PIR CENTER
Center for Policy Studies in Russia

ПИР-ЦЕНТР
Центр политических исследований в России

INFORMATION CHALLENGES TO NATIONAL AND INTERNATIONAL SECURITY

FALL 2001

MOSCOW, 2001

Contents

INFORMATION CHALLENGES TO NATIONAL AND INTERNATIONAL SECURITY

FALL 2001

Authors:

Dr. Irina **Alexeyeva**, Leading Researcher, Institute of Philosophy, RAS
Igor **Avcharov**, Ministry of the Interior
Alexander **Bedritsky**, Research Associate, Russian Institute for Strategic Studies
Prof. Dr. Dmitry **Chereshkin**, Laboratory Head, Institute of System Analysis, RAS
Prof. Dr. Vladimir **Dyachenko**, General Staff of the Russian Armed Forces
Ass. Prof., Dr. Alexander **Fedorov**, Foreign Intelligence Service (SVR)
Vladimir **Ilyin**, Federal Security Service (FSB)
Dr. Alexander **Kononov**, Senior Researcher, Institute of System Analysis, RAS
Dr. Andrei **Krutskikh**, Section Head, Department of Security and Disarmament Affairs, MFA
Konstantin **Machabeli**, Ministry of the Interior
Dr. Georgy **Smolyan**, Chief Researcher, Institute of System Analysis, RAS
Prof. Dr. Anatoly **Streltsov**, Deputy Department Head, RF Security Council
Prof. Dr. Vitaly **Tsygichko**, Chief Researcher, Institute of System Analysis, RAS
Dmitry **Votrin**, Senior Counselor, Department of Security and Disarmament Affairs, MFA

Editors:
Russian version: Ass. Prof., Dr. Alexander Fedorov and Prof. Dr. Vitaly Tsygichko
English version: Dr. Andrei Krutskikh and Prof. Dr. Dmitry Polikanov

Printed in Russia
Address: P.O. Box 17, Moscow, 117454, Russia
Phone: +7+095-335-1955
Fax: +7+503-234-9558
E-mail: info@pircenter.org
Internet: http://www.pircenter.org

To order Russian or English editions, please send requests to fax +7+095-234-9558 or e-mail: info@pircenter.org. Checks or wire transfers. Express mail delivery.

Circulation:
1,000 copies
Signed for printing
on October 1, 2001

- Statements of fact and opinion expressed in the book are responsibility of the authors alone and do not imply the endorsement of the editors and the PIR Center.
- The English text is an abridged version of the Russian book prepared by the PIR Center.

- The PIR Center wishes to express special thanks to the Center for Nonproliferation Studies at the Monterey Institute of International Studies for making this publication possible through its support.

Publisher: PIR Center for Policy Studies in Russia
Amb. Roland Timerbaev, Executive Council Chair
Dr. Vladimir A. Orlov, Director, and Executive Council Member
Dr. Vladimir A. Mau, Executive Council Member
Prof. Yury Fedorov, Executive Council Member

Dear reader,

Russia has set forth the initiative to submit to official consideration of the UN the issue of maintaining international information security. In the famous letter of September 23, 1998, the Russian Federation emphasized the need to take into account the potential, but, nonetheless, serious threat of using achievements in the information sphere in violation of the principles of maintaining global stability and security, non-use of force, non-interference in internal affairs, respect for human rights and freedoms. In our opinion, such menace is urgent and requires preventive measures nowadays. We should not allow the new area of global confrontation to emerge, for it may cause a new spin of arms race involving achievements of scientific and technological progress and diverting enormous recourses from peaceful and sustainable development.

I have to note with content that detailed discussion of this topic within the UN is under way. In the last three years political resolutions sponsored by Russia and entitled "*Developments in the Field of Information and Telecommunications in the Context of International Security*" have been approved by consensus by the UN General Assembly. Such broad support to the Russian initiative results from the constructive and non-confrontational character of the proposal.

The problem of creating global information community with ensured information security has become one of the important elements of international affairs in the 21st century. This issue is widely discussed at many world forums, including G-8. Russia is also raising this topic in bilateral negotiations at various levels – from experts to top-ranking officials.

We believe that the concept of international information security may be promoted step by step, by expanding the geographical coverage and the scope of debated issues, by filling the resolutions of the UN and other international forums with specific provisions meeting common interests of international cooperation, security, and strategic stability.

I hope that research conducted by Russian experts will enable the readers to understand better the substance of the problem of information security, to realize the challenges caused by the use of new information technologies for military, criminal, terrorist, and other illegal purposes.

Deputy Foreign Minister of the Russian Federation
Georgy Mamedov

Dear reader,

The core and the determining factor for human development in the 21st century is information and information technologies. Global IT revolution has dramatically changed political, economic and social life on the planet. Positive aspects of these changes are evident. However, one has to note potential challenges related to IT progress – cyber terrorism, interference in private life, cyber crime, and military use of information technologies, which is fraught with devastating consequences.

Parliamentarians of all nations are charged with particular responsibility – to provide adequate legal basis in order to repel the aforementioned threats. One of the ways would be to harness national legislations in order to ensure legal use of information technologies and to maintain international information security. At the same time, it would be important to guarantee that regulations pertaining to national and international cyberspace should not undermine the fundamental democratic principle – freedom of speech and access to information.

Chairman of the Committee for International Affairs,
State Duma of the Federal Assembly of the Russian Federation
Dmitry Rogozin

Dear reader,

Mankind has entered the new stage of its development characterized by the formation of the post-industrial society, which is often called information society.

Political program for forming global information community has been laid down in the 2000 Okinawa Charter signed by the leaders of G-8 countries. President of the Russian Federation Vladimir Putin also signed this document.

The Okinawa Charter emphasizes that ICT is one of the most significant factors affecting the development of the society in the 21st century. Their revolutionary impact afflicts the way of life, education and job, interaction between the government and the civil society. IT become a vitally important impetus for the development of world economy.

An essential element of the efforts to form the information society is to ensure its security. The latter may be attained by maintaining security of national information infrastructures of every country in the world and by providing security of the global information infrastructure in general, as a technological basis for world cyberspace.

The UN General Assembly Resolution "*Developments in the Field of Information and Telecommunications in the Context of International Security*" adopted in December 2000 calls for multilateral consideration of not only information security challenges, but also of possible response to such dangers.

I believe that this book will contribute to this noble goal.

First Deputy Secretary of
the Security Council of the Russian Federation
Vladislav Sherstyuk

INTRODUCTION

The very term "information security" emerged in the Russian Federation in 1992 after adoption of the Law "*On Security*". The Information Security Doctrine of the Russian Federation was approved by the President on September 6, 2000. The document defines information security as protection of national interests in the area of information determined by an aggregate balance of interests of individuals, society, and the state. The doctrine implies that:

- interests of the individual in information area consist of effective implementation of constitutional rights to access information, to use it for legal activities, for physical, spiritual, and intellectual development, and of protecting information pertaining to personal security;
- social interests comprise of the interests of individuals, strengthening of democracy, establishment of the social state with the rule of law, achieving and maintaining social consensus, in spiritual renovation of Russia;
- interests of the state mean creation of conditions to harness development of Russian information infrastructure, to implement constitutional rights and freedoms of citizens to obtaining and using information for the benefit of strengthening constitutional arrangements, Russian sovereignty and territorial integrity, political, economic and social stability, ensuring the rule of law, securing equal and mutually beneficial international cooperation.

Information security also implies resistance to enemy attacks against important information systems of the states, including the use of information systems for criminal purposes, whose most dangerous form is cyber terrorism. This provision is so significant because sustainable development and functioning of information systems is one of the key factors affecting success of social and economic reforms in Russia on its way to democracy.

There are several reasons for that. Globalization has become the most substantial trend in current global development. Countries that try to stay away from this process will inevitably find themselves in the position of losers. Technological backbone of globalization is integration of national information systems, formation of the single information space, including development of global information and communication networks; intense introduction of new ICT into all spheres of human activities. Rapid development of information infrastructure is a technological basis for transformation of economy, education, and culture. It makes people freer, expands their opportunities, contributes to elimination of obsolete ideological norms, and increases the potential for social adaptation, activities and self-realization.

According to the UNESCO estimates, there is a long-term positive dynamics in development of telecommunication systems. In 1995-2000 the number of phone lines in the United States increased from 165,000 to 199,000; in Germany – from 41,000 to 51,000; in China – from 41,000 to 241,000; in Russia – from 25,000 to 30,000. Meanwhile, the amount of phone lines for every 100 people increased in the United States from 63 to 72; in Germany – from 49 to 63; in China – from 3 to 19; in Russia – from 17 to 20. Investments in telecommunication sector amounted to $51 billion in the USA, $16 billion in Germany, $302 billion in China, $8 billion in Russia[1].

The number of global mobile phone users in 1997 increased from 70 million to 207 million people and by 2003 may amount to 830 million.

Swift growth of the Internet population is incredible. In 1993 this major information system of the world comprised 70,000 users, by late 2001 there will be 500 million people working with the Internet. Russian achievements are much more modest. However, one may note certain influence of information technologies on Russian economy. For instance, Russian information technology market after the 1998 financial crisis accounted for $2 billion. The number of registered users in Russia by early 2000 reached about two million people[2].

As a result, development, production and use of information technologies is expanding with tremendous pace, affecting economy in general. For instance, in the USA the costs of information components of equipment increased from 5% in 1960 to 45% in 1996. According to the US Department of Commerce, in 1998 the ICT-related industry produced $683-billion worth of goods and services. In some developed nations the share of GDP pertaining to the use of ICT amounted to 8% in 1997 and the GDP grew in this sectors by 12%. ICT account for 10-15% of global trade. Growing economic significance of ICT is partly connected with the progress of e-commerce. The profits of the latter in 1998 were about $26 billion and in the beginning of the 21st century they may exceed $1 trillion dollars[3].

ICT industry is one of the most dynamic sectors of world economy and its earnings are comparable to revenues of the fuel and energy sectors, car building, or agriculture. Scientific intensity and competitiveness of production depend on this industry.

Freedom of information activities becomes a generally recognized norm of the international law and, hence, the state's ability to limit these activities is diminishing, whereas new means of access to information develop, the role of social institutions (notably mass media) in formulation of public policy is growing.

The impact of mass media on public policymaking originates from their role of mediator between the government and the citizens, paving way to social dialogue and significance of public opinion. Free activities of mass media facilitate public control of state actions, its institutions, organs and officials. At the same time, the state uses media to explain to the citizens its goals, methods to attain them, successes and failures on this way.

Last, but not the least important thing concerning broad use of ICT in all social spheres, production and the Army is growing dependence of the state on sustainable work of information and communication systems, communication networks and security of information resources.

Errors in the work of information and communication systems may have devastating consequences. Technological gaps and mistakes may paralyze entire infrastructure of the modern society.

As the role of information systems grows, there is an increasing danger of hacking on the part of criminal groups. In 1997 the FBI investigated 200 cases of computer crime, in 1999 this number exceeded 800.

Russia also has to face a growing menace of computer crime. In the last three years the amount of registered crimes concerning computer information has increased by 63 times, the number of offenses pertaining to unauthorized access to computer information has grown by 30 times; harmful software was developed, used and distributed 137 times more; illegal production, sales and acquisition for further selling of specialized technical means for clandestine access to information occurred 75 times more often[4].

In other words, information sphere becomes an important factor for stable functioning and further development of the society. Mankind has reached the qualitative threshold of the Information Society. It seems to be a new stage of social development, when information and knowledge make the object of work and information technologies serve as a tool. This enables people to fulfill their potential and realize their aspirations. New economic, cultural and social standards will be formed depending on the level of informatization and the degree of integration in global community. In 2000 G-8 summit adopted the Okinawa Charter on Global Information Society stating the principles of international cooperation in this area. They renewed their commitment to the principle of inclusion: everyone, everywhere should be enabled to participate in and no one should be excluded from the benefits of the global information society[5].

In information society survival, economic prosperity, realization of social and political values are more connected with the development of the information sphere and neutralization of challenges pertaining to increasing vulnerability of the society and production to sustainable functioning of information systems.

Meanwhile, information infrastructure and information resources become the arena for inter-state rivalry. A substantial threat is posed by development of means for affecting coercively ICT infrastructure, for unauthorized access to information and communication resources. Such notions as information warfare, information rivalry, information operation, etc. are widely used, albeit they are yet to be defined by the international law.

A significant particularity of information society is shrinking of information distances (the time required for access to certain data). This may also lead to new opportunities for personal and social development and fulfillment of potential. Mankind reaches the line when information infrastructure will become the main source of information for people affecting their psychic activities and forming social behavior.

Complexity of modern ICT is critical for growing inter-personal dependence, especially among developers of these technologies creating algorithms for searching and retrieving information, its processing and presenting in user-friendly form. In fact, these people form the information background for the society and individuals and determine terms of their living. This is why it is extremely important to ensure security and safety of personal interaction with information infrastructure.

Another perilous source of threats to the interests of mankind is abuse of personal data collected by the state, as well as expanding of opportunities for secret gathering of sensitive and highly personal information about private life and family.

New challenges emerge as information systems and communication networks become more and more complex and crucial for public infrastructure. These may be deliberate errors or unintended faults, errors in hardware and software, harmful impact of criminal elements, etc.

One the most dangerous type of threats relate to enlarging scale of domestic and international computer crime, including fraudulent operations with information and communication systems; money-laundering; hacking of financial, bank and other data.

One should also note among menaces the uncontrolled proliferation of cyber weapons and arms race in this area, as well as information warfare. Their destructive effect may be more powerful and devastating in the information society than we expect today.

According to the Okinawa Charter, 'it is up to governments to create a predictable, transparent and non-discriminatory policy and regulatory environment necessary for the information society.' We believe that this principle should also relate to security of the technological basis of the information society. G-8 leaders, who signed the document, reiterated the need to develop effective national and international strategies for forming the information society, 'to fight abuses that undermine the integrity of the network', 'to foster crime-free and secure cyberspace', to seek urgent policy responses to hacking and viruses. This will help to create an efficient system of international information security, to reduce the risk of transforming information sphere into the scene for inter-state rivalry due to political contradictions.

One may specify few key directions of preparatory activities to establish the international information security system:

- improving national legislation regulating information sphere and strengthening international agreements containing responses to security challenges for the information society;
- enhancing capabilities of law-enforcement and judiciary at national and international level to ensure legal interests of the citizens, society and the state in the information sphere;

- fostering technological support to information security, including data protection means, investigations and legal norms for the investigations;
- advancing the training system to maintain efficiently information security;
- developing the system of cultural and educational support to information security activities.

INFORMATION SECURITY AND INTERNATIONAL POLITICS

As the information society develops, global balance of power depends on the ability to introduce highly efficient information systems and technologies in economic, military, technological, and cultural spheres.

The 20th century is known as a period of dramatic changes concerning scientific and technological development. The multiplying effect of inventions in the area of information and communication becomes more and more obvious. Emergence of the global cyberspace is one of the major factors in the development of modern civilization, for it encourages:

- further scientific, technological, economic, social and cultural development, benefiting from increasing amount and speed of information exchange regardless of distances, possibility to disseminate new ideas and knowledge, including scientific and technological achievements;
- development of new social concept based on recognition of unity and variety of the world and understanding of commonality of global problems;
- global integration;
- creation of conditions for development and introduction of new methods to enhance national security;
- progress in political, economic, production management and military command and control.

The level of information, transport and technological infrastructure determines country's role in world affairs in globalization era. They all depend on ICT that attract investments and speed up economic and social development. Post-Cold War global politics is quite contradictory. On the one hand, technological and economic interdependence grows, partly thanks to global cyberspace. On the other hand, inter-state contradictions, source of international instability and conflict exist and even aggravate in some Third World countries. Ways and methods of inter-state

[1] World Communication and Information Report 1999-2000. Polpred ASBM: 5-900034-10-0. Paris, UNESCO, 2001.

[2] Commentary to the Russian Edition of the Global Information and Communication Report 1999-2000. Polpred ASBM: 5-900034-10-0. Paris, UNESCO, 2001.

[3] World Communication and Information Report 1999-2000. Polpred ASBM: 5-900034-10-0. Paris, UNESCO, 2001.

[4] I. Yegorov, "Rules of the game for all mass media should be the same". Interview with Gennady Yemelyanov, Department Head of the Russian Security Council, February 2001, www.strana.ru

[5] Okinawa Charter on Global Information Society. G-8 Summit Documents, Okinawa, July 22, 2000.

confrontation are being transformed under the influence of new ICT.

