Information Technology: US/Russian Perspectives and Potential for Military-Political Cooperation

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

This article first appeared as a chapter in the book
Global Security Beyond the Millennium
Edited by Sharyl Cross, Igor A. Zevelev,
Victor A. Kremenyuk and Vagan M. Gevorgian

First published in Great Britain 1999 by MACMILLAN PRESS LTD
First published in the US 1999 by ST. MARTIN'S PRESS, INC.,

Posted to the Web with the permission of MACMILLAN PRESS LTD
(e-mail correspondence dated 21 Jul 99)

Advanced information technology (IT)[1] systems and weaponry have caused significant changes in the international security environment. The changes are monumental, and not all are positive. Non-state sponsored groups with access to advanced IT can present dangers nearly on a par with nations. A threat could originate from a drug cartel, warlord, or mafia group's attack on an IT such as a nuclear power plant, or from the chaos generated by a computer virus inserted into a country's defense (air defense, nuclear, and so forth) computer system prompted by a variety of agendas.

At the same time, situational awareness in nations with access to high technology is more complete than ever before. The ability to monitor conversations and movements is extraordinary and affects the character, speed and precision of diplomatic and military responses against all types of threats. Realizing the impact of rapid new developments in information technology on the emerging twenty-first century security environment, security officials in both the United States and Russia are trying to monitor and coordinate defenses and active measures. In the end, this will require closer coordination between the United States and Russia to ensure that one side does not misinterpret an event and send the world to the brink of an information war (IW).[2]

Following reconsideration of military priorities and national security interests as a result of rapid technological advances, both the United States and Russia elevated the protection of information assets to a strategic level. They also recognized the compelling need to master the speed of change in IT and to monitor its spread to rogue nations. IT change is reflected in restructured defense budgets, infrastructure reorganizations, and the security policies of these nations. Policy must address not only high technology threats from other nations but also the ability of terrorists

to affect national interests as national armies once did. Further, IT has upset traditional military considerations such as the employment of military art.

This chapter will discuss three IT related topics: Russian and US views of the impact of IT on military-political considerations; how both countries are managing IT concerns, to include civilian restructuring; and opportunities and challenges for US and Russian cooperation in IT. The discussion is important in that IT offers a threat similar to what Herman Kahn termed "spasm war" in *On Escalation,* an irrational, spasmodic response to an attack (whether nuclear or IT) on a power's C3I (command, control, communication and intelligence) before or during crisis.[3]

THE IMPACT OF INFORMATION TECHNOLOGY ON MILITARY CONSIDERATIONS

Russian Views

For Russia, the initial concern regarding IT was its impact on society, and on the strategy and tactics of the armed forces. Over the past three years, Russia has actively pursued a methodology for the use of IT as well to ensure military-political stability. The conditions (to a Russian, contradictions) that IT methodologies must address are the same as in the past: social, political, economic, territorial, religious, nationalist, and ethnic, among others. Security analysts recognize, however, that the form or manifestation of these conditions has changed, as each now relies heavily on IT. Thus, as Russia develops policy to protect its national interests, preserve its territorial integrity, maintain its national sovereignty, and protect its population, information security and IT sit at or near the top of its priorities. Real military power, for example, will not only be determined by the quantity of forces but by the qualitative parameters of the force, allowing for the implementation of IT to achieve interoperability in planning; to integrate technical systems that support command and control and logistics functions; and to successfully utilize indirect actions (economic sanctions, communications blockades, demonstrations of force, use of peacekeeping forces, and so forth) to supplement direct deployments and strategies.

The impact of IT (from a Russian viewpoint) on military-political considerations affecting national security takes many forms. First, information resources require effective state policies that monitor information security, especially since the use of IT may not involve physical damage or loss of life, making it more acceptable (no ecological fallout) than nuclear weapons.[4] Attempts to disrupt information exchanges or flows, the illegal use and collection of information, unsanctioned access to information resources, the manipulation of information, the illegal copying of data from information systems, or the unauthorized theft of information from data bases and banks are all threats that can disrupt economic or military relations between nations and require a serious response.[5]

Second, parity in nuclear forces now can only be achieved through parity in IT. Information warfare systems (including intelligence and information collection) have upset norms of parity based primarily on numbers and quality.[6] Intelligence, command and control, early warning, communications, electronic warfare, "special software engineering effects," and disinformation are issues that upset the traditional correlation of forces, and appear as a hidden form of miltary-

political pressure.[7] Superiority in IT, for example, could debilitate a nuclear coding or launch command procedure, making them unreliable or useless.

