet corrupts people's minds, influences and changes people's moral perspectives and ethical values. Driven by the profits in the numbers of hundreds of millions of dollars, the pornography merchants in Western countries have opened pornographic websites, massively producing various kinds of sex information. Nude males and females are everywhere, performances by "computer prostitutes" have also openly entered the Internet. This development has led the Commerce Committee of the U.S. Senate to propose the "1995

Communications Act for Good Behavior" to prohibit sex crimes committed on the Internet.

3. The Security Threats

   a. Internal networks become susceptible to invasion. Various kinds of computer hackers (excluding the just curious) consist of complicated groups with all sorts of ulterior motives. They can strike anywhere, making trouble to no end. Some hackers defaced the website of the U.S. Department of Justice and changed it to include a Nazi emblem. Others have entered other people's computers and destroyed programs and data. In this regard, our country has seen an increasing number of hacker attacks. Furthermore, some unnamed organizations have entered our internal networks and caused major damages to some technical devices. The Internet can also be used to launch computer viruses targeted at specific networks so that the networks will be damaged or paralyzed. At present, live computer viruses are numbered more than 14,000, and they constantly evolve, the danger of which can never be underestimated.

   b. The Internet makes it easy to lose and leak secrets. Because cleared staff can freely send and receive electronic mail, voluntary leaking of secrets has become remarkably easy. Under the current circumstance, stealing secrets by people from outside is not all that difficult either. As long as one knows the working mechanism and the techniques of breaking passwords, many internal networks can be broken into at ease. Therefore, obtaining political, economic and technological intelligence through the Internet has become one of the important methods in contemporary political and economic espionage. To use the Internet to steal new and advanced technologies, economic policies and other classified information is a modality of obtaining enormous benefits with relatively low cost. According to the statistics of the U.S. FBI, incidents of the American Internet networks being broken into are rapidly increasing by 30% annually, making the U.S. suffer tremendously. With the widening application of the Internet in our country's political, economic and military realms, we must keep sufficient vigilance against such situations.

   c. The Internet poses the potential threat of information warfare. Some countries have applied the Internet into military operations, have conducted mock attacks against other countries' networks, or have fabricated deceptive information harmful to other countries' military forces. At a time when the information networks have become an important infrastructure of the nation and the military, the information warfare will be a war without the explosives, a war with a high invisibility, low cost, international, and multi-area (political, military, economic, social and material resources etc.) approach. The high-tech nature and the unpredictability of combat intelligence in information warfare have made it extremely difficult to organize an information defense. The U.S. Department of Defense has specifically established an "Executive Committee on Information Warfare," which is devoted to studying national policy for information warfare,

and conducting war games on some websites. According to a report by the Sunday Thames of England, on 29 June (1998), experts from Great Britain and the United States conducted a secret military exercise in the destructive attacks on computers, with the objective of preventing a blitzkrieg in an information war. The result of the exercise indicates that just a few hackers can paralyze the stock market, military systems and airports, making the superpower, the United States, unable to move around. This exercise greatly shocked the Clinton Administration. In a future information war, national financial transaction centers, stocks exchange centers, air traffic control centers, telecommunications control centers, railway control headquarters and various military networks, will inevitably become the main targets of information warfare.

d. The Internet can be used to commit crimes. The globalized Internet has provided wider horizon and more numerous technical means to commit computer crimes. In recent years, Internet crimes have skyrocketed. Mainly, these crimes include illegal intrusion into others' computer facilities, spreading viruses through the Internet, stealing and modifying commercial secrets, unlawful transfer of others' funds, and intentional destruction of parts of the networks by using computer programs. In the United States, where the Internet was invented, the financial sector loses $10 billion every year to Internet crimes. Other major developed countries also suffer from losses between tens of million dollars and several billion dollars annually. In our country, computer crimes are also increasing. So much so that in the new Criminal Codes implemented on 1 October of last year, specific clauses on punishing computer crimes were added. The North American Security Management Association warns, "If people are not careful, the information super highway will become a criminal super highway."

4. Information Flooding Has Caused Waste of Resources and Time

On the one hand, because the Internet is capable of connecting to tens of millions of consumers all over the world, some smart and omnipresent merchants have figured out all the methods to penetrate everywhere; and many of them use the Internet to disseminate their product catalogues and advertisements, thus creating "Internet junk." Many who manufacture and disseminate "Internet junk" have mastered the complicated Internet skills and are able to, at extremely low cost, spread massive amount of "junk" to create Internet traffic jams, making it difficult for the normal information traffic to go through smoothly. On the other hand, because of the lack of regulations and standards to follow, anybody can use any means to produce any type of information—real and fake information, correct and wrong information, good and bad information, wanted and unwanted information—thus creating a flood of information online. The result is to make it easier to mislead people into prohibited areas, while in the meantime increasing the difficulty and cost of searching and using valuable information, thus wasting considerable Internet resources and time.