Informatization results in a number of negative consequences, such as increasing polarization of the world, growing gap between the rich and the poor, technologically backward and advanced states. There are more pariah states and collapsed states. All this leads to instability and conflicts that may expand to the global scale. Military might of technological advanced states is sharply being enhanced, changing global and regional balance of power. States that lag behind may seriously be concerned and even irritated by this progress; hence, the animosity will lead to the emergence of new hotbeds of confrontation.

In other words, informatization does not only promote global development, but also poses new threats to national, regional and world security.

ICT cause dramatic changes in military sphere. They enhance combat capabilities of traditional arms and materiel, intelligence and communication. New generation arms have more accuracy, range, and power. ICT facilitate the processing of large amounts of data. All this enables the Army to assume new methods of command and control of personnel and military equipment at strategic and tactical levels. ICT enhance capabilities of electronic warfare means and serve as a basis for cyber weapons. This leads not only to changing forms and methods of conducting operations, but transforms entire traditional paradigm of warfare, including the mechanism of armed conflict escalation. Some experts presume that even selective use of cyber weapons against military and civilian information infrastructure may help to win in the conflict at the early stage, before the large-scale hostilities. Ownership of such weapons increases the superiority of *haves* over *have-nots*. In the near future information and psychological factors may become more crucial than nuclear ones. Information weapons, like nuclear arms, may serve to exert political pressure and to deter the aggression.

Development of cyber weapons and preparations for cyber warfare generally coincide with the vision of developed world concerning the objectives, terms, forms, and consequences of the use of force.

Strong civil society executing public control over the state has promoted a new system of values, whose core is human life, rights and security. Civil society becomes stronger (and this process seems irreversible) in many parts of the world. It cannot stand military solutions to contradictions and huge casualties, if only it is not a matter of national emergency and survival of the nation and the state. Developments of the recent decade indicate that the level of acceptable casualties for democratic countries is dozens, or even a few lives. This is the most significant factor making the state refrain from the use of force.

Globalization, including growing convergence of economic and political interests of developed democratic countries, rules out the possibility of armed conflict among them. Their common interests demand for reliable security of each member of the club and for the concerted possible solutions to urgent international problems, sometimes with the use of force. This task is often carried out by military alliances of these nations and decisions are taken by consensus, taking into account strong public opinion. This limits their opportunity to conduct combat operations, if their security is not directly affected. Major solutions to global issues nowadays are international economic and political sanctions and the use of force in case of extraordinary events and only with low casualties. Under these circumstances, cyber weapons may become an efficient combat means to act in conflict situations without employing traditional arms.

Meanwhile, industrial, military and information infrastructure of developed nations becomes more and more vulnerable. Their destruction or malfunctioning may result in enormous technological and economic disasters, for major facilities are managed with the use of ICT.

All this determines the scale and terms of use of force by developed nations and probable types of acceptable conflicts. For instance, one can rule out the possibility of nuclear warfare, for the level of unacceptable damage for the USA in nuclear war is when a low-yield warhead hits any large city. It would be difficult to wage a large-scale non-nuclear war, if the enemy is capable of resisting the aggressor and inflict large casualties. Nowadays there are no political or economic reasons for the West to start the war that may threaten its economic thriving and prosperous and safe life of population in Western countries.

In other words, preventive use of military force by developed nations is possible only if they have overwhelming military and technological superiority over the enemy, whereas cyber weapons become more and more attractive combat means.

Global informatization makes modern society quite vulnerable to terrorist organizations, criminal groups and other malefactors. There is a need for negotiating coherent concerted global strategy to fight against cyber terrorism. The strategy should clearly identify powers of national law-enforcement agencies. It should rely on public compromise, be transparent and should exclude any monopoly of individual agencies.

NEW SECURITY CHALLENGES IN THE INFORMATION AGE

Crime and Information

ICT, as any other scientific achievement, are often used for criminal purposes. One of such abuses is unauthorized access to confidential information, money, tax dodging, etc. The number of computer crimes has recently been skyrocketing, due to availability of hardware and software, skills and knowledge. Cyber crime becomes one of the new sources of threat to business, including Russia.

The most notorious criminals in information sphere are hackers. Their ability to work freely with cyberspace is some sort of compensation for certain social isolation. Hacking often takes place without malicious intent, is caused by perverted self-esteem, desire to be respected by peers, or is committed with hooligan intentions. Hackers try to overcome their inferiority complexes and challenge the society. According to some surveys, most of the hackers are young people at the age of 20 or so having difficulties with inter-personal communication. They are normally bad students in school, but succeed in computing, thanks to self-education, patience and maniacal love to computer technologies. They often like anarchism, treating it as a freedom of actions in cyberspace. This sometimes leads hackers to aggression and may induce them to conduct terrorist acts of national and international scale.

At present, hackers are normally united in groups, exchange their knowledge and information. This enables them to use more and more powerful information resources. Groups may bring together all kinds of specialists: those who know weak points of certain operational systems, protection means, network protocols, etc.

Hackers are often ordered to commit certain crime. Criminal groups realize that without advanced information technologies one cannot obtain required data or money. Besides, computer crimes normally leave less evidence and are not highly time-consuming and expensive. This makes them a useful tool in the hands of criminals. This is why the latter study computer technologies, hire experts and pay them high salaries, exploiting leftist, anarchic, and other extremist views.

About 40% of computer crimes deal with obtaining access to confidential information, for management, banking and commerce widely use computers nowadays, hence, accumulating large amounts of information, sometimes with restricted access and valuable for the criminals. The victims of such crimes are normally databanks and databases, computer networks of governmental bodies at national, regional, and local levels, and personal data. As a rule, these actions make part of the industrial espionage.

Less visible part of the iceberg of computer crime is modification and deleting of valuable information. Criminals get access to information networks of banks and other organizations in order to manipulate finances. Another example is modification of fiscal information in cash registers. This helps criminals to hide enormous amount of money from taxation. Some swindlers hack computers of the Internet service providers (ISP) and mobile phone operators. Access to computer information of mobile phone providers is gained with the use of *cloned phones*. As a result, they obtain the opportunity to work with the Internet or to talk for free and inflict significant damage to ISPs, to operators and regular users.

Computer crime requires specially designed software. Development, use and distribution of such harmful programs is a crime by itself. The most notorious kinds of software are viruses that may replicate themselves and disseminate their own copies and often perform destructive functions. The scale detriment can be realized at the example of "*I love you*" bug. For example, only in the UK during one day of dissemination the virus disrupted work of three million employees. It paralyzed the work of *Barclay's*, *National Westminster*, *Virgin* air company, *Sky Network* TV company, the *Times* and the *Sun*. Many telecom companies could not function. The virus attacked electronic networks belonging to the Scotland Yard and the UK Parliament.

Information is also decisive for normal functioning of governmental agencies and it is a vulnerable link in the national infrastructure. According to Russian and foreign analysts, this creates prerequisites for the emergence of cyber terrorism phenomenon. As it was mentioned in 2000 by Richard Clark, who coordinated counter-terrorist and security activities in the residence of the US President, electronic Pearl Harbor was not a theory, it was a reality[1]. Louis Freeh, Director of the FBI, noted the threat of cyber terrorism for any country, which had banking, transportation, energy systems and whose government and private sector relied on computer networks and quick access to the Internet-technologies, such as the United States or Russia. He emphasized that if electricity nets in Russia or in the USA were switched off in mid-winter, this would be more devastating than any terrorist act of the past[2]. Russian officials are also concerned about these issues.

As a rule, cyber terrorism means activities or threats of activities aimed at disrupting computer systems and leading to the risk of death, substantial material losses and other socially dangerous consequences, if they are carried out in order to undermine public safety, intimidate population or exert pressure on decision-making by authorities.

Major goal of the terrorists is to make their act widely known and to have reaction of the public opinion. In other cases, the criminals may not put forward any claims and act anonymously for revenge, intimidation, or destabilization. However, the particularity of cyber terrorism, as a new form of terrorism, is the use of different ways for interim or permanent disruption of information infrastructure of the state or its elements, as well as in using this very infrastructure to inflict damage to the society, state, or individuals.

As other forms of terrorism, cyber terrorism implies the use of violence or threat of violence to coerce the political leadership to perform political, economic, religious, or ideological tasks. Terrorists also benefit from emotional impact on public opinion instigating fear, panic, loss of confidence in the authorities and, in the long run, political instability.

Cyber terrorism is different from other forms of destructive influence on information systems due to its goals, which are characteristic of political terrorism in general. The methods of cyber terrorists may include all types of modern cyber weapons. However, its tactics is substantially different from information warfare and cyber crime.

Cyber terrorist activities comprise:

- inflicting damage to certain physical elements of information systems and networks, e.g. disruption of power supply, jamming, use of special software to facilitate the destruction of hardware, biological and chemical means to destroy hardware;
- theft or destruction of information, software and technical resources by penetrating security systems, implanting viruses, bugs, etc.
- effect on software and information for the purpose of distortion or modification in the information and control systems;
- disclosure or the threat of disclosure of confidential information concerning the functioning of the information system of the state, important civilian and military codes, principles of encoding, propaganda of successful experience of cyber terrorism;
- false threat of cyber terrorist act with serious economic consequences;
- seizure of control over mass media to disseminate disinformation, gossip, to demonstrate the might of terrorist organization and to declare the demands;
- destruction or neutralization of communication lines, wrong routing, attacks on communications hubs and their overloading;
- pressure on operators, developers, maintenance workers of information and telecommunication systems (in the form of violence, threat of violence, blackmail, bribery, injection of drugs and other substances, creating illusions and multimedia to insert information in sub-consciousness or affect human health, etc.).

The efficiency of cyber terrorism depends on a number of factors:

- cheap and easy access to information infrastructure; terrorists may obtain it, like any other regular users;
- vague borders of information infrastructure, elimination of clear geographic, bureaucratic, legal and even conceptual limits that are traditionally connected with national security;
- possibility of manipulations with information and perception management; terrorist groups may disseminate via the Internet propagandistic materials to urge support for their activities, for disinformation, impact on public opinion, undermining public confidence in the government;
- the lack of information concerning realistic and potential challenges pertaining to cyber terrorism;
- complexity of early warning tasks and difficulties with assessing the real and probable detriment. Terrorist activities may quickly be carried out and it would be difficult, if possible, to find the terrorists, especially in crisis when there is no time for traditional investigation by law-enforcement agencies;
- difficulties with establishing and maintaining coalitions in international cooperation. When a serious cyber terrorist act takes place, any alliances may not survive the pressure of information *fog*. Urgent problems pertaining to the implementation of joint plans of actions against transnational criminal or terrorist organization may emerge.

When the state intends to join global open networks, it should provide for the protection of national information networks from cyber terrorism. These measures should ensure:

- the protection of facilities that make material basis of the information infrastructure;
- normal and uninterrupted functioning of information infrastructure;
- protection of information from hacking, distortion, or destruction;
- preservation of the quality of information (timely, accurate, full, and accessible);

- development of technologies for detection of attempts to affect the information, even in open networks.

The major form of cyber terrorism is cyber attack on data, hardware, data transmission devices, or other elements of the information infrastructure conducted by groups or individuals. Such attack enables the terrorists to penetrate the system, take up control, disable the means of network data exchange, etc.

The danger of cyber terrorism lies also in the fact that such actions may be performed from any part of the world. As a rule, it is extremely difficult to find the terrorist, for it uses dummy computers; he and his location can hardly be identified.

Cyber terrorism may be targeted at civilian and military facilities. According to US experts, the most vulnerable systems are energy, telecommunications, flying control units, electronic finance, governmental information systems and computer command and control systems. For instance, as far as nuclear energy sector is concerned, change of data or blockade of information centers may lead to nuclear disaster or power cuts in cities and at military facilities. Similar activities in financial sphere may result in economic crisis, while malfunctioning of command and control infrastructure may have unpredictable implications.

There is also a direct dependence between the level of information infrastructure and computerization of the country and the number of cyber terrorist acts. At present, cyber terrorism poses real and growing threat to leading computerized powers. For instance, in November 1994 the work of intranet of *General Electric* and *NBC* was disrupted for several hours. The organization responsible for this is called the *Internet Liberation Front*, which declared cyber war to these companies.

According to the UK media, in early 1999 hackers managed to gain control of military telecom satellite of the *Sky Net* series and to change its orbit. Special police unit launched investigation, for hackers wanted a ransom for leaving the satellite alone. Their demands were sent to the British authorities from a number of locations abroad. Several weeks after the British agencies reluctantly admitted the fact of penetration to the reserve command point and interfered the work of the satellite.

Until recently Russia's information infrastructure has not been extremely vulnerable to cyber terrorism. It has been accounted for by low level of its development, substantial amount of non-computer operations relating to control systems. At the same time, in the recent years many state and commercial structures, including the so-called natural monopolies, have started to reequip the production and management. This policy is mostly based on foreign hardware and software and, hence, is more vulnerable to cyber attacks. Sometimes buyers economize on minimal security and safety requirements.

ICT is widely used by terrorists to promote their activities and to recruit new members. Nowadays the Internet contains Web sites of nearly all more or less large Islamic organizations, including followers of radical Islamism. Besides, the Internet is used by radical groups, as means of communication. Analysts of the Israeli counter-intelligence service assume that terrorists use e-mail to transfer encoded instructions, maps, schemes, passwords, etc. Experts speak about international Islamic organization of new type, which relies on single information environment rather than on clear organizational ties[3].

One of the latest developments is cyber nuclear blackmail. In early 1999 the governments of more than 20 countries (the USA, the UK, Israel, Austria, etc.) received e-mails allegedly signed by Russian officers serving in the missile unit in Kozelsk (the Kaluga region) and armed with strategic missiles. The letters argued that the officers were discontent with degrading position of Russia and threatened to launch missiles against targets in the capitals and industrial centers of Western nations. To avoid this option, the terrorists claimed a large sum of money. The governments under psychological attack addressed the Russian Foreign Ministry, expressed their concerns and asked for assistance in finding blackmailers. The FSB conducted an investigation and detained two inhabitants of Kaluga, who were not military. The court found them guilty of making the notification of false terrorist act[4].

Thus, the challenge of cyber terrorism is an urgent problem and its danger will grow, as the ICT spread. The developed countries take measures to resist cyber terrorist activities.

As for computer crimes, they are normally latent and take place in the Internet beyond any borders. Many victims do not often know that they have suffered from swindlers. Sometimes the victims do not turn to the law-enforcement agencies for help in order to avoid detriment to their reputation (notably large financial and governmental entities).

A matter of particular concern is dissemination of knowledge and practical recommendations on subversive activities and development of weapons, including WMD, in the Internet.

Illicit trafficking in intellectual property is a source of large economic losses. According to Russian and foreign experts, the turnover of this trade is billions of dollars, whereas the profits amount to hundreds of percents. These activities affect the state and the right owners, as well as rank-and-file consumers of this production. The turnover of intellectual property stored in electronic form amounts to dozens of millions of copies. 70-80% of them are illicit in violation of legal property rights and are not levied with taxes.

Illicit trafficking in specialized electronic systems, radio-technical and other devices means sales of products that are not supposed to be widely distributed. Special technical equipment are normally used by secret services. The scale of economic damage in this sphere is determined by the level of danger to public. Meanwhile, the use of such devices may interfere with the work of traffic control systems of any kind of transport (aircraft, vehicles, ships, or railroads). Illegal communication means produce jamming for communication channels of law-enforcement agencies, emergence and rescue services, etc. Illicit trafficking in specialized electronic devices can be compared with the illicit trafficking in electronic intellectual property, as far as the turnover is concerned.

Unauthorized access to confidential and commercial information through public telecom networks is a multi-facet phenomenon. Security arrangements for the first analogue mobile phone networks were at a very low level. The systems lacked encoding, as in voice line, and had no mechanisms for authentication of users. Hence, they were more vulnerable to bugging and *phone cloning*. As analogue systems were replaced by digital standards (*GSM*), the type of access was changing and it became more and more difficult for the violators to clone phones and intercept data. Technical access without authorization was replaced by procedural and contractual fraud.

Experts assume that such criminal activities affecting mobile communication networks resulted in more than $25-billion losses. Therefore, it is very important for operators to ensure detection, prosecution, and prevention of such acts. To solve this problem one has to take additional security measures. Different types of unauthorized access have small distinctive features impeding concerted efforts of operators and criminal justice to analyze the methods of penetration and swindle. Besides, the very notion of computer and telecom network fraud does not yet exist and recognized.

To put it simple, fraud related to mobile phone networks can be defined as illegal activities enabling the violators to obtain access to communication services without appropriate payment. At the same time, the difference between fraud and legal behavior often very small in practice. One may, however, identify four major type of unauthorized access to telecom networks.