Third, Russia cannot allow a PSYWAR-IT (psychological warfareinformation technology) campaign to destroy the Russian economy. According to some Russian analysts, the US Strategic Defense Initiative (SDI) was an attempt to economically exhaust the Soviet Union by causing it to spend money it did not have on systems it could not use. Some Russian analysts view current United States interest in "information warfare" as another such attempt.[8] Russian analysts advise not to enter an arms race such as IW that is planned by other countries, but to devise military - technical priorities that are suited to the economic opportunities and strategic goals of the country. An IT strike against the Russian market is another threat in this category.

Fourth, Russia cannot allow IT and information operations to debilitate the nation's psychological stability, or to cause leaders to make incorrect judgments and decisions. Information currently presents a threat to society, the individual, and state institutions in Russia since the population is in a transition period and many citizens are psychologically vulnerable (that is, without a firm ideological basis). Control of the mass media is one manifestation of this threat.[9] The Internet is also a concern to some Russian officials, since it potentially can be used to commit crimes or unite political parties and groups against the government. Finally, if a country's decision-making cycle is damaged through computer network penetration and insertion of disinformation, governments or agencies may reach incorrect conclusions and decisions.[10] This is particularly dangerous in crisis situations when nations are working under extreme time constraints.

Fifth, and perhaps most important, IT's use in information operations blurs the Russian concept of the initial period of war. Since information attacks may be silent and capable of hiding their source or origin, planning for or responding to an initial period of war becomes treacherously complicated. What constitutes and differentiates the start of a crisis period, period of imminent war, and an offensive information operation, and how would one determine when or how an operation started? How does one determine with accuracy who delivered the attack? Should one respond with information actions against all probable enemies or only the most likely? How long can one delay a response before the entire information infrastructure of a country is under attack and a response is no longer possible?

Sixth, IT greatly enhances the military effectiveness of weapons systems and exploits point targets. Qualitative and quantitative indicators of weapon effectiveness have been replaced by the amount of informatization (digitalization, miniaturization, computer coding, and so forth) that a weapon contains, allowing huge amounts of information to be processed. IT raises the combat potential of precision weapons, and affects correlation of forces calculations since the ability exists, theoretically, to hit strategic point targets (nuclear weapons, command and control nodes, centers of political and economic significance) anywhere via cruise missiles. Computer viruses are another concern generated by IT. Many viruses and counter virus agents have been developed,[11] including a stealth virus.[12] By the year 2000, Russian scientists also expect to confront distance virus weapons, computer viruses introduced through radio channels or laser lines of communications directly into computers of strategic significance.[13]

Finally, IT has had a significant impact on military art. The spaceair-ground character of contemporary war includes satellites that process information and offer navigation assistance, and airborne sensors that detect movement and coordinate fires on ground targets. The center of gravity for military confrontations has changed from land and sea theaters of military action to the air-space theater. Warfare has a real-time aspect, requiring forces to acquire/engage/move. Formerly cyclical military operations (periods of intense conflict followed by periods of standown) will be replaced by operations that are less cyclical and more linear. Winners will acquire/shoot/move faster than their opponents for longer periods of time. IT also assists in overcoming uncertainty in war, producing streams of information allowing for accurate situational awareness, limiting surprise in the traditional sense, and offering IT landlords the perspective of a chess player peering five or six moves into the future. Most significantly, Russian theorists realize that military art must be designed not only for opponents who are equal in the use of information technology, but also for those adversaries who are superior or inferior to friendly forces in this respect.[14] IT and the infosphere, defined as a body of general and specialized programs for creating, processing, and storing computerized data, will be likely targets if war occurs.