In our country, those who often have contact with the Internet are Internet technicians, frequent Internet users, and Internet managers and monitors. Most of them are the

younger generation of cadres. (Related statistics show that among the Internet users in our country, 68.7% of them are between 21 and 30 years old). They have the following characteristics:

Low level of immunity. Due to their relatively young age, they have had insufficient time to receive political and ideological education, making them less capable of being immune to the negative impact of the Internet.

—

Higher level of "dissemination power." Due to work demands, these young cadres are usually higher ranked and better educated with most of them being post-secondary graduates and above. They are knowledgeable and are influential to people around them. Therefore, whether it's positive or negative influences, these people have a more powerful way of disseminating information.

Higher probability to be impacted upon. These people are mostly engaged in jobs that are technical by nature, and are regarded as "making a living by their skills." Therefore, some of them pay insufficient attention to the importance of political studies and thought reforms. Furthermore, because they tend to be lone operators on single machines, if they cannot be vigilant against being alone, they are more likely to be impacted by the negative sides of the Internet and are more likely to develop a "no one really knows what's going on anyway" psychology.

Solutions Leading to the Reduction of the Internet's Negative Impact

Solution 1: Strengthen our educational programs on patriotism, socialism and communism; keep up our mental firmness on ideological correctness. Because one can get in contact with all sorts of information through the Internet, some positive, some negative, we must avoid arbitrariness in our efforts of political education. We must start with placing ourselves in the position of a student, gradually and patiently provide guidance to them. We the educators must establish a dialogue with the educated to discuss and explore the level of truthfulness of the information from the Internet, telling them the truth from the fakery, and point out to them the negative and positive impact of certain information. To do this, the educators are required to possess solid grounding in theories, in our Party's policies on current events, and the latest conditions in the Internet and our personnel's thought development. To accomplish such an educational task, we must rely upon constant work on people's thoughts at the basic work unit level. As long as these people are solid in their political convictions, there won't be major problems resulting from the Internet, and the young cadres won't be seduced by promises and invitations to visit abroad, to study abroad and other activities, thus making it impossible for them to surrender to the enemy forces.

Solution 2: Strengthen moral construction, resist the penetration and influence of corrupt thoughts and culture, and keep the purity of our thoughts and morality. There are two "many's" on the Internet. The first is there are many mythologies about individualistic endeavors leading to personal successes. The second is there is much pornographic information. We must pay attention to these mythologies that exaggerate individualistic will to succeed, thus separating individuals from reality, from the collective groups. We

should strengthen our ability to identify and resist the seductions through intensified education on moral values and collectivism.

Solution 3: Educate our personnel and enhance our personnel management, enact strict rules and regulations on the Internet to prohibit leaking and selling secrets. We should regularly conduct the appropriate amount of education on keeping secrets through the measures that have been proven effective in the past. We should make various regulations to keep secrets on the Internet, requiring all personnel to strictly implement the necessary working and operating procedures so that we can to a large degree prevent loss of secrets through negligence. We can also discover problems by checking the websites the target individual under investigation has visited and the email messages the individual has sent and received, so that we can prevent the "I may get lucky and no one will ever know" psychology.

Solution 4: We should launch counter-invasion and counter-propaganda campaigns online against the views and actions in violation of our sovereignty and interfering in our internal affairs. Although the Internet is not like physical media with black characters clearly written down on a blank sheet, it has a much larger radioactive range with unimaginable influence. Any views and actions harmful to our country are not acceptable to us. Besides taking diplomatic approaches, we can also adopt various Internet technologies to wipe out the pernicious influences, or use counter measures to force it to rectify. As far as those views and actions expressed or taken in the guise of caring for our country's human rights and thus violating our country's internal affairs, we can counter attack online with rationality, tactics and evidence. By so doing, we can add an invisible battlefront online in the defense of our sovereignty.

Solution 5: Actively study how to counter-attack online intrusion for military purposes, and be prepared for future information warfare. Because Internet development in our country came relatively late, we are in a relatively backward situation. Yet precisely because we started late, we have an advantage in selecting the newer technologies, better deployment plans, and equipment with superior specifications and functions. Because we obtain our network software and hardware equipment, especially the network security products that are out of our own security control, mostly through import, we run great risks. Among the equipment we import, there may be pre-inserted viruses, hidden information channels, even recoverable keys to transmit passwords. These risks will bring great harm to us and make us controlled by others. Therefore, we must first solve the problem of obtaining control and sovereignty over the security mechanisms of Internet-related equipment so that we can establish our independent network security product system as soon as possible. To get ready for the challenge of future information warfare, we may consider formulating a cross-the-board information defense strategy and building an elite, efficient corps of information warfare analysts in the course of constructing our country's national information infrastructure.