Firstly, it is fraud with the use of the contract. There are two subtypes: the contract may be signed without the intention to pay for the services, or the users, who are parties to the contract, decide not to pay for the service some time after signing the contract. The second subtype is when swindlers use a legally obtained discount fee and buy several phone lines connected to these preferential services.

Secondly, it is *phreaker* access, when the criminals penetrate ill-secured system and use (sometimes sell) its capabilities.

Thirdly, one should speak about technical access, mostly including attacks against technologically weak sections of the mobile phone systems. Vivid examples are phone cloning and intra-corporate technical fraud. During cloning the parameters of the authentic phone are copied into another mobile phone, whereas the operator believes that the original one (identified before) is working. As for intra-corporate activities, company employees may make some changes to internal information in order to gain access to services with discount or at low price. The attack against the automated phone station implies the devices to replace the user number. False pulse is sent in response to the identification request from the phone station, enabling the swindler to access automatically and for free (as a service of the network) international and long-distance calls.

Fourthly, it is procedural access. These are attacks on procedural algorithms designated to lessen the risk of swindle, i.e. weak points of the billing system and business procedures used to access the system.

Taking into account real technological capabilities, nowadays only a few percent of cloned phones and telecom centers are being discovered. The flaws in legislation often do not allow for adequate measures against offenders. The danger of these crimes is constantly growing. One of the major tasks of the criminal community is to get secret and unauthorized access to public and state radio and phone systems in order to obtain confidential information for criminal purposes.

Information Security in Business

The competitiveness, efficient functioning and management, and, finally, survival of the company depends on the quality of information, its adequacy, accuracy, and credibility. Besides, activities of the company depend on reliability and protection of computer systems that make the basis of its information networks.

The challenges to business information security in the *pre-computer* era were as follows:

- industrial and economic espionage;
- loss of documents due to theft, fire, or other disasters and emergencies;
- carelessness, ill-competence, or malicious intent of the employees.

Traditional systems of paper document storage made losses of data irreparable in case of fire or other emergencies and forced companies to suspend or stop their activities. Ill-competence, carelessness, or malicious intent of the employees could lead to losses of documents, distortion of information, errors in reporting.

Business entities are doomed to develop information systems, for they are crucial for normal business development. To ensure security of data, it may be encoded, different categories of personnel may have differential access, etc. To avoid irreparable losses of data, it may be stored electronically, as reserve copies, in different locations. Good system of logical control have emerged and seriously reduced the amount of errors by employees. However, new technologies also make the systems more vulnerable.

To maintain security of the automated information systems, one should comply with the number of rules mentioned below:

- to place orders for the development of information systems and sub-systems to companies that are licensed by the appropriate authorities dealing with information security issues;
- to purchase properly certified devices;
- to assess the planning project decisions and devices from the point of information security;
- to evaluate challenges and risks concerning implementation of the projects;
- to develop and fulfill the security policy, including appropriate normative documents;
- to ensure the use of data protection systems in order to avoid unauthorized access.

As far as the operation of the information systems is concerned, the comprehensive information security system should be established in order to accomplish the following tasks:

- control of functioning of the information security sub-system;
- non-stop security monitoring and registration of interference attempts;
- analysis and investigation on the facts of security violation;
- study of the known models of hacker attacks, analysis of the capabilities for their implementation, taking measures to eliminate such capabilities;
- anti-virus protection of the computers;
- monitoring of possible threats of the information security violation;
- security risk management and insurance from these risks;
- personnel management in information security area.

One of the most important parts of information security management in business is the analysis of threats and elaboration of measures to prevent or respond to such risks, minimizing the scale of damage.

Business information security challenges may be divided into the following categories:

- leakage of information via the channels that do not involve the information systems;
- unauthorized access to the resources of the system without telecom access;
- hacking through telecom networks;
- threats to the systems of electronic documentation and payment;
- information security threats that are not caused by unauthorized access to data.

The analysis of threats and the level of danger implies that their impact on availability, confidentiality and coherence of information should be assessed. Company leadership should set the priorities and decide on adequate measures to be taken. A normal practice nowadays is to insure against risks of information security violation.

In Russia the business information security does not only depend on specific practices of the companies, but is also affected by a broad range of external factors and general problems of the country. The state plays a special role in these activities, as the Information Security Doctrine indicates. The document contains nearly the entire spectrum of tasks to be performed in order to secure normal conditions for business development in Russia. Now it is the matter of taking specific decisions and their practical implementation.

Security of Open Information Systems

In practice, information security is connected with data transmission via information and telecom networks. Security of closed systems may successfully be ensured, whereas open networks are more vulnerable and difficult to protect. Moreover, the task of protecting open networks is often the most decisive element of the information security activities.

Open information systems:

- are open to the public, i.e. their use does not require from the user any affiliation with the specific community;
- provide for information interaction with other systems;
- maintain information exchange without any restrictions and distortion of transmitted data;
- use coherent and approved complex of protocols and data presenting formats, encouraging exchange of different types of information (text, sound, pictures, video, etc.).

Development of open information systems has also some negative consequences. One of them is the growing number of challenges and risks to facilities and information resources connected to the system. Integrity, credibility, availability and confidentiality of data may be affected by penetrating the net, or organizing the leakage of information; this may be achieved by penetrating the computers or networks of users via the open information system. In the first case, it is the matter of protecting the integrity of the net, in the second case – protecting the users from being hacked via the net. Moreover, open character of the network enables the hackers to penetrate it from abroad. Hence, there is a need for international norms and regulations to ensure the information security of the global net.

It is noteworthy that the criminal acts against open networks become a common place and this demands from users the most efficient employment of known methods and means of information protection, especially when it comes to financial and trade activities.

During cyber wars the open networks may be used as the major field for the use of cyber weapons to penetrate the national telecom infrastructure of the enemy and destroy his command and control system, as well as the infrastructure itself.

At present, national open network architecture does not provide for guaranteed security of data. The information from the Internet or sent to the Internet may be distorted, disclosed, forfeited, read and disseminated without notification of authors. As a result, the Internet may become a global mechanism for disinformation, compromise data, and machinations. Uncontrolled use of the encoding devices may make the Internet become an ideal medium for criminal information exchange. It is necessary to ensure that the all law-abiding users have access to safe and secure exchange of information. If such medium emerges, this would ensure authorized access to any electronic information, reduce costs of data protection for companies, enable them not to install their own expensive data protection systems. Nowadays, it may be achieved by improving the data protection infrastructure in open networks. There is rich experience in this area, albeit the ideal system is yet to be developed.

Protection of information in open networks implies that their users should be able to use standard and safe cryptographic algorithms. Hence, there must exist the infrastructure ensuring this security to the users and the state.

At present, Russia and other countries have not yet realized the need for comprehensive systematic approach to the problems of information security in open networks. There are some interim solutions, which cannot be regarded as a long-term way out.

The importance of maintaining security of the open networks is pre-determined by two factors. Firstly, they are global and have no governing body that may take appropriate security measures. Secondly, the information exchange is normally going beyond the borders and connects users, whose activities are regulated by different national legal systems. At the same time, open networks make the most vulnerable element of the international system of information exchange.

Thus, one may make the following conclusions concerning the security of open networks:

- This is a classic example of a complex task requiring systematic solution. Any attempts to solve the problem in parts will not and cannot yield any satisfactory result. This is true with respect to information security of national and global open network infrastructure.
- Within the country this task may be accomplished by forming a national medium for protecting the information exchange. This is possible only by developing the infrastructure for protection of information in open networks.
- The problem of information security of the global open network may be ensured only with close interaction of all states in formulating fundamental and mutually acceptable regulations for the international information exchange.
- The international community, authorities and public should realize the importance and complexity of joint efforts to ensure information security of open networks.

Information and Psychological Security

The Information Security Doctrine contains the term "illegal information and psychological actions". Such activities are regarded as a serious threat to individuals, public and the state, above all as a challenge for constitutional rights and freedoms of the person, his/her spiritual life and information activities, individual, group and public consciousness.

It is a matter of possible transformation of mass information and dissemination of disinformation, which may undermine social stability, be harmful to public health and safety. This may also be a propaganda of racism, social, national and religious animosity and hatred, dissemination of information about activities of totalitarian sects that advocate violence. Such information and psychological influence on individuals and social groups is constantly growing. For instance, a significant danger for psyche is dissemination of pornography and other immoral information via the Internet.

The instruments for affecting mass thinking are also being developed. Their objective is to provoke certain conflicting behavior in certain (political, military or emergency) situations. Some of the examples are to initiate panic, to convince people to surrender, to mobilize the rally to resort to violence, etc. Fine mechanisms of their implementation, benefiting from particularities of mass thinking, have been described in famous books on psychological warfare. The most vulnerable to such manipulations are marginal segments of the society, who find them under pressure of psychological influence and suffer from general poverty and disorder in their lives.

It would be useful to study the consequences of such manipulations with mass thinking. 'Negative information and psychological influence is manipulative influence on personality, its perceptions and emotional sphere, its will, on group and mass thinking, an instrument of psychological pressure for explicit or implicit inducing of individuals and social entities to act in detriment to their own interests and to the benefit of certain individuals, groups, or organizations that perform the influence.'[5]

Obviously, information and psychological influence targeted against the population or certain social groups may seriously damage normal functioning of social institutions, state structures, public organizations and associations, and individuals. This impact is regarded as negative, for it causes the psycho-emotional and socio-psychological tension, distortion of moral criteria and norms, moral and political disorientation and, as a result, inadequate behavior of certain persons, groups and masses. However, the state also often manipulates the mentality of people. It is a matter of criteria to assess the direction of manipulation. The most independent political criterion (regardless of left, right, centrist or ultra positions) is the following[6]. The democratic state is a guarantor of social rights and freedoms of people and a device to deter against possible destructive impact of corporate and private interests. One should proceed from this ideal. If information and psychological influence works against such functions and activities, it should be qualified as negative, as a threat to individual and mass thinking, typical of authoritarian and totalitarian regimes.

Information and psychological influence on individual minds may lead to two types of inter-related changes. Firstly, these are changes of psyche, a threat to psychic health of a human being. It is difficult to distinguish here between the norm and the pathology and hence, the indicator of changes would be the loss of adequate reflection of the world in one's mind and changes in one's attitude to the world. One may speak about degradation of personality, simplification of the forms of reflecting the reality and turn from high demands (self-realization, social recognition) to low demands (physiological and material). Secondly, these transformations affect values, life position, orientation and perceptions of an individual. This may lead to anti-social behavior and is dangerous for the society and the state.

In case of manipulations with mass thinking it is extremely important to take into account its trustfulness to the press and other media, readiness to perceive political and quasi-scientific myths. As far as information process is concerned, masses may be regarded as the population, the crowd and the collective. For the crowd the major sources of information are the leader and his closest aides (charismatic core), as well as the gossip and excited individuals within the crowd. For the collective, official information is more important; it comes from the officials and informal leader. There is nothing special about information impact on masses that are in normal, calm and self-assured psychological state. Less is known about particularities of information and psychological influence on masses in risky socio-psychological situations. Such conditions imply that the masses may easily break moral and legal norms and, as a result, this state of masses is quite perilous for normal functioning of the society[7].

Dynamics of this risky trend may be described in the following manner:

- the first stage is unrest of masses, dissatisfaction with the situation, articulation of common demands, understanding and acceptance of the common goal and common opinion on external threats;
- the second phase is understanding of what and when should be done to meet common demands and to overcome obstacles, or to eliminate the threat and form the group structure and general emotional mood for struggle;
- the third stage implies actions to pursue the goal with the use of legitimate information and psychological methods of influencing the rivalry;
- the fourth phase is actions with the use of illegitimate means, including the use of force;
- the fifth stage (if the goal has not been attained) is characterized by emotional decline and panic, cessation of activities, re-thinking of the program of actions and possible restructuring of the role organization within the group.

The following sources, channels and technologies are used to influence individual, group and mass consciousness:

- mass media and special means for propaganda and dissemination of information;
- global computer networks and easily distributed software for dissemination of materials in the net;
- devices for illegal modification of the information medium, which is used by the individuals for decision-making;
- instruments for creation of virtual reality;
- gossip;
- technologies of sub-critical psycho-semantic influence;
- means for generating acoustic and electromagnetic fields.

Mass media are the most efficient means for exerting information and psychological influence on large masses of people. The most dangerous aspect of the media, as many experts believe, is their ability to present the information in such a way that large masses of people may have a virtual perception of reality and believe it to be true and unbiased. However, as soon as the person starts to call into question this virtual picture of the world, the efficiency of information and psychological influence is shrinking. These doubts may be reinforced with counter-propaganda technologies also applied in the media. High efficiency of information and psychological influence of the media, notably the TV, is accounted for by the strong psychological effect of participation in the event, when a person dives into this reality. This *CNN* effect is considered by many to be the major condition for efficiency of information and psychological influence with the help of the mass media.

Special means of information and propagandistic activities are mobile radio- and TV-broadcasting centers, mobile propagandistic loudspeakers, posters, and leaflets. The technologies of their use have been developed and further progress relates to methods of influencing consciousness and sub-consciousness.

Cheap access and free dissemination and obtaining of information make the Internet be an efficient tool for using information mechanisms to influence individual and mass thinking.

Nowadays, political organizations may use the Internet for mobilization of their supporters, including emergency situations. Unregulated distribution of information in the Internet results in free spread of defamatory and incredible information, enabling to organize propagandistic campaigns.

The power of network technologies is enhanced by new multimedia and virtual reality technologies. The virtual reality is an imitation of reality and may be regarded as a tool of psychological influence on consciousness and sub-consciousness of a human being. It involves the person into the new forms of existence and, to a certain extent, may form a personality. New forms of indirect social control may also emerge and be based on hidden manipulations of mind, soft suppression of psyche, and changes in the structure of personality.

Rumors also play important part in psychological manipulations. They are an indispensable element of informal communication and present unverified data of unknown origin transmitted in the process of inter-personal communication. Gossip performs some significant social functions. Rumors help to identify an individual in the society and increase the homogeneity of opinions within the group. Inter-group discussion on gossip helps to find a common viewpoint.

Rumors are sometimes decisive for inter-group, inter-ethnic and international conflicts. In many cases the warring parties lack the possibility of affecting each other due to legislation and public opinion. Besides, the outcome of the conflict is often a legitimate solution consolidating consensus (elections, referendum, etc.). In this connection, the importance of techniques aimed at changing the perception of the majority to the benefit of one of the conflicting parties is growing. Such transformations may be achieved by disseminating specially selected data via the mass media and channels of informal communication. In comparison with the media, the use of informal communication is even preferable, for there is no information about the author. This anonymity diminishes suspicions of political engagement of the gossip and promotes its efficiency.

Widening spread of new means for affecting the mind sets up the task of its protection from destructive influence. The methods of psychological protection of an individual and his protection from information and psychological influence do not always coincide. The aim of the protection is to lessen emotional tension threatening the individual. As for protection from information and psychological influence, one has to think about preserving basic characteristics of psyche and spiritual development, individuality, values, moral criteria, intelligence, etc. The leading theoretical mechanism of protection is intellectualization. Only deep analysis of the information situation (if other characteristics of the person are high) enables the individual to reveal the manipulating character of information and psychological influence, assess the credibility of information and work out the most acceptable forms of protection from undesirable consequences. It is noteworthy that the inherent protection features of personality are formed during human life and make a mixture of experience, education and self-education.

It is more difficult to protect masses. Naturally, the more individuals with good personal protection it comprises, the more stable it will be. Meanwhile, the society should have a high positive self-identity of "we" and be low susceptible and not easily *infected* (unlike the crowd)[8]. This positive image of "we" is formed on the basis of self-identity and people's desire to identify them with certain social environment. Self-identification is always a political factor.

However, not all information and psychological influences are dangerous. Moreover, some of them may be useful to raise the sustainability of population, as far as destructive information and psychological impacts are concerned, to enhance the psychological potential of the population. Such forms of psychological influence are aimed at strengthening the social character, political mobilization of the society to overcome common difficulties, such as war, natural disasters, etc.

[1] *Interfax*, June 20, 2000.

[2] *ITAR-TASS*, February 21, 2000.

[3] *NG-Religii*, No. 3/3, April 7, 1999.

[4] *Trud*, July 7, 2000.

[5] V. Anosov, V. Lepsky, "Prerequisites for Information and Psychological Security". In: A. Brushlinsky, V. Lepsky (eds.), *Problems of Information and Psychological Security*. M., 1996, pp. 7-11.

[6] See, for example, Y. Sherkovin, *Psychological Problems of Mass Information Processes*. M., 1973; G. Schiller, *Manipulators of Mind*. M., 1980.

[7] G. Zarkovsky, N. Avdeyeva, G. Stepanova, "Socio-Psychological Consequences of Global Changes in the Environment". *Chelovek*, No. 3, 1995, pp. 97-104.