US Views

For the United States, initial concern centered on how to employ or use IT, since America was dealt a superior IT hand from the beginning. Only later did the impact of IT on society and the nation's infrastructure become an issue. For example, the 1997 *United States National Military Strategy* refers to information warfare as an asymmetric challenge that could circumvent US strengths, exploit US vulnerabilities, or confront the nation in ways that could not be matched in kind.[15] This also prompted the creation of a presidential commission to study the problem. The response of the US military to this challenge was a conceptual warfighting template entitled *Joint Vision 2010*, which rested on information superiority and technological innovation, and strived to implement new operational concepts of dominant maneuver, precision engagement, focused logistics, and full-dimensional protection.[16]

The impact of IT (from a US viewpoint) on military-political considerations affecting national security are, first, that the security link between the commercial and military sectors has grown much closer. In order to enable IT strategies, the military had to link itself closely with civilian technology. The military-technical revolution and revolution in military affairs (RMA) actually started in the civilian sector, led by computer chip and optical fiber technology. Military applications soon followed. It became apparent, however, that since the military sector continued to rely heavily on commercial technologies and enterprises (such as phone systems), it was as prone to criminal attack as the commercial systems. This has forced both sectors to share more ideas on joint commissions, and to develop joint visions for information security systems to protect IT.

Second, an extended reliance on IT may invoke an asymmetric attack from a weak IT opponent. America was confronted by this eventuality during the Gulf War. Saddam Hussein, unable to counter the coalition's high-tech force, resorted to SCUD, chemical, and ecological terror as counters. A better equipped and prepared force than Iraq could inflict serious damage on an IT force, as the Gulf War demonstrated. IT weaponry is a technique but not an end-all. One Russian

has warned that an information attack against it will result in a nuclear strike against the source of the attack and the country that authorized the attack.[17]

Third, IT can contribute to maintaining an overseas presence with fewer forces. IT can provide a virtual presence almost anywhere in the world and monitor early indications and warnings of potential conflict areas or of treaty or international law violations. Overseas presence is provided by IT-equipped UAVs (unmanned aerial vehicles) and satellite surveillance. IT in a virtual presence role is supported by the worldwide presence of the US Navy, whose IT ability to affect ground operations has improved significantly, especially through the increased role of sensors and ships armed with cruise missiles. IT also supports the thinking of General Dennis Reimer, Chief of Staff of the US Army, who believes in strategic pre-emption, the ability to halt or prevent a conflict or crisis before it becomes debilitating or protracted - before it spreads out of control.[18] Pre-emption can contribute to shaping the environment diplomatically and economically, and can compel compliance with specific IT measures. The US learned prior to its intervention in Bosnia that modeling conflicts with superior computer graphics and virtual reality helped to compel compliance among the parties at the Dayton Accord negotiations. A three-dimensional computer model of Bosnia's terrain was developed and used by negotiators to show the presidents where the zone of separation must be located, and where their boundaries would be, with mapping provided by using real-time satellite images from flyovers of Bosnia.[19]

Fourth, IT allows for communications directly from the Pentagon to the foxhole, blurring the distinction between levels of action and complicating command issues. IT has produced communications achievements that are staggering. Senior officials in the Pentagon can now literally sit in on operations conducted by their forces or by others.

Fifth, IT is assisting in the discovery of new non-lethal weapons based on physical principles. The US military is working on the development of acoustic, vortex and microwave weapons.[20] Computers and recent advancements in miniaturized electronics, power generation, and beam aiming may finally have put pulse, electromagnetic radiation, and beam weapons on the cusp of practicality, according to some experts.

Sixth, IT has brought changes in several issues of military art. According to one analyst, some of the most significant are 1) an increase in the tempo of operations, which limits time for planning and decision making, requiring organizational, doctrinal, force structure, and technological changes, and adaptations to both regular and irregular operations to compel or enforce norms of behavior; 2) the extended use of robotic reconnaissance mechanisms (such as UAVs, Joint Surveillance, Targeting and Radar Systems - JSTARS) and precision munitions, which allow tanks and artillery to discard range and other targeting essentials (terrain, multiple shots for bracketing, and so forth) and makes battlefield awareness and management easier; 3) increased rates of movement with precision, allowing units to outpace an adversary's ability to react; 4) use of sensors on vehicles, which allows reporting to be instantaneous, and provides situational updates at the flick of a switch at higher headquarters; and 5) the ability of small units to employ the former combat power of a division, affecting the balance between combat power and manpower, the nature of command and control, and distinctions of strategic and tactical levels of war.[21]

Another analyst has noted that complexity, a spontaneous consequence of imposing regulation and control on a chaotic state, is the defining characteristic of modem military organizations and operations, and is controlled by the cohesion and integrating ability of information. Military art is affected in that the military uses information to describe itself and an adversary, to organize itself, to offer visual or situational awareness through extracting, processing, and distribution of data, to execute a mosaic of deep and protracted operations (operational art), and to offer the grammar, language, syntax, and logic of complex systems, making them not only understandable but showing their evolutionary qualities. Armies are complex systems that flow in a sea of information, and only the use of cybershock can stop the flow via operations security, deception, psychological operations, electronic warfare, reconnaissance and counter reconnaissance, and tempo and surprise.[22] IT can also be useful to train the force via computer simulations and virtual reality scenarios. Also, IT can be used in training the force en route to a crisis by offering computer-generated problems in accordance with the situation on the ground.