—

Solution 6: Scientifically make laws, complete the legal system; strengthen law enforcement, and strike hard against Internet crimes. At present, our country has the following laws that are concerned with computer and the Internet: "Regulations of the People's Republic of China to Safeguard Computer Information Systems, " Provisional

Rules of the People's Republic of China on Managing The Computer Information Networks and the Internet," "Regulations of China to Manage Public Multi-media Communications," "Rules of Managing the Internet Security," and the newly enacted clauses in the Criminal Codes with regard to punishing computer crimes. But, with the rapid development of the computer networks, many new situations and problems are confronting us. The fragmented nature of our laws and regulations are thus thoroughly exposed as a result. Especially for our military, we lack a complete set of measures and regulations that are compatible with the military network's development and applications. Therefore, we must keep these new situations in mind and quickly amend, revise the related laws and regulations so that we can gradually establish a complete system of law in this area. The Internet system is a fragile one, in order to guarantee its healthy development and the wide application of the electronic commerce, we must strengthen the power with which to deal with the Internet crimes, to enhance the protection of the networks. In addition, it is also imperative for us to stop the spread of Internet viruses, participate in international cooperation to identify and weed out the sources of viruses, and to punish the virus originators.

Solution 7: Further develop our country's information industry, expand the influence of our country on the Internet, and increase the percentage of information resources from our country on the Internet. We should greatly generate information in Chinese to utilize the superior quality of our nation's culture, to resist the negative impact upon us caused by the unhealthy elements in the imposing foreign cultures. To prevent bad information from entering and polluting our country, the State Council's Office of Information and the specific agencies in charge of our national security have all adopted various measures from the perspectives of management, education, legislation and technical operations, and the concerned agencies are also using certain methods and facilities to monitor obviously harmful websites. Yet, there are simply way too many websites out there, with some of them hiding their web names, highly unpredictable and hard to catch. Therefore, to fundamentally change the current situation of our culture being the object of foreign impact, of our nation's culture being placed in the danger of being homogenized by foreign cultures, we must greatly propagate the main stream of our nation's culture to make it an important step to develop our socialist spiritual civilization through massive Chinese information influx into the Internet.

—

Solution 8: For specific purposes, we should develop various information search software to reduce the waste of resources and time caused by the increasingly saturated information. The information on the Internet is infinite. Up to the end of last year, there had been more than one million information sources that were providing services. The information on the Internet is increasing exponentially. Nobody and no organization can browse and read all the information on the Internet. Therefore, how to "find information by specific need" has become a major task. The current search software and websites categorize information only in a very simple way. Right now, the concerned agencies of many countries are using various technical approaches to study and develop "smart search software." If our country can first make highly intelligent search software, we can not only quickly, accurately find the information the users seek, but also avoid the harassment caused by Internet junk. If necessary, we can even to a certain extent prevent users from contacting harmful information.

Solution 9: We should take various technical actions to reduce loss and leak of secrets, and quarantine harmful websites. First, we must protect the areas where sensitive data resides. We must place in safe locations the network servers and databases that contain secret contents, and use various kinds of conventional classified information protection methods to make sure that unrelated personnel couldn't reach them. Secondly, we must place in safe areas the information delivery facilities. Currently, fiber optic material is recognized by all as the ideal information delivery material, because it can prevent most of the known methods of eavesdropping. Thirdly, we must protect the information in circulation, either by adding security levels to the software or by adopting methods of our own design to compress the data. Fourthly, we must prevent our internal networks from intrusion. One method is to set up many "firewalls;" another method is to use jamming devices to disguise electronic radiation; the third method is to make sure, when the computer is dealing with a leak, to physically separate the computer from the Internet connection, and to reconnect the computer with the Internet only when it is absolutely sure that the leaked information has been effectively deleted. We can use various kinds of preventive methods to strictly restrict the spread of classified information online, stop the silent entrance of espionage information, and effectively quarantine the pornographic websites and other obviously harmful websites.

In conclusion, it's impossible not to open up the computer networks and there is only one way to be totally risk free—closing the networks. Once the Internet is open, the benefit of people using it to the Internet resources will be accompanied by its negative impact. Therefore, at a time when the Internet applications have penetrated to all the aspects of our nation, to our military forces, we must control and to our best ability destroy its negative impact, making sure that while we can fully enjoy the power of the Internet in our nation and our military, we can also destroy the problem at its root, before it even begins to germinate.

http://210.79.226.16:81/cetinq2/qk/gfxx/xx1998/xx980515.htm