[8] S. Moscovichi, *The Age of Crowds. Historical Treatise on Mass Psychology*. M., 1996.

23

CYBER WEAPONS AS NEW MEANS OF COMBAT

Cyber Weapons – A Product of New Information Technologies

The use of ICT changes not only the combat means, but also the strategy and tactics of modern warfare. New concepts of warfare in the information age have emerged and they take into account new factors of vulnerability of the parties. If in the past one could compensate for the lack of tactical information with the use of additional force, nowadays information superiority predetermines the outcome of the modern short-term armed conflict.

The efficiency of the modern arms depends on the capabilities of computer control and communication systems. There is a wide range of methods and devices to influence these systems by disrupting the work of certain elements, key operators or by manipulating with information. The conflict may not even transform into armed struggle and may finish after the stage of information struggle, when one of the parties realizes that it may no longer rely on efficient use of its arms. Anyway, the party that has better knowledge of tactics and strategy of warfare in the cyberspace will have significant advantages.

Cyber weapons include different types of arms: high-precision systems to destroy command and control structures and some electronic means; electronic warfare systems; sources of powerful electromagnetic pulse; software viruses, etc. The criterion for defining certain systems as cyber weapons is the possibility of their employment in cyber warfare missions.

Offensive with the use of cyber weapons may be conducted independently or in interaction with traditional offensive, before it or supporting it. Any cyber attack is aimed at ensuring information superiority in the course of the conflict by affecting the data collection, processing and storage systems, as well as by influencing the personnel responsible for decision-making and maintenance of equipment. According to the US specialists, a substantial threat is the expanding access of some nations to space intelligence (digital maps) with the resolution of five meters and less. Such resolution enables the party to identify key elements of the enemy infrastructure and target cruise and ballistic missiles at them, especially employing global positioning system (GPS).

The high-speed transmission of a large amount of information becomes the most crucial task in the process of developing advanced command and control systems. The solution to the problem are space communications and wide use of fiber-optic lines. At the same time, these components of information infrastructure become the most vulnerable to cyber attacks. Concentration of resources within the limited number of infrastructure units results in vulnerability of entire system, if appropriate offensive means are available. However, even destruction of the large number of elements of information infrastructure may reduce the efficiency of information processes only for a short period of time. Deliberate accomplishment of such missions is a priority task, when cyber weapons are used to perform an offensive and to secure domination over the enemy.

Classification of Cyber Weapons

At present, there is neither established classification of cyber weapons, nor clear definition of this term. Normally, cyber weapons are those that efficiently pursue the objectives of cyber warfare. Cyber weapons should also facilitate achieving of military superiority, excluding massive casualties and relying on high-precision and hidden non-lethal methods of influence.

In accordance with their purposes, cyber weapons are divided into offensive and defensive. Defensive cyber weapons are systems of multi-layer computer security and various systems for active resistance to enemy cyber weapons. Offensive arms are designated for destroying critical elements that support decision-making. The organization of decision-making contains the points and bodies for command and control, the system of automation of control, communication, specialized systems for collection and processing of intelligence data, sensors. The efficiency of such territorially distributed system may be diminished by affecting its structure or its resources:

hardware, software, information, communication, or personnel.

In theory, the following types of cyber weapons may be named (table 1):

- means of highly accurate positioning of equipment with electromagnetic radiation and of its destruction by prompt detection of the elements of the information system of command and control, identification, guidance and destruction;
- means to affect the components of electronic equipment and their power elements for interim or irreversible disruption of electronic systems;
- means to impact electronic operational modules, for their destruction or changes in the algorithm of their work by using special software;
- means to influence the process of information transmission aimed at disorganizing the functioning of sub-systems of information exchange by affecting the medium for the spread of signal or the working algorithms;
- propagandistic and disinformation means used to make changes to the data of the command and control systems; creation of virtual reality; changes in the system of values of a person; inflicting damage to moral and spiritual life of the enemy population;
- psychological weapons to affect the psyche and sub-consciousness of a human being and to suppress his will and activity.

This classification can hardly cover all possible cyber weapons that may emerge in the future. However, the results of all known practical research and development activities that are under way have been included in this classification.

According to the type of influence, cyber weapons may be divided into three categories: weapons based on information technologies, weapons of energy and chemical effect.

The examples of energy weapons are:

- high-precision self-guiding munitions, including specialized cruise missiles and attack unmanned aircraft;
- means for forced electronic suppression, powerful high-frequency generators, means that employ electricity grid for destruction;
- land-based and air-based electronic warfare systems, disposable jamming transmitters;
- specialized radiation generators affecting human psyche.

Examples of cyber warfare based on chemical effects are munitions armed with gases, aerosols or biological cultures destroying the components of electronic hardware; specialized pharmacological means for psychological influence that have negative impact on human psyche.

The most promising devices are that based on information technologies. IT make an integral part of high-precision weapons, for their guidance is ensured by positioning and intelligence systems. This is why these sub-systems should be regarded as cyber weapons as well.

Table 1 contains the classification of cyber weapons by type and sorts. This division into types is quite relative, for cyber weapons will be employed in complex in real hostilities and are being developed as a semi-automated set of different means requiring specially trained personnel.

Destruction of communication means requires highly accurate guidance involving radio and radio-technical intelligence. At present, land-based and air-based systems of radio and radio-technical intelligence that are operational in the range of 0.5 GHz and more, have the positioning accuracy amounting to 0.06-0.1% of distance. The range of intelligence is nearly equal to the range of direct visibility of aircraft and is 30-35 km for ground surveillance systems. Such accuracy is sufficient for target designation of artillery and aircraft. To enhance the range and accuracy of targeting, multi-position land-based and air-based positioning systems are being developed. These systems should locate the electronic systems with accuracy sufficient to target high-precision weapons. Later the position of these targets may be specified with the help of visual, radar and other decamouflaging characteristics. High-precision weapons employed against communication systems may be guided by their emanation, by high-frequency emanations and correspondent thermal radiation. New cyber weapons (non-nuclear generators for electromagnetic pulse, bombs with current-conductive fiber, etc.) are being designed to destroy computers and power systems.

Table 1. Classification of Cyber Weapons

Kinds of cyber weapons	Mission	Possible types of cyber weapons	
		On the basis of energy and chemical principles	On the basis of IT
The means for highly accurate positioning of equipment with electromagnetic emanation and for its destruction with firepower	Prompt detection of certain elements of the information system, their identification, targeting and destruction	Self-guiding high-precision munitions used against communication means. High-precision weapons, whose target designation and orientation depends on highly accurate navigation system	The devices for highly accurate positioning (including coherent sources). Reconnaissance means using radar, visual and other decamouflaging characteristics.
The means to affect components of electronic equipment and their power supply systems	Temporary or irreversible disruption of the work of certain components of the electronic systems	Means of electronic suppression: powerful high-frequency generators (gyrotons, reflective triodes, relativist magnetrons, tubutrones); explosive magnetic generators; explosive magnetic and hydrodynamic generators. Means of influence through the electricity grid. Means to disrupt the functioning of electricity grids.	Software means for damaging the equipment (resonance of heads of hard disks, burning of screens, etc.). Software to delete records. Software to influence power supplies, etc.
The means to affect software of electronic control modules	Disruption in the work of algorithms of the control systems with the use of specialized software		Means to penetrate the information protection systems. Means to penetrate the information networks of the enemy. Means to disguise sources of information. Means to disrupt the functioning of system's software at certain point of time or in case of specific event. Means for hidden partial changes in the algorithms of software. Means for collection of data circulating in the information system of the enemy. Means for delivery and insertion of certain algorithms in specific place

			within the information system. Means of affecting security systems of the facilities.
Means of influencing the data transmission process	Disorganization of the subsystems of information exchange by affecting the medium for spread of signals and the functioning algorithms	Electronic warfare means, especially land-based, air-based (helicopters and unmanned aircraft), stations for jamming (probably with elements of artificial intelligence). Disposable jamming devices	Means to affect data transfer protocols of the communication systems. Means to affect algorithms of addressing and routing. Means for interception of information, impediment of its transmission. Means for overloading the system with false queries.
Means of psychological influence, propaganda and disinformation	Making changes in the information of the command and control systems, creation of the virtual reality different from actual reality, changes in the system of human values, damage to spiritual and moral life of the enemy population		IT of the mass media, propaganda, labeling. Means to develop or modify the virtual reality. Means for voice imitation of operators (e.g. air traffic operators) and manipulation with visual images (leaders of parties and states). Means for modification of information stored in enemy's databases. Means of inserting false information in the enemy information systems (e.g. target designation or delivery of supplies). Means for the deception of security systems Means for modification of navigation data, data of the meteorological systems, exact time systems, etc.
Psychotrone weapons	Influence on psyche and sub-consciousness of a human being in order to suppress his will and ensure incapacity.	Psycho-pharmacological means, Psycho-dyspeptic. Sedatives. Antidepressants. Hallucinogens. Narcotics. Drugs with special structure. Special generation of emanation affecting human psyche.	Special video, graphic and TV information (25th image, increase of blood pressure, provocation of epilepsy, etc.). Means for creating virtual reality suppressing the will and intimidating (projecting of the "God" image on the sky, etc.)

The use of advanced electronic warfare systems faces some difficulties pertaining to identification of the sources of radiation within the radar range. This is accounted for by differences in the design and use of radars and the fact that modern radars can change the characteristics of emanation in the process of work. Analysts pay special attention to the emergence of radars with permanent frequency modulation and poor decamouflaging characteristics, such as Scout (the Netherlands) or Pilot MK-2 (Sweden).

In the foreseeable future, the disposable transmitters for suppressing electronic systems will presumably be further modified, e.g. by equipping them with intelligence components and artificial intelligence devices for independent detection and identification of targets, target selection and optimal suppression, guidance of the jamming transmitter, control over the efficiency of suppression, tracking the target by frequency and modulation parameters. The efficiency of such systems may also grow, thanks to increasing accuracy of their delivery to the target and duration of their work.

Qualitatively new electronic warfare systems are being developed to suppress or disrupt the work of electronic chips by providing jamming with non-linear effects and parasite receiving channels. Such systems are characterized with the power of the jamming signal, which is several times higher than regular and useful; these devices can be referred to both as electronic warfare systems and high-frequency weapons.

They may also employ low-yield beam weapons. The major difficulties concerning the development of such weapons are:

- poor knowledge of mechanisms of destruction of electronic devices with high-frequency radiation;
- existing and developed superpower high-frequency generators do not meet the requirements;
- large power sources can hardly be applied to the conditions in the field.

The major areas of work, as far as high-frequency generators are concerned, are:

- enhancement of output power of the traditional generators (klystrons, magnetrons, etc.);
- development of new types of generators on the basis of relativist electronic beams (gyrotrons, electronic lasers, etc.), generators with virtual cathode (vircators, tubutrons, reflective triodes, etc.);
- development of disposable and multi-usable generators transforming chemical energy of the explosive into the energy of electromagnetic field (explosive and magnetic generators, explosive magnetic and hydrodynamic generators, etc.) and improvement of beam and plasma generators.

Quite promising means of electronic suppression are explosive magnetic generators. Their major advantage is the possibility to deliver them directly to the location of the potential target. One of the ways to generate powerful high-frequency pulses is the use of electron accelerators, which enable to obtain a powerful direct high-frequency emanation in the process of interaction of the beam of relativist electrons and plasma. During the experiments the fields with the tension of 10^4 V/m were obtained. Another area of research is development of explosive magnetic and hydrodynamic generators that transform the energy of explosive into electric power. According to some estimates, they may produce up to several thousands of GW of power, one mega joule of pulse and up to 100 Hz of frequency. Electromagnetic generators with output power of more than 100 MW, 10-1,000 joule of pulse energy, 10-100 ns of pulse duration and 100-1,000 Hz of pulse frequency are being developed and tested. In the foreseeable future, an electromagnetic bomb with effective range of 1,000 m and more may be produced.

Superpower high-frequency generators may be used at unmanned aircraft to interdict the work of enemy air defense and command and control systems. Presumably, during one flight an unmanned aircraft with a generator may produce up to 100,000 pulses. Taking into account that each target will require about 1,000 pulses, one flight may be lethal for 100 targets.

Research is conducted to study the possible use of generators in close combat. Some experts argue that they may also be used to neutralize nuclear weapons. Samples of high-frequency generators have the weight of 20 kg and 1-GW pulse. If the generator weighs 200 kg, it may provide for 20-GW pulse then. The most convenient carrier would be the unmanned aircraft.

Wide use of computers and territorially distributed networks makes command and control systems be lucrative targets, vulnerable to practically all aforementioned types of weapons. Computers, however, are more resistant to electromagnetic emanation, for they lack the assemblies for receiving the pulse.

The use of different gases, aerosols and biological cultures for destruction of electronic components has widely been discussed in the foreign press. Theoretical examples were given, but there is no evidence of practical results of research in this area.

The possibility of developing and use of cyber weapons on the basis of program code is not doubted nowadays. The cases of their employment are known. According to US specialists, every year information resources are attacked about 250,000 times by anonymous users. It is assumed that only 1% of all attacks is registered. However, one has to note that US experts do not specify what kind of impacts they regard as attacks.

Cyber weapons using program code may hit the target in the following manner:

- self-dissemination of virus-like modules; the most advanced viruses use algorithms to penetrate the security system and spread in the computer networks by themselves (the so called worms);
- by transferring along with some other widely used software, whose launch leads to functioning of cyber weapons (software viruses);
- by various means of long-term information storage, including re-programmed chips (labeling the memory);
- Trojan horses;
- remote introduction of program code through data ports.

Such cyber weapons may:

- disrupt the work of electronic equipment by provoking the resonance of heads of hard disk or by burning the devices for visual reflection;
- delete records during over-recording;
- switching off the protection of power supply systems or causing their malfunctioning;
- conceal the sources of data receiving;
- destroy all software of the information system at certain time or before certain event;
- hidden partial change in the algorithm of software functioning;
- collection of data circulating in the enemy information system;
- delivery and insertion of certain algorithms in specific place in the information system;
- impact on data transfer protocols;
- impact on algorithms of routing and addressing in communication and data transfer systems;
- interception and interdiction of information flow in technical channels;
- blockade of the system;
- imitation of voices of operators responsible for the control systems and creation of virtual video images of certain people with their voice;
- modification of information stored in the databases of the enemy information system; insertion of false information in such databases;
- deception of security systems;
- modification of the data by positioning systems, meteorological systems, exact time systems, etc.;
- negative impact on a human being with special video, graphic and TV information;
- development and modification of virtual reality that suppresses the will and causes fear.

Taking into account the importance of information protection and struggle against cyber weapons, the US DOD budget for FY2000 got extra $515 million to protect computer networks and information infrastructure. The Internet is widely used to develop technologies of information security. Such systems, as Predator, enable to penetrate PCs without physical access from any part of the world (the listening point), obtain data and install secret software. So far, in practice, this method is normally used to control home PCs of officials.

Another technology provides for labeling of electronic documents stored on the hard disk. If someone attempts to open the labeled document, the information about this is immediately sent to the control center situated in any part of the world. The document will be followed through many protection screens around the world to detect the address of the receiver.

The US National Security Agency got a patent for the system of voice identification that should become an instrument of control of voice traffic and data. If an attack is detected, the investigation procedure starts – analysis of data sufficient to start the criminal case, collection of evidence and identification of the source of attack. Besides, the automated medium for detection of penetrations is being developed for the US DOD and private sector.

Combat Use of Cyber Weapons

Analysts define four factors facilitating the use of cyber weapons. They determine key directions of research concerning the combat use of cyber weapons.

Freedom of access to information systems. Development of information networks leads to the emergence of new challenges on the part of cyber weapons. A competent swindler has a potential opportunity to gain immediate access to a wide range of national strategic targets making the global information infrastructure. Under these circumstances, inter-connected computer networks may become a victim of many threats initiated by skilled individuals, non-governmental structures (such as international crime groups) and states possessing well-trained personnel for combat operation in cyberspace.

Transparency of state boundaries. One of the most significant particularities of global information infrastructure (and national infrastructures) is the elimination of traditional borders. The growing interdependence of national and global systems inevitably undermines national sovereignty. One of the most serious aspects of such transparency of borders is the lack of distinction between internal and external threats and vanishing difference among various forms of action against the state – from regular crime to military operations. Without clear distinction into external and internal threats, it is difficult to identify traditional espionage, crime, or war.

Some countries that lack sufficient military and economic power may try to profit from this situation and attack the enemy infrastructure through the cyberspace by using individuals or international criminal community. It is practically impossible to identify the organizer of such *strategic criminal operations*, i.e. the person who has given the order. As a result, a victim of cyber attack cannot understand what is going on and what actions should be taken in response.