Seventh, centers of gravity in warfare have changed. Past strategies involved the concentration of one's forces at a particular time and place to win a decisive battle. Information centers of gravity focus on weaknesses in information infrastructures and equipment. IT's disabling capabilities prohibit forces from massing, planes from finding targets in a quick and accurate manner, strategies from developing, and decisive points from being located, calculated and attacked. These operations could occur in peacetime as well as wartime, according to some. The main point to recognize is that the greatest challenge for the policy maker will be to manage a national intelligence architecture, which can rapidly identify the information center of gravity, prepare the information battlefield, and deliver the appropriate (non-lethal) information munitions to carry the day.[23]

Finally, IT can affect the weakest link on the battlefield: the individual soldier's mind. The mind is not protected by a firewall as is the computer, and the ultimate operator of equipment, the soldier/leader, is offered little protection in the IT environment. There are two forms of protection required: one from physical attacks (electromagnetic pulses, acoustic weapons, voice synthesis, and so forth) and one from attacks on the perception capabilities of the mind. This is especially true due to the quick pace of development in the production of holograms. These can be used to make an army look larger than it is, or to make life-sized tank and soldier holograms appear to move and thereby confuse or intimidate soldiers. Hologram technology "uses a laser to illuminate an object and write its image into a photo-refractive crystal, while another laser projects that image into a liquid scattering material."[24] Holograms are also being considered for their value in propaganda productions, such as morphing images of political leaders. Soldiers require training to recognize misleading information produced from holograms, voice synthesis or other psychological tricks.

Other reports indicate that the computer-operator interface will be a crucial area requiring attention. Progress in neuro-muscular control, mind control and connectivity developments suggest additional areas of focus. The point to underscore is that the mind is vulnerable and, therefore, it is necessary to devote greater attention to the potential use of non-lethal or other information-based technologies.

MANAGING INFORMATION TECHNOLOGY

Russia's Responses

In September 1997, Russia's Security Council discussed the draft version of the country's information security policy. It consisted of five parts: general principles (legal basis and role of information in society); threats to the Russian Federation's information security (to the country's information infrastructure and information resources, especially technical and constitutional ones); methods of ensuring Russia's information security (legal, organizational, economic); government policy foundations for ensuring information security (openness, ownership, legal equality); and the organizational structure and principles for designing the system (an aggregate of federal government agencies and organizations to coordinate activities) to ensure the country's information security (strategy, evaluations, coordination, certification, licensing, and implementing a unified technical policy). This policy is the strongest element of Russia's response to its concerns over the use of IT by foreign countries.[25]

To combat information threats to Russia, primary responsibility lies in the hands of the Federal Agency for Government Communications and Information (FAPSI). This agency combats hackers, foreign special services, and domestic criminals who aim to gain unsanctioned access to information and to disable electronic management.[26] FAPSI's deputy director, Colonel-General Vladimir Markomenko, is the only official voice to define Russian IW to date.[27] His definition suggests that IW is the use of IT against the state in the form of special electronic and communication devices, hardware and software attacks, and other technical means.

The Russian armed forces are working on combining IT with older psychological concepts such as reflexive control (a means or method used to convey specially prepared information to a person, organization or country to influence the adoption of a predetermined decision desired by the initiator of the action). Some Russian analysts believe that a combination of information warfare and reflexive control offers a greater danger than the direct use of military power:

> The most dangerous manifestation of the tendency to rely on military power relates not so much to the direct use of the means of armed combat as to the possible results of the use of reflexive control by the opposing side via developments in the theory and practice of information war.[28]

The Russian military is proceeding to develop IT even in the current military and economic crisis. Some of the effort involves skipping over several generations of weapons. Russian military officers write about using IT to develop virtual realities and synthetic environments in military affairs. Virtual reality to one Russian officer is a complex set of artificial images of an environment (situations) that take place in a real time or close to real time scale, replicating processes that are created in the human mind by software and hardware means.[29] Current uses for virtual reality training include creating systems to synthesize routine, crisis and battle situations at various levels; creating means to generate models (for preparing information for decision-makers) to help forecast political and military -political situations in regions and different countries; developing forms and methods of conducting the armed struggle; creating systems to train officers individually or in groups; and creating means of psychological influence for individuals and the mass consciousness of people.[30] It is believed that from the use of virtual reality systems, one will look at a battlefield from a bird's eye view and from the enemy side,

providing an opportunity for preparing and running operations repeatedly in selected ways. Also, one can test weapon systems through virtual reality means before acquiring them. Virtual reality will also be used by the military leadership to improve doctrine and test personnel and equipment loss-free under varying climatic conditions, times of day, and levels of readiness.[31]

Russia's computer research and development process, which continues unabated, has produced some unexpected results unique to the Russian experience. One result is the neuron computer which, according to one expert, is expected to replace the pentium chip for speed and effectiveness in Russia. They are reportedly 1000 times faster than traditional computers. Military uses include the development of state-of-the-art high precision weapons, optic devices to detect missiles, and use in anti-ballistic missile (ABM) programs and dual technologies. In financial markets, the computers could make highly accurate forecasts (reported 90 per cent accuracy) of currency and futures rates, stocks and other securities.[32]

In other fields, the government's science and technology committee approved the following information-related fields as priority directions in the area of critical federal-level technologies:

- multi processor parallel-structure computers
- computer systems based on neuronet computers, transputers, and optical computers
- speech, text, and image recognition and synthesis systems
- artificial intelligence and virtual reality systems
- information and telecommunication systems
- mathematical modeling systems
- microsystem technology and mircosensors
- superlarge integrated circuits and nanoelectronics
- optical and acoustic electronics
- cryoelectronics production technologies
- laser technologies
- precision and mechatronic technologies
- robotic systems and micromachines
- electronic-ion-plasma technologies
- intellectual systems for automated design and control[33]

US Responses

President Clinton signed Presidential Decision Directive 39 (late 1995) and Executive Order 13010 (15 July 1996) to establish a President's Commission on Critical Infrastructure Protection. The commission was to develop a national policy and implementation strategy to protect critical infrastructures from cyber or physical threats. The commission received the report of the Defense Science Board for its consideration as well. By November 1997, the commission had written its report, distributed it, and disbanded. How the President will use the report remains to be seen. Critical infrastructures identified were: telecommunications, electrical power systems, gas and oil storage and transportation, banking and finance, transportation, water supply systems, emergency services, and continuity of government services.

High technology responsibility for protecting critical infrastructures and combating information threats to US society lies with the US National Security Agency (NSA), especially the relay of indications and warnings information to command authorities. NSA warns decisionmakers of potential threats. This responsibility differs from the period of the Cold War when one department focused signals intelligence (SIGINT) specifically on the former Soviet Union, and another focused on Asia. These missions are gone, and the new missions of these two departments are to combat criminals involved 1) in transnational issues, irrespective of geography, and 2) in attacks on the commercial sector's information resources. A new threat matrix uses IT as one of its principal combatants and operators. NSA is also responsible for identifying and combating threats to and vulnerabilities of technologies and infrastructures (such as telecommunications). The focus for NSA has slipped to the infrastructure of an adversarial force's operating capability instead of planes, tanks, and ships. Regarding the protection of commercial projects, NSA is to provide technical expertise on encryption standards for commercial firms and on systems for recovering data in secure environments.[34] Many of NSA's responsibilities correspond with those of FAPSI, noted above, to include the close relationship with IW. In 1996, John Deutsch, then director of the Central Intelligence Agency, announced his intention to create a cyber warfare center at NSA.

The US armed forces' major contribution to its information security was a report issued in 1996 by the Defense Science Task Board entitled the Defense Science Board Task Force on Information Warfare (IW-D). The board made 13 recommendations to the Chairman of the Defense Science Board.[35] The board members did not prioritize the key recommendations, deciding that all should be implemented immediately. The board recommended establishing a center to provide strategic indications and warning, current intelligence, and threat assessments. They also recommended developing a process and metrics for assessing infrastructure dependency.

The US armed forces' focus on the development of a high-technology fighting force, known as Force XXI for the army and listed under varying names for the other services. Army testing at the National Training Center in the Spring of 1997 yielded significant results that appear to have placed the development and fielding of IT systems ahead of schedule. The only criticism to direct against the army's approach is that it has somewhat neglected the psychological impact of IT on the soldier.