Perception management. As a result of development of information systems, diminishing costs of access to the information and undermining of national sovereignty, there are expanding opportunities for manipulations with information that enable to shape the perception. For instance, the Internet may be used for dissemination of propagandistic materials from different sources. Political groups may use the Internet to mobilize political support.

It is quite possible that facts describing certain event may be distorted with the help of text, graphics and video techniques. This will enable a broad range of individuals and groups concerned to affect public perception and organize large propagandistic campaigns in order to undermine people's trust in the government. Such campaigns cause serious problems not only for the government, but also for the mass media, which are supposed to disseminate objective information. The direct consequence of such use of cyber weapons is deception of the leadership and the society.

The lack of intelligence data. In the conditions of transparent borders and free access to information, the intelligence service faces serious problems in providing the government with reliable and timely strategic information concerning current and prospective threats of cyber warfare. It becomes more difficult to identify the objects for intelligence. The classical geo-strategic approach (focusing on specific state as a source of threat) is now nearly obsolete. The targets for intelligence are transnational non-governmental and criminal organizations and non-state actors. The significance of information challenge will depend on the assessment of capabilities and intentions of potential enemies in the cyberspace and vulnerability of targets.

To identify the capabilities of the enemy employing cyber weapons, one should learn to resist dynamic development of telecommunication systems used by hardware and software, as well as by protection means (e.g. encoding devices). The future national information infrastructure will include the set of different components of technologically and economically developed society. Such components may be:

- general purpose commutation systems;
- control systems for oil and gas pipelines;
- electric power supply grids;
- transport systems;
- systems for maintaining federal reserves;
- different systems to support bank transactions;
- healthcare;

Some of these factors have been studied, some are yet to be explored. It would be extremely difficult for the intelligence community to develop and control the fixed list of potential threats. As a result, the country may not even learn who the enemy will be, what his intentions and capabilities are in the area of cyber weapons.

It is even more difficult to prevent the attack and evaluate the damage due to the difficulties in conducting intelligence, time deficit in case of crisis, etc. One cannot rule out that assessments prepared by law-enforcement and intelligence community with respect to certain situations may substantially contradict each other.

The offender using cyber weapons is capable of conducting swift strategic operations and return to certain locations in cyberspace. At the same time, the growing complexity of communication, database management and operational systems leads to the situations when some developments similar to cyber warfare may, in fact, be the result of unfavorable coincidence or errors in design.

One cannot rule out the possibility of strategic offensive after several years of clandestine preparations. When required bugs and devices are installed, they may ruin the entire system, when necessary. Such activities may often be wrongly diagnosed. The country, hence, may be completely unaware of the cyber attack, its initiator, and methods.

It will be quite difficult then to form and maintain coalitions of states for joint actions, due to the effect of cyber weapons. First of all, the members of the coalition will face a complicated issue of providing credible strategic intelligence, tactical warning and damage assessment. If cyber weapons are employed, the durability of the coalition may be tested, for the allies will find themselves in the information *fog*. There also may emerge some problems pertaining to the implementation of coalition plans if one of the partners feels less secure from cyber attacks.

Secondly, many countries remain quite vulnerable, as far as their economy is concerned. Key economic sectors may be attacked by the enemy to undermine the unity of the coalition. Systems acquired abroad for quick installation are particularly fragile and vulnerable to such attacks. Interdependence of partners within the coalition will make them change their national security strategies, so that technologically advanced states may render assistance to cyber-under-developed nations.

The use of cyber weapons leads to high uncertainty pertaining to identification of the attack, identification of the enemy and evaluation of the damage. Even if the limited cyber attack is detected, this may result in an assumption that it makes a part of the large cyber offensive. Such conclusion may be followed by limited or massed use of nuclear weapons.

General principles concerning the use of cyber weapons are the following:

- primary targets for cyber weapons are systems of control, communication and enemy decision-making bodies;
- the priority targets for suppression or destruction are enemy information and intelligence means, which should be

- neutralized before the beginning of large-scale combat operations;
- intelligence data should be delivered directly to users in the field, not through the chain of command;
- all available means should be employed to destroy the information infrastructure; one has to outdo the enemy in cyber battles;
- efforts concerning organization and use of information weapons should be large-scale and comprehensive, but should not be under political control at the operational level, for the decision-makers should only take a principal decision on the operation.

Nowadays the most detailed concept of cyber weapons employment is the US plan of fighting against command and control systems. It was laid down in the early 1990s and provided for the set of deliberate combat tasks to disorganize, suppress and destroy the enemy command and control structures. High effectiveness of such strategy has repeatedly been demonstrated in local conflicts, during the military exercise and modeling. According to the US analysts, disorganization of the command and control system reduces the enemy combat potential by 50% and more, providing for US superiority in conflict[1].

The impact on communication systems is as follows:

- destruction with conventional munitions guided by radio and radio-technical intelligence means;
- destruction with high-precision weapons guided by radio and radio-technical intelligence means with further targeting by other means and partial self-guidance at the last stage of the flight;
- destruction with new generation high-precision weapons guided by radio and radio-technical intelligence means to the area of the target with further self-search for the target and self-targeting at the most vulnerable elements of the target;
- radar jamming of communication means;
- generating imitating jamming impeding connection, synchronization in data transfer channels, initiating functions of repeated queries and duplication of messages;
- electronic suppression with the help of powerful electromagnetic emanation producing jamming by *parasitic* receiving channels;
- destruction of electronic components with high-level electromagnetic and ionizing radiation;
- spoiling the medium for dissemination of radio waves (e.g. modification of ionosphere and disruption of short-wave radio communication).

The combat use of cyber weapons based on program codes depends on two factors:

- external impact on the system through the devices connecting it to another system with facilitated access for the enemy;
- internal impact on the system by its administrators.

It is presumed that in case of real conflict the most critical elements of the state and military infrastructure may be isolated from accessible information systems. Besides, the United States works at the possibility of isolating its systems from the information systems of the allies. However, if multinational units are deployed the prospects for the use of IT to conduct cyber offensive are increasing.

The use of IT in cyber offensive is highly efficient in case of internal impact on the system. Depending on the level of responsibility of the agent, the outcome of such impact may be total disruption of its functioning for a long period of time. Such activities may involve either recruited personnel, or earlier installed software and viruses initializing at certain moment and in certain situation.

The efficiency of the use of cyber weapons is also closely connected with the issue of complex intelligence and counter-intelligence support. Intelligence support should include:

- development of databases and collection of detailed information on the situation in the potential conflict zones;
- discovery of key elements in the enemy control systems, communication and

receiving centers. This analysis should become a basis for the general list of facilities containing detailed description of major targets and time parameters for the work of certain elements of the control system. It is extremely important to know the procedure of functioning of the enemy control and communication systems during peace and war, organization of signal units, their activities and mobilization deployment plans. Such data should be detailed and provide for efficient use of high-precision weapons and electronic warfare means;

- assessment of capabilities and weak points of the potential targets in the system of control and communication. This information will help to identify the elements, whose early destruction will facilitate the accomplishment of combat missions;
- identification of key political and military figures of the enemy. Work with formal and unofficial power structures. Collection of biographical data and psychological characteristics of the leaders to ensure that they are affected with psychological warfare means;
- analysis of the enemy capabilities to influence control and communication systems. Collection of precise information and classification of all sources of radio emanation in the entire band of electromagnetic spectrum;
- provision of timely and credible information on the possibility of sudden attack. Timely informing officials on the current situation, opportunities and probable actions of the enemy.

INFORMATION RIVALRY – INVISIBLE WAR IN TIMES OF PEACE

The consequences of information influence may be comparable to the consequences of traditional hostilities. This is why the information rivalry should be studied in the context of inter-state relations and with respect to terrorist (or quasi-terrorist) organizations, whose actions may affect vitally important interests and are directly aimed against this or that state.

Key Areas of Cyber Warfare

Nowadays particular attention is paid not to the technological aspects of the problem, but to organizational and psychological aspects of information warfare. This does not, however, overshadow the importance of technical issues, for IT remain to be the essential component even in the most futuristic theories of information rivalry.

One may specify four major groups of the targets of information influence:

- control and decision-making systems;
- civilian information infrastructure (telecom systems, information systems of transport, energy, finance and industrial sectors);
- military information infrastructure (C3I systems);
- weapon systems.

The aforementioned facilities may be attacked in the course of cyber operations. For instance, a computer network may either be destroyed or damaged, or significant information may be stolen, or software may be changed by virus or hacking.

Detailed analysis of cyber struggle requires clear identification of its major areas. According to Martin Libicki[1], there are seven areas:

- command-and-control warfare;
- intelligence-based warfare;
- electronic warfare;
- psychological warfare;
- hacker warfare;
- cyber warfare;
- economic information struggle.

[1] Cyber War and Fight against Command and Control Systems. Directive by the Chief of Staff of the US Navy 3430.25, 1999.

Combating Command and Control Systems

The struggle against command and control systems provides for physical destruction of such systems or disruption of their work by separating the Armed Forces from command and control bodies.

Elimination of enemy command is an old and well-tested method of warfare. At present, command structures comprise both compact staffs and large command centers, whose diversified internal system contains developed information infrastructure (equipment, internal and external information flows) that has an impact on efficiency of pursuing military goals. Well-planned cyber attack against such command center may frustrate enemy plans without physical destruction of command. The thing is that crucial information is normally concentrated in the small number of easily identified places, some sorts of nerve-knots: command points, communication centers, power supply systems, etc. The elimination of such nerve-knots may deprive the enemy of any control of his forces.

Electronic systems may be hit with a powerful electromagnetic pulse, while data and software may be destroyed by viruses. The advantage of such operations is the difficulty of their detection, as well as the ability to conduct them before traditional hostilities. At the same time, the use of such soft weapons requires preparatory activities, including identification of key command centers and their weak points to facilitate the method of attack.

The enemy has to face the problem of protecting such centers from cyber attacks. For this purpose, it is important:

- to reduce the dispersed electromagnetic emanation of information systems or to generate covering background radiation;
- to cut off power of the inactive energy systems and communications connecting command centers with external systems;
- to duplicate power supply chains for information systems through independent power generators situated at the command point;
- to decentralize information networks, to develop closed non-interconnected functional information circuits;
- to develop of minimal required information infrastructure containing the smallest possible number of information systems that provide sustainable functioning of control systems in general and that may easily be restored if attacked;
- to preserve information systems and to create reserve copies of crucial information;
- to decentralize command and control structures before the conflict, i.e. to limit the personal contacts of the staff at the command point and to cancel large staff meetings requiring the attendance of decision-makers. Teleconferences and other similar activities are more recommendable.

In general, the aforementioned measures may be divided into three areas: decentralization, reduction in the number of excessive communication channels connecting the command structures with the external environment, and creation of duplicating and reserve systems that may fall victims of cyber attack.

The strategy of suffocation, unlike decapitation, provides for destruction of external communication systems, notably the nerve-knots containing critical information. The command and control systems then will not be able to perform their functions in due manner. The success of such strategy depends on accurate vision of the structure of the enemy communication system and information infrastructure. If the enemy information infrastructure is based on satellite communications, its work may be disrupted not only by destruction of the satellites (if they belong to the enemy), but by jamming and distortion of information.

Success of such operations also depend on the level of use of modern IT by the enemy. Wide use of IT enables the enemy to created reserve communication channels, whose suppression will be a more difficult task. Besides, such channels may be a disguise for really significant communication lines connecting command centers.

However, the abundance of communication systems should be a well-thought out and well-planned thing. For instance, duplication of information traffic ensures safety of incoming crucial information, whereas duplication of information flows in reduced networks (especially if their architecture is chaotic) may overload the system and make it stop data processing.

Intelligence-Based Operations (Digital Battlefield)

Contemporary concepts of information and intelligence operations are the follow-up of the concept of operational intelligence. However, it is noteworthy that such operations bring data (e.g. for target designation or data on inflicted damage) that goes to the actors directly involved in hostilities (even at the digital battlefield), whereas normally military intelligence data goes to the command centers where it is summed up, processed and then sent to the subordinates in the form of orders. In other words, the operational intelligence becomes adapted to the decentralized system of command and control. This requires additional changes in the system of collection, processing and distribution of intelligence data. It is necessary to ensure unification of sensor systems, distributives and weapon systems, so that each element has an access to aggregate information resources.

The theory of offensive information and intelligence operations formed the basis of the concept of digital battlefield. According to the latter, operational information from the battlefield is provided with the help of a system of sensors with different levels of details concerning the information received. There are four such levels:

- systems of long-distance detection, such as space surveillance systems, seismological sensors and acoustic systems;
- operational and tactical systems, such as unmanned aircraft with electronic, thermal visual and other equipment enabling it also to conduct electronic warfare;
- hydroacoustic buoys to monitor the situation in the seas and oceans; certain types of land-based stationary radars;
- tactical systems, such as optical, gravimetric, biochemical, acoustic and other sensors;
- navigation systems and guidance systems for weapons and military equipment.

The development of the multi-tier system of information gathering enables to obtain real picture of the situation in the combat zone and facilitates distribution of information among the users. At the same time, general integration of such components requires special algorithms for coordination of their work, and this is a difficult task. This intensifies research and development activities in the field of artificial intelligence and support systems for decision-making.

Offensive intelligence and information operations are aimed at collecting, processing and distributing among end-users the fullest possible information about the enemy, whereas defensive operations strive to protect such data from the enemy or to distort it at any of the aforementioned levels.

Another aspect of defensive information and intelligence operations is not only to prevent enemy's access, but also to protect the data from enemy's activities. One of the most efficient methods would be to simplify and, hence, to make the cheapest possible such systems, so that the attempts of their destruction become unfairly costly. For instance, expensive and few aircraft with long-range radars are quite vulnerable and make lucrative targets, but it would be inefficient to use air defense missile systems against cheap and numerous unmanned aircraft.

Methods of protection providing for distortion of information may be effective if appropriate data is obtained from distributed information systems requiring comparison and complementing each other. Such distortions tend to increase, as the information is processed and flows from one level to another. Hence, it is an urgent problem nowadays to develop the systems for comparison and evaluation of incoming information in the conditions of uncertainty.

Electronic Warfare

The goal of electronic warfare is to reduce the information capabilities of the enemy and, hence, it is subdivided into electronic warfare (interdiction of data transmission by jamming), cryptographic warfare (distortion and elimination of information) and struggle against enemy communication systems.

Electronic warfare has been known for a long period of time. At present, many experts name it among key elements of cyber warfare in pre-war and wartime. The methods and means of electronic warfare are always being improved. For instance, it is not only a matter of jamming to impede data transmission, but also the use of parameters of irradiating equipment of the enemy to target firepower and to ensure their physical destruction. Such guidance does not use passive characteristics of the target (effective surface of dispersion, thermal emanation, visual image), but active parameters; therefore, the very possibility of use of antiradar weapons may hamper or even lead to refusal to employ transmitters and receivers.

Struggle against communication systems is more difficult than electronic warfare. It is easy to detect transmitters and receivers, whereas radiation of communication lines and channels is minimal. Screening of such lines and the use of fiber-optics and laser equipment helps to diminish distortion of information and prevent the enemy from interception of transmitted data. Nonetheless, in some cases the channels of information exchange remain potentially vulnerable, especially for wireless data transmission from facilities (from satellites or unmanned aircraft), whose location may easily be identified and fixed. An efficient way to affect such systems would be chaotic jamming filling the medium used for data transmission.

The cryptographic warfare implies encoding of data and obtaining access to data hidden by the enemy. Decoding is a complicated and labor-intensive process requiring the use of powerful computers. It takes long and information may become obsolete during this time. This is why one of the major missions of cryptographic units is to assess the value of information and how long it is valuable, before decoding it. The similar problem has to be solved in the process of encoding, for the unjustified use of complex methods of cryptography may significantly increase the amount of transferred data, decrease the speed of transmission and lead to general overloading of communication channels.

Psychological Warfare

Psychological warfare means manipulations with public opinion at different social levels. Western experts normally sort out the following categories of information and psychological operations:

- operations against the governing bodies;
- operations against the military command;
- operations to demoralize the personnel.

Key objects of information and psychological operations against the governing bodies are the society in general and principal state organs. Public opinion, however, is more susceptible to such operations, whereas the authorities (due to certain conservatism and inertia) are less susceptible to standard ways of manipulating public consciousness.

One may name the following stages of influence:

- through national mass media of the enemy;
- by using alternative channels of information and psychological influence (alternative mass media, foreign broadcasting, the Internet);
- external pressure on political leadership and public opinion of the enemy; creation of the international climate impeding implementation of enemy’s plans;
- suppression of the systems of national broadcasting, e.g. destruction of relay satellites, TV and radio stations, etc.

Disorganization of command and control is the top-priority task during the cyber warfare. One of the major tools used against such structures is disinformation. Besides, it is possible to provide the enemy with abundant and contradictory information, disrupting adequate decision-making in the conditions of time limit. Another method of disorganization is to deter the enemy, e.g. to form a stable perception about superiority and senselessness of resistance. The primary objective would be to eliminate the watershed between the reality and the impossible. To achieve this goal, the US military suggested the strategy of imposed value. Its author, Col. (USAF) D. Warden[2], believes that if the party manages to impose on the enemy the costly tactics, the enemy will eventually refuse to continue the struggle.

Psychological operations against the personnel apply two major emotions: the fear of death and mutual dislike, as well as the lack of direct connection between the front and the rear. It would be efficient to provide combatants with plausible, but frightening information. Another tactics in low-intensity conflict (when the front and the rear have insufficient information about each other) is to provide them with separate or dozed information, sometimes using national information channels of the enemy.

Hacker Warfare

Hacking is mainly confined to attacks on various components of computer networks and information resources. The program finds a weak spot in the security system and penetrates the computer enabling the hacker to control the functioning of the system and to manipulate (delete or change) the information contained. Some Western analysts, e.g. Winn Shwartau and Rato Haeny[3], tend to assume that information warfare may, in general, be reduced to hacking.

The most notorious means are computer viruses, worms, Trojan horses, logical bombs, holes in the system, and bugs in the hard disk. Haeny believes that the aforementioned tools along with new emerging program means of hacking may be regarded as existing or potential samples of cyber weapons[4].

Computer viruses are the fragments of program code capable of reproduction by copying themselves into codes of other software subject to penetration. Such virus disrupts the work of the software or local system. It initializes when the program is started and copies itself into another program, or distorts data, or disrupts the operations of the system. A disadvantage of viruses, as far as cyber warfare is concerned, is their autonomy (except the need to start the master program) and, hence, inability to control or correct their work in the enemy’s system.

Unlike viruses, worms are independent programs designed for self-dissemination by copying this package from one computer to another via the net, including the Internet. Worms do not modify the programs and do not hit the data on local computers, but may disrupt the work of the net and enables the enemy to obtain access to information resources of the net under attack. In some cases, when the work of an organization depends on the stability of work of corporate computer network, e.g. in banking, the use of worms for cyber warfare may be quite efficient.

Trojan horses are fragments of computer code concealed within the infected program and are widely used to disguise the penetration of worms and viruses into the system. Trojan horses may be hidden in auxiliary programs supplied with commercial and other security systems. Potential swindler may modify a part of software of the system and then disseminate the modified version.

Logical bombs are varieties of Trojan horse programs and are sued to launch a virus or other program attack on the computer system. The most notorious and widespread kind of bomb is that initialized by preset context (keyword).

Logical bomb may be an independent program or a fragment of the code distributed by programmers or producers of some software. At present, when entire world uses mostly US products (*Ms Windows* or *Unix*), which have become a certain standard software, the employment of logical bombs is quite probable and may be initiated not only by manufacturers, but also by their governments.

Black holes are special program mechanisms circumventing the security systems and built in by the manufacturer, in order to gain access to the information resources and its settings. This method is quite attractive for information and intelligence activities. Producers of hardware (especially hard disks, like *BIOS*) also build in logical bombs and black holes in computer systems.

Cyber Warfare

Concepts of cybernetic struggle become more and more popular when it comes to highly intense conflicts. Cybernetic warfare was even mentioned in the revolution in military affairs – the use of new technologies and organizational and command changes in military sphere.

The role of network struggle increases in low-intensity conflict and other than war operations, non-military conflicts, crimes and terrorist activities. The network struggle is more the struggle using information capabilities than the struggle against information structures of the enemy. Moreover, the concept of network struggle implies the use of enemy information infrastructure for one's own purposes. In this connection, it has many things in common with terrorism, whose major actors are small groups, such as transnational terrorist groups, illicit arms traffickers, transnational criminal syndicates, drug traffickers, Islamic fundamentalists, ethnic and nationalistic movements, information pirates, smugglers, etc. Thus, at the state level the network struggle is reduced to resisting the activities of such organizations, i.e. to anti-terrorist work.

There are three major problems that emerge during the counter-network struggle:

- Hierarchical state systems are, as a rule, less efficient in combating network structures. The time they need for adequate decision-making and response is much higher than in network structures.
- Efficient anti-terrorist activities require the establishment of counter-terrorist units based on the network principles and, hence, possessing broad decision-making powers. Such requirement does not imply the mirror copying of the structure and methods of the terrorist organizations. The problem may efficiently be solved with the help of technical innovations, new mechanisms of inter-agency coordination and development of inter-state cooperation, including unification of national legislations.
- The advantages in network struggle may be gained by efficient use of opportunities given by the network organization and information nets (the Internet).

US specialists had to face all this problems in the process of establishing the counter-terrorist center under the CIA aegis. On the one hand, the center benefits from functional principles of network organization; on the other hand, it interacts actively with traditional military and state hierarchical institutions.

Economic Information Warfare

Nowadays, thanks to the information networks, users may access information in any part of the planet. Analysts believe that advanced societies are equally dependent on the stability of information traffic and material supplies. Normal functioning of some sectors of the economy and finance totally depends on the availability and timeliness of access to information resources. Moreover, globalization of world economy and development of non-monetary economy make this dependence practically absolute.

Under these circumstances, information blockade becomes a flexible and efficient instrument of influence on potential enemy. It may be clandestine, whereas appropriate information operations may be disguised as accidental errors in information systems or occasional hacking of computer hooligans.

Information Warfare and International Cyber Terrorism

Rapid progress in IT gives a new meaning to the problem of international terrorism. Terrorists use information infrastructure to develop the so called network methods of self-organization and affect information infrastructure.

Many analysts presume that terrorist organizations, regardless of their motivation, gradually evolve from initial hierarchical structure into information-oriented network organization. Inside groups the leader's personal appeal is replaced by simplified decentralized system. Separated groups often merge into terrorist communities. Changes in the organizational structure of terrorist groups led to transformation of their strategy and tactics. They comply with the principles of affecting facilities, whose destruction may cause numerous casualties or provoke public and political repercussions, but their vision of the terrorist struggle as the immediate tool to attain the goal is changing. It is much more efficient to paralyze the information infrastructure than to undertake single terrorist acts. Moreover, the transition from isolated activities to deliberate terrorist campaigns (often not limited to the activities of one group and quite complex in their implications) impedes the counter-terrorist struggle.

Combat against terrorism may be hampered by expanding opportunities for terrorist actions. Until recently the terrorism has been the lot of small and somewhat professional groups, whereas IT help the amateurs to resort to hacking for terrorist purposes. Taking into account crucial dependence of many vital sectors on information systems, such amateur actions may be no less dangerous, albeit they may even be unaware of their perilous implications.

Besides, terrorist organization, as a rule, are quick in adopting advanced IT than the states. Many experts even think that terrorists will not strive to disrupt the work of information networks in general. They will be more interested in preserving them operational, so that they may easily coordinate their activities (like now in the Internet), hide them and propagate their views. Thus, any open information infrastructure is potentially vulnerable to terrorist acts.

Finally, one has to bear in mind that the states conducting information operations may cover their activities and claim them to be terrorist acts by some notorious and hardly known groups. In this connection, another urgent task that emerges nowadays is identification of the enemy in cyberspace and adequate response to emerging challenges. It is crucial to decide what the source of malfunctioning is: occasional internal error, or deliberate attack.

Russia in Information Struggle

Russia has to face two major problems, as far as information struggle is concerned. On the one hand, the involvement in global informatization processes, integration into cyberspace are indispensable conditions for further development. On the other hand, large-scale spread of IT without any substantial barriers brings about new security challenges for individuals, society and the state in the Russian Federation.

In comparison with many states, Russian cyberspace seems to be more vulnerable due to the low level of development of communications and vast territory of the country. As a result, information control of Moscow over northern and eastern parts is difficult to achieve. This causes problems in Russia's relations with its neighbors, notably China, which, as some Russian specialists assume, uses weak information control of the Far East to impose indirect Chinese control over the region[5].

The heterogeneity of cyberspace and the emergence of cultural and language sub-spaces also run counter to Russian interests in the information sphere. This is accounted for by maximal striving for power on the part of regional elite and by activities of extremist, sometimes criminal organizations working under disguise of nationalistic and religious ideas.

In this connection, one may sometimes hear the recommendation to isolate Russian public from the global information space. However, we assume that it would be more dangerous for the future of Russia if it is cut off world information resources, global exchange of knowledge and other achievements of civilization. Accelerated development of advanced IT and integration in global cyberspace may ensure economic growth and authority on the international arena. This is why the most rational way of repelling information threats would not be passive, but active resistance, including the development and implementation of measures to forecast, detect, prevent and eliminate challenges at an early stage, in beforehand.

[1] M. Libicki, "What Is Information Warfare?" *ACIS Paper*, No. 3, August 1995.

[2] Z. Khalilzad, John P. White, Andrew W. Marshall (eds.), *Strategic Appraisal*: *The Changing Role of Information in Warfare*, *RAND*, 1999.

[3] W. Shwartau, J. Draper, *Thunder's Mouth*. Princeton, National Books, 2000; R. Haeny, *Information Warfare. An Introduction*. Washington, The George Washington University Cyberspace Institute, 1997.

[4] R. Haeny, op. cit.

[5] See: S. Modestov, *Information Struggle as a Factor of Geopolitical Rivalry*. M., MPSF, 1999, 80 pp.

INTERNATIONAL INFORMATION SECURITY AND NEGOTIATIONS

Emerging threats to information security require diplomatic efforts aimed at strengthening strategic stability on the basis of international cooperation. There is a growing danger of cyber warfare and proliferation of appropriate cyber weapons, which may lead to new arms race at the qualitatively new technological level and in the new strategic context.

International Law and Cyber Wars

Most types of traditional hostilities nowadays include some aspects of cyber warfare, notably attacks against information systems with the use of traditional weapons, psychological operations, disinformation, traditional electronic warfare (electronic suppression of receivers/transmitters and other systems). However, in the recent years new kinds of weapons have emerged, which may be regarded as both traditional and information (explosive generators of electromagnetic pulse, powerful microwave devices, orbital lasers, graphite bombs, etc.). They may be subject to existing norms of international law and customs of war, albeit some specific types of such weapons are not covered by arms control agreements.

The situation is different, as far as information operations are concerned, since they do not provide for physical destruction of the components of information systems. Traditional international norms can hardly be applied in such cases. This is why it seems necessary to elaborate the internationally recognized system for assessing the scale of danger of cyber attacks and negotiate the list of countermeasures: from international sanctions and political pressure to enforcement operations and war against the identified aggressor. According to the 1999 US DOD report – "An Assessment of International Legal Issues in Information Operations" – the response to cyber attacks against the USA will be fierce, whereas possible consequences of the large-scale network attack justify the large-scale military countermeasures.

The most heated debate concerned the problem of definition – whether cyber attack against the information and network resources of the state might be considered an act of war. In theory, the act of war is the violation of rights of another nation stated in the international law and, as a result, the victim of aggression declares war against the enemy. Hence, US military believe that the concept of the act of war has no importance for the contemporary international law. Sanctions with the use of military force may follow much smaller breaches of rights of another nation and will not be regarded as an act of war at the same time.

The similar situation occurs concerning the provisions of the UN Charter and the *Declaration on Principles of International Law concerning Friendly Relations and Cooperation among States in accordance with Charter of the United Nations (*UN General Assembly Resolution No. 26/25 of 1970). According to Article 2 (4) of the UN Charter, the member states commit "to refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations". Resolutions 26/25 and 33/14 (1974) "*Definition of Aggression*" set forth the key criteria for aggression and it is defined as the crime with appropriate liability under the international law. Finally, Article 51 of the UN Charter provides for the right to individual and collective self-defense in response to military aggression. Thus, if information operations are not defined as military aggression or the act of war, any self-defense will not be legitimate from the point of international law.

After adoption of the aforementioned resolution "*Definition of Aggression*" by the UN General Assembly, the US delegation argued that this declaration did not set rights and responsibilities of the states and might only be a useful guideline for the Security Council.

US military experts have repeatedly criticized the intentions of the world community to link cyber attacks with the notions of the act of war and use of force[1]. European analysts share different opinion.

For instance, O. Bringmann, who studied this problem under the request of the German and Dutch defense ministries, maintains that offensive information operations may be interpreted as an act of aggression and, hence, adequate and legitimate response measures may be taken[2].

The international legal definitions of such terms, as the use of force, act of aggression, armed attack or the act of war, provide for the existence of weapons and their use. In other words, they imply that there is a special threat originating from the use of weapons. Armed attack means a certain level of physical destruction and occupation of the territory of the victim. However, such definitions do not take into full account the characteristics of some combat means that are recognized as weapons. For instance, CW and BW do not destroy facilities and are employed against personnel. Laser systems, infrasound generators and other non-lethal weapons have limited effect on human beings, but are still regarded as weapons. Hence, the international law should seek other criteria to define the notions of weapons and armed aggression. It is more important to look not at the effects of the weapons (destructive, incapacitating, etc.), but at the objectives of the aggressor. Thus, weapons may generally be defined as the means to achieve military superiority over the enemy capable of destruction, if necessary. This extended definition of weapons enables us to consider cyber attacks against other states be an act of armed aggression.

In this case, if the consequences of the information operation are comparable to the consequences of conventional weapons use, it would be legitimate for the state to act in self-defense. It may not only conduct an information operation in response, but also launch some traditional combat operation (if principles of proportionality and necessity are observed). Such approach leads the advisability of resolving some other issues: definition of the threshold of cyber attacks provoking response; justification and proportionality; principles of identification of the aggressor; possibility of actions against the third country, whose territory is used for accomplishment of the information operation.

At the same time, there is a trend in contemporary debate characterized by attempts to classify the cyber attacks as terrorist actions and to solve the problem of response within the counter-terrorist framework. Cyber attacks are, thus, defined as terrorist acts (since many of them are conducted anonymously) and the United States keeps the right to launch asymmetric counter-operation, using both traditional and non-traditional combat means. At the same time, Washington tries to justify the availability of offensive capabilities for information operations with the need to protect its rights and ensure defense against potential aggressor.

The aforementioned 1999 US DOD report maintains that if the anonymous cyber attack might be identified as planned and conducted by another state, the victim would have the right to protest against such actions and submit the dispute to the international organization. And only if the international community is sure that such attack or series of attacks may be regarded as an armed aggression, the victim should have the right to response with counter information operation or with traditional combat means.

This reflects a contradictory character of the US position on the legality of cyber attacks. On the one hand, the United States reserves the right to conduct information operations as soft sanctions envisaged by the international law or as *humane* methods of prevention of aggression. On the other hand, taking into account the threat of cyber attacks for its own information systems, Washington strives to define them as terrorist activities and to outlaw them. The US leadership may, hence, decide to launch a response cyber attack against another state, although the right to self-defense cannot fully justify the active defense, especially if the attack is conducted by the terrorist organization or an individual from the territory of another states, which cannot stop these actions, and the international sanctions are inefficient.

There are other approaches to the issue of international legal qualification of information operations. It is possible to divide them into information operations against information infrastructure and special operations, such as disinformation of the population, exertion of pressure via the mass media, etc. In fact, operations against national information systems may be harmful for international information infrastructure that is protected with a number of international agreements[3]. It is important that many of such treaties cover member states and third parties that use protected facilities. In many cases the parties pledge not to use international information systems for military purposes.

Practically all countries admit the advisability of negotiating the list of key information systems (both governmental and non-state), whose functioning is crucial for national security. If such types of systems are selected, their protection may be enhanced, including the legitimacy of response (active defense) to information operations. This will enable the international community to work out emergency mechanisms of international response to information challenges, taking into account their effect on national security of various states.

Another important problem that should be discussed is the use of information operations during the peaceful time as an instrument of state sanctions or intervention. If the internationally protected rights of the nation are breached, the victim may undertake proportional reciprocal measures, if they are not aimed at provoking the use of military force. Among such countermeasures one may name the suspension of diplomatic relations, trade and transport embargo, refusal to render assistance, freezing of bank assets belonging to other nation, etc. However, it is suggested that information capabilities of the violator should also be restrained. If international embargoes begin to cover the information sphere, the party that dominate the market of telecom services in the world will have a monopoly on applying this tool.

The international law prohibits to interfere in domestic affairs of the states, banning the pressure of one state on another in order to make it change or suppress the capabilities of its free will. At the same time, the UN Charter does not provide for self-defense with the use of armed forces or weapons in response to such interference.

If the expanded version of the term "weapons" is approved and the information medium become the zone protected by the international law, if asymmetric actions against another state in information sphere afflict the functioning of its significant information systems, such actions may be treated not as economic or diplomatic pressure, but as an armed attack entitling the victim to resort to self-defense.

The Rules of Armed Conflict and the Cyber Warfare

Western specialists often raise the issue of application of traditional rules and regulations pertaining to armed conflicts and wars to cyber warfare. Some experts strive to replace the term "laws and customs of war" with the "rules of conducting armed conflict". They emphasize that at present, the states rarely declare war, but are often involved in armed conflicts of different scale. However, the very of term "international armed conflict" is beyond the definitions contained in the Hague and Geneva Conventions and other international agreements. This is why such substitution of terms makes a dangerous precedent, for the states, avoiding the declaration of war, face the need to clearly identify the fine line between the end of the political phase of the conflict and the beginning of its military stage. This is extremely important, bearing in mind the recent boom in new notions (low-intensity conflict, other than war operations, the rogue states, humanitarian interventions), which can hardly be clearly defined.

If the cyber attack is not defined as an act of aggression, the United States (which has the most developed and vulnerable information infrastructure) may fall victim of such actions (this is already true with respect to criminal attacks). The intervention of the international community in such conflict becomes impossible, for such arbitration will be reduced to the question "who is to blame?" without recognized criteria. If cyber attacks are treated as combat operations, they should be subject to major laws and customs of war, whereas the replacement of the term "war" with the term "international armed conflict" may return the situation to the initial level of debate.

The use of force is allowed if it is not banned by laws and customs of war, is controlled and is kept at the level required for partial or full suppression of the enemy with the minimal casualties, losses of time and resources. All known interpretations of this principle agree that the use of force in war should be selective. Some types of cyber weapons, such as computer viruses, Trojan horses, logical bombs and other devices that destroy information systems and are not selective, cannot be regarded as legal means for cyber warfare. They should be treated (in accordance with the scale of possible implications) as the means of terrorist struggle, or WMD, whereas their development and production should be regulated with the norms of international law.

The situation is much more complicated when it comes to selective cyber weapons that are used against certain elements of information infrastructure and such legitimate targets, as military information systems.

On the one hand, the principle of military necessity is beneficial for the proponents of expanded use of information operations, for they are humane, non-lethal, short-term and do not require physical destruction of enemy's resources. Meanwhile, complete destruction of information and telecommunication infrastructure, as many US experts demand[4], may paralyze the economy, disrupt air traffic and the work of energy systems. Such actions will have devastating effect and will lead to deaths of civilians that cannot be justified in terms of military necessity.

Thus, the demands for inflicting maximal damage to information structure of the state contradict the principle of military necessity. Besides, they run counter to existing international agreements and a number of international conventions concerning the rights of the neutral party.

One has to point out that difficulty of distinguishing between military and civilian information systems. For example, 95% of military communications in the United States are crossed or even based on civilian facilities of information infrastructure. The destruction of military facilities may be justified, but one cannot rule out the possibility of damaging civilian systems. The United States, hence, faces the dilemma caused by the asymmetry of offensive and defensive information operations.

According to the principle of humanity, it is prohibited to use military force, regardless of its scale, if it does not serve the objectives of war (partial or full suppression of the enemy with minimal casualties, losses of time and resources).

This principle mirrors the principle of military necessity and is often used by the proponents of cyber warfare for its legitimization. It is true that information operations do not directly affect human lives. However, if the cyber attack is performed by a terrorist group not related to the state, the large-scale information response against the state, whose territory is used for such act, would have dramatic consequences and would hardly meet the principle of humanity.

The planning and implementation of information operations should take into account the principle of proportionality of the damage inflicted to civilian and military facilities. The provisions of international law regulating the use of force and the principles of conducting the war should also be born in mind. Anyway, decision-maker should proceed from the need to minimize the civilian casualties. According to the humanitarian law, as Lawrence Greenberg, Seymour Goodman and Kevin Soo Hoo fairly emphasize, the evaluation of legality of operations should be based on the assessment of damage to civilian population, rather than on the assessment of means and methods of attack[5]. In other words, the indirect damage of information attacks, e.g. air crashes caused by malfunctioning of air traffic regulation services, should also be taken into account, as an argument against even narrow cyber attacks.

It is also useful to outlaw the use of international systems as the means to accomplish information operations and other military activities. In this case response will be focused on the state-violator and will not affect the international system.

If the world community approves the aforementioned principles of conduct of information operations, it would be advisable to make a list of civilian and transnational facilities protected by the international law and a list of military systems, which may be subject to legitimate attacks.

The aforementioned arguments referred to the activities targeted against information systems, while the issue of psychological manipulations was not covered. In fact, such actions hardly comply with laws and customs of war. Meanwhile, many Western experts assume that the use of social technologies, top-level political disinformation and propagandistic campaigns against the enemy (actual or potential), shaping the image of the enemy in the world may have a decisive impact on military capabilities of the enemy. According to Colonel (USAF) Richard Szafranski, cyber warfare may be confined to such actions.

International Legal Limitations on Cyber Weapons

There is a number of important international agreements that may relate to information operations.

Modern telecom and navigation systems cannot work without space satellites. The 1967 Space Treaty contains the provision banning the deployment of nuclear weapons and other WMD on the Earth orbit. WMD normally refers to nuclear, chemical and biological weapons, for experts still hesitate whether cyber weapons should be regarded as WMD. However, many analysts tend to apply this provision of the Space Treaty to cyber warfare. At the same time, the problem is that the treaty prohibits deployment of WMD at orbital objects, whereas artificial Earth satellites and other spacecraft may be used as relay facilities supporting the work of different weapon systems, including WMD and cyber weapons.

The Space Treaty and other appropriate agreements agree that outer space should be used for peaceful purposes only. At the same time, INTELSAT-60 and INTELSAT-61 systems developed for peaceful purposes may be used for information operations. The question is whether the system may be regarded as civilian, if the information from satellites is used for military purposes? The answer is yet to be found.

Thus, along with the ban to deploy combat elements in outer space (such as space-based components of missile defense systems), experts call into question the possibility of distinguishing between civilian and military satellites that may be used for information support of combat operations. Hence, the collision with the international laws on the use of outer space emerges. This issue is quite topical for some modern weapon systems may be used only in conjunction with space systems[6]. Moreover, one may argue that indirect use of space systems for military purposes will grow in the future.

The Convention on International Liability for Damage Caused by Space Objects is another international agreement regulating human activities in outer space that may be applied to information operations. However, this document refers to peaceful time and does not restrain the development of space-based cyber weapon systems.

Development and production of some cyber weapons may run counter to a number of provisions of the *International Telecommunication Convention*, which state that all receiving and transmitting stations, regardless of their purposes, should be deployed and operate in such a manner that they do not have dangerous impact on radio services an communications of other members of the convention. To a certain extent, this agreement place restrictions on the use of jamming aircraft, whose equipment may affect both military and civilian electronic means. Nonetheless, the document speaks about the use of electronic warfare systems during the war and, besides, the civilian facilities are not the immediate targets of such systems.

Another important issue is whether the physical destruction of civilian receivers and transmitters of TV and radio systems can be regarded as the breach of the convention.

Cyber weapons are not subject to any international treaty pertaining to arms control and arms reduction. Meanwhile, there is an urgent need to negotiate and sign the treaty curbing the proliferation and development of cyber weapons. Wide use of IT in military affairs can significantly enhance the efficiency of military operations, all other things being equal. Such treaties, as START I and START II, or the CFE, despite any shortcomings, helped to maintain the balance of power and curtailed uncontrolled arms race, as well as increasing military confrontation. Regardless of current efficiency of cyber weapons, their existence should be taken into account by military-political leadership. The inability to make adequate assessment of the consequences may result in asymmetric answer. In this case, cyber weapons may catalyze the escalation of traditional conflict.

Debate on the problems of curtailing cyber weapons should cover not only new and disputable aspects of cyber warfare, but also some traditional types of weapons remaining beyond the framework of current agreements. They are:

- jamming aircraft and aircraft with long-range radars that enhance sustainability and effectiveness of command and control during the war;
- orbital groupings used to collect and retransmit information for military purposes;
- means to disrupt the work of energy and information communications;

Thus, cyber warfare is not covered by any existing international agreement. The treaties that somehow mention this problem do not give unequivocal interpretation of the information security issues. Modernization of the existing agreements, taking into account the possibility of development of cyber weapon systems and high vulnerability of information infrastructure of the majority of developed nations, is desirable, but can hardly be implemented. Hence, negotiations should start to elaborate a new agreement with clear international legal norms pertaining to cyber warfare and information operations.

If the international community fails to agree on conceptual basis of international agreements putting constraints on new types of weapons, military-political situation may be destabilized.

At present, practically all nations, including Russia, the United States, China, and Europe, start to pay much attention to the problem of curbing cyber weapons. At the same time, there are serious contradictions in the approaches towards this process. The very notion of cyber weapons is not clear yet; therefore, the rules of the game will be determined by initiators (and most active participants) of the negotiation process. For instance, *RAND* suggests that Washington benefits from this ambiguity to lay down its own approaches towards arms control, export regimes and international cooperation with respect to cyber weapons, so that the United States may enhance its national security in the future[7].

Washington strives to outlaw weapon systems targeted against information infrastructures (this is the most typical issue for the USA, taking into account their developed and potentially vulnerable information infrastructure) and leave intact the use of information capabilities for traditional military purposes. According to the US experts, another probable issue for negotiations would be prospective types of weapons (in which none of the countries have superiority so far). Such weapon systems comprise electronic pulse systems designated for attacks against information systems (i.e. again the components of offensive systems). It would be fair to emphasize that US analysts more and more often ask how long the US domination will be and what US long-term strategy in the area of information security should be[8]. Thus, one may assume that the United States will stick to wait-and-see policy, as far as control of cyber weapons is concerned.

The mission of any nonproliferation and export control regime is two-fold: it strengthens national security of the state by ensuring technological superiority and it strengthens overall stability, preventing the use of technological innovations for terrorist purposes. However, it may be difficult to apply export control principles to IT.

Firstly, under the pretext of strengthening the nonproliferation of cyber weapons, free use of international information resources and systems may be restricted to a number of states.

Secondly, efforts to curb proliferation of IT will hardly be accepted by business communities, especially in developed countries.

Thirdly, the international nonproliferation regime should take into account the hidden capabilities of information systems, which should then undergo compulsory international certification.

Under these circumstances, the Russian initiatives at the UN envisage that the states should commit to refrain from:

- activities leading to domination and control in cyberspace;
- restricting access to new IT, creating conditions that may promote technological dependence in the area of informatization in detriment to other states.

The adoption of these provisions, even at the level of declaratory policy will help to avoid the use of nonproliferation regime to the benefit of individual countries or groups of countries.

Beside arms control and export regimes, world community may be interested in developing international cooperation and expanding interaction in information security sphere, in order to harness national legislations and promote joint counter-terrorist efforts. It would be advisable to sign bilateral and multilateral agreements on mutual security arrangements.

The basic elements for such cooperation would be:

- joint assessment of emerging challenges pertaining to cyber warfare and common understanding of potential threats;
- joint development of protection mechanisms and practical methods of reducing vulnerability of information systems and networks;
- permanent exchange of information on potential enemies and emergencies concerning the work of information infrastructures, in order to work out adequate response measures;
- agreed measures to detect attacks against critical information infrastructure and, if detected, the use of certain coercive measures to stop the attack;
- agreed measures of mutual assistance if information infrastructure is damaged by natural disasters.

Positions on Information Security Issues at the International Level

In mid-1998 Russia offered the United States to sign a joint presidential statement on information security issues. The draft of the document contained the vision of the current situation in information sphere characterized by unprecedented progress in human development and obvious threats to global stability and security. Moscow emphasized that the existence of such challenges required some preventive measures. This process would comprise the following stages and steps:

- identification of general views of the world community on the problems of using IT for military purposes as weapons;
- definition of key terms (cyber weapons, cyber warfare);
- full count of the possibility of using IT to enhance existing weapon systems and to develop new arms;
- consideration of the advisability of establishing the international system (center) to monitor information security risks;
- submission of the information security issues to the UN and other international forums for consideration, in order to negotiate the international legal regime banning development, production and use of the most hazardous types of cyber weapons;
- negotiations on the international multilateral treaty on combating cyber terrorism and crime.

Russia believed that such joint statement would have facilitated the specific, comprehensive and meaningful discussion of the aforementioned matters.

However, the draft was not approved. General concerns about information security challenges were reflected in the Joint Statement on Common Security Challenges at the Threshold of the 21st Century signed in Moscow on September 2, 1998. The parties:

- 'agreed to intensify joint efforts to counteract the transnational threats to our economies and security, including those posed by […] computer and other high-technology crime;
- 'recognize the importance of promoting the positive aspects and mitigating the negative aspects of the information technology revolution now taking place, which is a serious challenge to ensuring the future strategic security interests of our two countries;
- 'declare that the common security challenges on the threshold of the 21st century can be met only by consistently mobilizing the efforts of the entire international community. All available resources must be utilized to do so. In the event that it is necessary, the world community must promptly take effective measures to counter such threats.'

The statement maintained that the parties agreed to intensify joint efforts to repel transnational threats, including computer crimes; recognized the importance of enhancing positive aspects of information revolution and mitigating its negative consequences; argued that common security challenges should be met only by mobilizing endeavors of entire international community.

Russian approach towards international information security issues was also reflected in the special address of Foreign Minister Igor Ivanov to UN Secretary-General Kofi Annan in September 1998[9]. The letter contained the draft resolution of the UN General Assembly entitled "*Developments in the Field of Information and Telecommunications in the Context of International Security*". This draft developed ideas of the UN General Assembly resolution on the role of science and technology for this specific area. The document pointed out the need to prevent the emergence of IT and means, whose employment for military purposes would be comparable to the use of WMD.

Russia's proposals were modified, mostly as far as recommendations to inform the UN Secretary-General on views and assessments of the member states were concerned, and on December 4, 1998, the resolution was passed by consensus and without voting (A/RES/53/70).

Some provisions of the initial Russian draft, such as the use of IT for military purposes, the advisability of defining cyber weapons and cyber warfare, the need to establish the regime banning development and use of cyber weapons, as well as the comparison with the WMD were not reflected in the resolution. The US delegation noted to the First Committee the flexibility of the main sponsor in promoting this initiative.

Later on the UN Secretary-General received comments and assessments of Australia, Belarus, Brunei, Cuba, Oman, Qatar, Russia, Saudi Arabia, the UK, and the USA published in the appropriate report (A/54/213).

Australia believed that, despite the urgency of the matter, the principles of global information security should not be worked out at the UN Department for Disarmament Affairs. Information infrastructure is crucial for trade, economy, welfare of the planet, law, order, and security. But principles and guidelines have already been negotiated at other forums (the OECD, the ISO, the ITU, the international centers to prevent and combat crime) and with much broader approach than in Resolution 53/70. Hence, Australia found it senseless to duplicate such work.

Belarus noted the timeliness of the resolution and backed the idea of negotiating the concept of international information security and principles aimed at enhancing security of global information systems and preventing cyber terrorism and crime.

Brunei emphasized the importance of information security in the age of IT, but assumed that the International Court of Justice should be responsible for determining the liability for violation of security of international communications.

Cuba pointed out that the process of computerization and new Information Age lead to new security challenges that should be considered by entire world community. The UN is an appropriate forum for such discussions. Besides, some measures should be taken to ensure access to new IT for development purposes, especially the access of developing countries.

Cuba presumed that the international community should recognize the right of any state to protect its information resources. Some multilateral treaties prohibiting aggressive acts against such resources may be concluded within the UN framework. It would also be advisable to consider the idea of agreements securing the use of IT to be developed for peaceful purposes and their availability to all states.

Oman stressed the right of the national telecom regulation authority to restrict access to public information through certain channels, e.g. the Internet. The legislation of this state provides for protection of material and moral value of information. Oman endorses the idea of negotiating international principles aimed at strengthening the security of information systems.

Qatar argued that general assessment of information security issues may be facilitated by exchange of technical knowledge and understanding of the danger of hacking, as well as its impact on security and finance. Some methods to ensure information security may include:

- encoding;
- use of software that provides control of access to data;
- verification of the user's right to access data;
- use of hardware and software means for network protection.

The Russian Federation submitted the most detailed document on this issue. It maintained that universality, secrecy, or depersonalization, opportunities for wide trans-border use, economical character and general efficiency made cyber weapons be an extremely dangerous means, whereas development and use of such weapons were not regulated under the modern international law. There is an obvious need for such regulation of global processes of civilian and military informatization, development of agreed international platform of actions on information security. Russia set forth the plan of actions of the international community providing for further debate on information security issues and adoption of appropriate resolutions by the UN General Assembly that would specify and restrict criminal and military challenges in this area. Russia also suggested that the parties should negotiate the principles of international information security (regime, code of conduct of the states, etc.), as some common approaches were achieved. These guidelines would first have taken the form of multilateral declaration and then might be transformed into international legally-binding document. Moscow also proposed to discuss these matters within the framework of the Conference on Disarmament in Geneva.

Saudi Arabia emphasized that rapid progress in IT led to the growing number of acts against normal functioning of information systems, their destabilization and interference for criminal purposes. Such activities damage economy and undermine security. Introduction of international principles and norms is important to resist information security challenges. The international agencies concerned should see to it that authors of such acts appear in court and are punished.

The United Kingdom mentioned the increasing interdependence of information systems in the world and noted that the majority of states were under threat of electronic attack by criminals or terrorists against vitally important elements of infrastructure.

As the use of computer systems is growing, such danger will only increase. The systems are connected at the international level, so the challenge is trans-border and makes a problem for all UN members. The United Kingdom welcomes the steps to study the appropriate mechanisms for repelling such threats, including multilateral mechanisms.

The British Government recognized the importance of international cooperation in this area. The dialogue on this matters includes the efforts of the G-8 Lyon Group on High-Tech and Organized Crime and the

Council of Europe (the draft *Convention on Cyber-crime*). The UK assumed that the UN should follow the debate at these forums and take it into account in its own work. The UN might devise international principles of strengthening security of global systems and facilitating combat against international terrorism and crime.

The United States regards the information security, as a complicated topic, afflicting many factors and activities of individuals, groups, and governments. Information security has some aspects pertaining to international peace and security, but it also covers technical aspects of global communication systems, non-technical issues of economic cooperation and trade, intellectual property rights, rule of law, struggle against terrorism and other matters subject to the consideration of the Second and the Sixth Committees. The United States noted that the methods of using electromagnetic pulse against the enemy were not new. In the future, the Armed Forces would pay more attention to protection of their own information networks. Besides, the states should be able to restore the information networks in case of emergency. Information security also affects the protection of data related to military might and other aspects of national security. The concept of information security should provide for the protection of results of commercial research, technologies and other confidential data (marketing plans, work with the clients) and should be connected with the international treaties regulating intellectual property rights. As for technical aspects, Washington assumed that the norms of the ITU and national agencies concerned ensured the reliability of international communication network. Appropriate standards guaranteed the rights of producers and users of electronic devices. The United States regarded the potential threat of criminal IT use, as a problem urgent for all nations, and shared the opinion on the advisability of unilateral and multilateral measures to ensure the security of respective resources.

The United States also assumed that any illegal interference or attempts to threaten its national information systems was a challenge to US national interests. Bearing in mind the potential gravity of this threat, the United State initiated a number of national programs in public and private sectors to protect the critical facilities and elements of infrastructure. At the same time, taking into account the global interdependence of infrastructures, national efforts would depend in the long run on the security of systems situated beyond the US territory. This is why the United States presumed that all nations should undertake national measures to punish criminals and terrorists operating on their territory and preventing normal functioning of information systems.

The problem of information security has many dimensions. It is absolutely significant to analyze all aspects of this issue, but it would be too early to negotiate comprehensive principles of information security. The international community should instead give a systematic assessment of the previous stages and then move forward. Hence, the states should strive to get to know the opinions of a wide range of experts.

Further international discussions highlighted, at least, two different attitudes towards information security.

Experts from developed nations, including the USA, pointed out the priority of measures to combat cyber terrorism and crime. They regarded the challenges of cyber weapons and cyber warfare mostly as theoretical. Hence, there was no need in discussing disarmament aspects of international information security. It was suggested that further debate take place at regional and functional forums (the EU, the G-8, the Organization of American States, the OECD, etc.). The UN should have studied these issues in its Second (economic matters) and Sixth (legal matters) Committees rather than in the First Committee.

The supporters of different course (mainly representatives of developing countries) endorsed the concept of complex evaluation of information security issues and backed the priority of curbing potential threat of cyber warfare. They emphasized the need to start immediate discussions and elaboration of the legal basis for the universal regime of international information security. It was suggested that the International Court on Cyber Crime be set up.

On December 1, 1999, the UN General Assembly passed by consensus the renewed Russian draft of the aforementioned resolution (No. 54/49). New provisions of the resolution, which also reflected the outcome of debate at the CD in Geneva, stated that information technologies might have negative impact on the security of the states with respect to their civilian and military spheres[10]. Thus, while the 1998 resolution only mentioned the existence of a common problem, the 1999 document was more specific concerning military and disarmament dimension.

The UN Secretary-General also submitted the appropriate report to the 55th session of the UN General Assembly (A/55/140). The document contained the positions of Jordan, Qatar, and Russia. Jordan stated the possibility of abuses of IT innovations and their use for terrorist purposes. In response, Jordan proposed to lay down special emergency legislation, so that security services might have access to the control centers of the companies dealing with such systems and supervise in part their activities.

Qatar offered some definitions concerning information security.

Russia put forward the draft of the document entitled "*Principles of International Information Security*". These guidelines comply with UN practices and conform to a number of documents on space matters approved by the UN General Assembly. These resolutions are not treaties, but place political and moral commitments on the states that have voted for them.

The Russian draft contains the terminology: definitions of basic terms, such as cyber weapons, cyber warfare, and information security. The key idea of the document is reflected in Principle I – activities of any state in cyberspace should contribute to common progress and should not contradict the task of maintaining global stability and security, security interests of other states, principles of the non-use of force, non-interference in internal affairs, respect for human rights and liberties. The document argues that such activities should comply with the right of everyone to seek, obtain and disseminate information. However, it is noted that such right may be restricted by the law in order to protect the security of any state. Moreover, all member of the international community should have equal right to protect their information resources and crucial infrastructure from unauthorized cyber interventions. The Principles also identify major threats to international information security and name the efforts that may contribute to the development of international legal basis to meet such challenges.

The aforementioned topic ("*Developments in the Field of Information and Telecommunications in the Context of International Security*") was included in the agenda of the 55th session of the UN General Assembly. This proved the interest of the global community in discussing this topical issue. The resolution adopted by consensus (No. 55/28) confirmed the previously approved recommendations. Paragraph 2 of the resolution stressed that such measures would be facilitated by examining the respective international concepts designated for strengthening the security of global information and telecommunication systems.

Many Western states showed restraint in endorsing further steps toward global information security and explained it with the complexity and novelty of the topic, as well as with concerns about possible constraints on the freedom of information exchange and competition on the IT market, which might allegedly emerge, if the concept was implemented.

Some Western analysts assume that massive cyber attacks may be conducted with regular PCs and opportunities granted by the Internet. The governments are not allegedly involved in development and control of such technologies. In other words, the international community today has neither technological capacity, nor legal mechanisms to identify the author of the attack and punish him. Moreover, the attacks may be accomplished via mediators (this was proved later – in April-May 2000 – during the hacker war between China and the United States). And vice versa: the third party may launch a cyber attack in such a manner, as to make guilty of it some innocent nations (as it was during the attack against Indonesia from the territory of European countries). Hence, they say, reliable, specific and practically applicable restrictions cannot be invented and introduced.

It is assumed that international legal norms applicable to armed conflicts, such as the principles of military necessity, proportionality and minimization of collateral damage, already regulate the use of IT in such conflicts. Therefore, there is allegedly no need in devising any new international principles. Besides, they argue that even if some states commit themselves to such code of conduct, this will not affect the criminal and terrorist challenges to information security. The criminals, by definition, do not follow international agreements.

Such position, in fact, removes from the agenda the issue of establishing the international system of information security. At the same time, if the world community does not come to an agreement on common approaches stated in the Russian draft of the Principles, the document may be regarded as a basis for the multilateral treaty establishing the universal regime of international information security. The key idea of such treaty would be the commitment of participants not to resort to activities in cyberspace that may damage information systems, processes and resources of other states, its critical structures, undermine political, economic and social systems, provide for massed psychological attack on the population in order to destabilize the society and the state.

The parties to such treaty should also refrain from:

- developing, production and use of means to influence and damage information resources and systems of other states;
- unauthorized interference in information and telecom systems and information resources, as well as their illegal use;
- activities leading to domination and control in cyberspace;
- restricting access to advanced IT, creating conditions for technological dependence in the sphere of informatization in detriment to other nations;
- promoting activities of international terrorist, extremist and criminal communities, organizations, groups or individuals that pose a threat to information resources and critical structures of the state;
- devising and adopting plans and doctrines providing for the possibility of conducting cyber wars and provoking arms race, as well as causing tension in relations among states and the outbreak of cyber war;
- the use of IT in detriment to fundamental human rights and freedoms in the information sphere;
- trans-border dissemination of information contradicting principles and norms of international law and domestic legislation of individual states;
- manipulating information flows, disinformation and concealing of information in order to distort psychological and spiritual medium of the society, erosion of traditional cultural, moral, ethical and esthetical values;
- information expansion, gaining control of national information and telecom infrastructures of other state, including the conditions of their functioning in the international cyberspace.

The treaty should then contain:

- the definition of characteristics and classification of cyber warfare, cyber weapons and related means;
- the measures to curb trafficking in cyber weapons;
- the regime to ban development, dissemination and use of cyber weapons;
- the measures to prevent the threat of cyber war;
- the provision on the danger of using cyber weapons against critical infrastructures and its hazardous consequences comparable to devastating effects of the WMD;
- the conditions for equal and safe international information exchange on

the basis of internationally recognized norms and principles of international law;

- the measures to prevent the use of IT for terrorist and other criminal purposes;
- the procedure for mutual notifications and prevention of trans-border unauthorized information influence;
- the conditions for establishing the system of international monitoring to detect the information challenges and the verification mechanism for the international information security regime;
- the mechanism for dispute settlement in the area of information security;
- the conditions for setting up the international system of certification of technologies and informatization and telecommunication means (including software and hardware), in order to ensure information security;
- peaceful development of the system of international cooperation among law-enforcement agencies in preventing illegal activities in cyberspace;
- the recommendations on voluntary harnessing of national legislations in the area of information security.

In accordance with the treaty, the states and other actors of the international law could be responsible for activities in the cyberspace under jurisdiction of or within the international organizations, whose members they are, and for the compliance with the provisions of the treaty.

The final goal of international efforts (and Russian initiatives are aimed at this) would be to declare the cyberspace a weapon-free zone.

[1] Although such approach exacerbates the problem of defining cyber attacks, since it claims to define the cyber weapons as an instrument of armed aggression, it may, however, be useful to determine the threshold of use of cyber attacks, as a legitimate means of influence under the UN mandate, if threats to peace emerge.

[2] O. Bringmann, *Information Operations-Legal Aspects*. Briefing. Germany.

[3] It is quite difficult today to distinguish between national and international infrastructure, for it is necessary to define and list numerous parameters and the very notion may have broad interpretation. This is why the interference in the work of national information systems affecting the functioning of international and global systems should be outlawed. It would be logical to adopt the international convention granting the cyberspace with the status of international protectorate, similar to outer space or open sea. Global information systems should be defined as demilitarized zones.

[4] O. Jensen, "Information Warfare: Principles of Third World War". *Airpower Journal*, Winter 1994, pp. 35-44.

[5] L. Greenberg, S. Goodman, K. Soo Hoo, *Information Warfare and International Law*. National Defense University Press.

[6] Navigation system and target designation equipment of B-2 bomber depends exclusively on space systems. However, its development has never been questioned from the point of the Space Treaty.

[7] L. Davis, "Arms Control, Export Regimes, and Multilateral Cooperation". In: *Strategic Appraisal*: *The Changing Role of Information in Warfare*, *RAND*, 1999.

[8] According to L. Davis, US military will be against any restrictions pertaining to new types of weapons, unless they have adequate assessment of its capabilities and expediency.

[9] Disseminated as an official document of the 53rd session of the UN General Assembly (A/C.1/53/3).

[10] A/54/49, December 1, 1999.

CONCLUSION

What is the adequate Russia's response to the emergence of cyber weapons and the threat of cyber warfare? The answer to this question should comply with the general policy of the state in the area of national security. There is an urgent need for new realistic national security policy in conformity with Moscow's limited resources. We believe that this policy should be based on long-term objectives and priorities of national development rather than on the Great Power ambitions – remnants of mentality of the past. Nowadays the stereotypes of thinking in terms of confrontation, as well as the corresponding principles and methods of maintaining strategic stability and national security impede the shaping of rational policy, which would take into account new realities and would meet Russia's national interests.

Russia strives to become an equal member of the community of democratic developed countries, find its niche in the international division of labor, and become a bridge between Europe and the Asia-Pacific. In military-political terms, Russia should remain the force maintaining stability in Eurasia. To achieve this goal, Russian military policy should provide for strategic cooperation with Europe, the United States, China and other nations in joint struggle against current and potential security challenges.

At present, national security issues are more and more connected with the problem of global security and, hence, should be resolved in the spirit of partnership and cooperation. The most significant area of such cooperation would be maintenance of international and national information security.

To work out rational policy in the area of information security, one has to make a realistic assessment of the current situation, particularities and prospects for the development of cyber weapons and the methods of their use. This is a basic prerequisite for formulating domestic and foreign policy of the state, whose military and military-technical units should be able to prevent and repel emerging threats and ensure the security of the state.

The threat of cyber warfare is a factor of clandestine military-political pressure and intimidation that may breach world and regional stability and security. This is why it is important to monitor the threats of use of cyber weapons and permanently assess the efficiency of functioning of the systems designated to resist such weapons. This monitoring should not only cover scientific and technological achievement concerning cyber weapons and means of protection, but also the dynamics of prerequisites and conditions for their possible employment, i.e. changes in the foreign policy situation, forecasts on global and local conflicts threatening with the possibility of cyber warfare.

A natural response to such new high-tech weapons would be the development of adequate means for counteraction. They should not be limited to technologies of detecting the cyber attacks, but also include early warning systems. These means should be complemented with the devices for counter-control of cyber weapons, as well as with different legal, organizational and economic measures aimed at protection of state information resources.

Economic and scientific policy of the state should also be considered in the light of information security. This policy should be open and should be aimed at protecting the legitimate rights of people to information and intellectual property, but at the same time, the state should support domestic manufacturers of technologies, who defend the internal market from penetration of secret cyber weapons.

In the age of globalization of information systems, any country cannot ensure economic flourishing without joining the international cyberspace. However, one has to realize that Russia's participation in international telecom and information systems will be imperfect without resolving the problems of information security.

Therefore, there is a need for international cooperation in negotiating and adopting legal documents ensuring information security in the processes of trans-border information exchange. It would be useful to support the activities of different international groups discussing various aspects of domestic and international legislation, international standards and possible areas of mutual interest in the information sphere. The international measures concerning prevention and liability for computer crimes should be agreed upon and become legally-binding.

It is obvious that one cannot prohibit the development and use of cyber weapons today, as it happened to CW and BW. Evidently, it is impossible to restrain the efforts of many nations to form single global cyberspace. This is why the solution would be to conclude reasonable agreements based on international law and minimizing the threats of use of cyber weapons. Such agreements, as a real contribution to international law, would strengthen the national security of their state parties. It would be useful to benefit from the experience of compromises and agreements pertaining to the prevention of nuclear war, missile threats and maintenance of strategic stability and balance of conventional forces in Europe.

ACRONYMS

BW – biological weapons
C3I – command and control, communication and intelligence
CD – Conference on Disarmament
CFE – Conventional Forces in Europe Treaty
CIA – Central Intelligence Agency
CW – chemical weapons
DOD – Department of Defense
EU – European Union
FBI – Federal Bureau of Investigation
FSB – Foreign Intelligence Service
FY – fiscal year
G-8 – group of eight developed nations
GDP – gross domestic product
GPS – global positioning system
ICT – information and communication technology
ISO – International Standardization Organization
ISP – Internet service provider
IT – information technology
ITU – International Telecommunication Union
MFA – Ministry of Foreign Affairs
MPSF – Moscow Public Science Foundation
OECD – Organization for Economic Cooperation and Development
PC – personal computer
RAS – Russian Academy of Sciences
START – Strategic Arms Reduction Treaty
SVR – Foreign Intelligence Service
TV - television
UK – United Kingdom
UN – United Nations
UNESCO – United Nations Education, Scientific and Cultural Organization
US – United States
USA – United States of America
USAF – United States Air Force
WMD – weapons of mass destruction