The US military, like Russia, is also pursuing the use of virtual reality mechanisms to create artificial battlefields and work on potential problems in advance. Known as the Joint Training Confederation (JTC), 12 interacting systems (such as the Air Warfare Simulation [AWSIM]; the Corps Battle Simulation [(CBS]; and the Navy's Research, Evaluation and System Analysis Simulation [RESAJ) were developed to train military forces of the US all over the world.

US research and development in the field of IT is focused on many items. Dr. Alvin H. Bernstein of the National Defense University divided technologies into pop-up (those that can distinguish threatening objects from decoys and then hide in their own signature) and fire-ant (the fiercely

stinging, omnivorous side of technology). He listed "pop-up" as signatures, platforms, stealth, drones, loitering missiles, autonomous land crawlers, and submersibles, and "fire-ant" as sensors,

emitters microbots, mini-projectiles, miniaturization, and integrated software.[36] Thus, the implication is that core research and development strategies must focus on electronics, nanotechnologies, energy, software that emphasizes integration, and manufacturing technology to produce counter-stealth technology, automatic target recognition capabilities, robotics, non-lethal weapons, and rapid power projection capabilities.

OPPORTUNITIES AND CHALLENGES FOR US-RUSSIAN COOPERATION IN INFORMATION TECHNOLOGIES

The Russian Draft Doctrine on Information Security indicated great interest in developing cooperation with other nations in the area of information security and technology. The doctrine notes that

> ... international cooperation on questions of ensuring information security is an indispensable component of the political, military, economic, cultural, and other forms of interaction of countries participating in the world community. Such cooperation should promote an increase in the information security of all members of the world community, including the Russian Federation.[37]

While it is unknown if the President's Commission on Critical Infrastructure Protection suggests cooperation or not, the US Defense Science Board report did not mention it. Cooperation is significant on a non-governmental level, however. For example, when Bill Gates, founder and President of Microsoft, visited Moscow in 1997, he discussed several cooperative ventures with his Russian hosts. His agenda included intellectual property rights and copyrights, and the use of Microsoft products in the Russian space agency, Central Bank, and various industrial companies. In an agreement with LUKOIL, a Russian oil conglomerate, it was decided to sign a general agreement defining a strategy for mutual cooperation.[38]

Governmental cooperation between the US and Russia in IT has moved more slowly. While there have been limited meetings at the highest levels to discuss some of these problems, there has been a heavy reluctance by the Pentagon and others to provide momentum to the process. Perhaps the Pentagon is in no hurry to share IW information because they are uncertain of tomorrow's geo-strategic arrangement. The fall of the USSR appeared to happen overnight, after all. On the other hand, any risk of giving away valuable information nearly has dissipated due to the vast amount of IW-related information available to the public. To date, well over 500 articles have been written by US analysts and scientists about US information systems and operations. Russians have been escorted to demonstrations of US advanced information-based and -supported artillery systems and even been briefed on information operations plans for a US theater.

While a variety of options exist, limited discussions do deserve to be explored in more detail, perhaps in a conference setting. Nuclear age discussions that proved so beneficial underscore the necessity of changing this reluctance. If computer viruses attack critical systems in the future, and appear to come from a state, when in reality an individual has sent the virus, will Russia and America launch nuclear weapons, as one Russian indicated their side would, because the sides didn't talk to one another? Without dialogue, the potential for improving global security is

undermined. By failing to work together in the management of IT, misunderstanding and fear are encouraged.

Opportunities now exist for dialogue, but such operations may become even more limited over time if suspicion builds. Russia's willingness to discuss these issues is tied to its domestic and economic situation. There are many conservatives in Russia, as in the US government, who still see a US footprint (and vice versa, Russian) on every issue under discussion today. Some believe that a massive information operation has already been conducted against Russia. On the other hand, there currently are scores of well-informed Russian leaders, academicians and analysts who do not see an American conspiracy everywhere they look, want to exchange opinions, and can offer a tremendous representative sampling of expertise on all areas of information technology and theory.

Yet another reason for dialogue is the number of ties that Russia maintains with so-called rogue states (Iran, Iraq, Yemen, Libya, and so forth). Russia may be best positioned to help control non-state sponsored sources of information terrorism. This could only help America, which is the number one enemy of most of these states. On the other hand, some fear that Russia would share US conversations on these topics with these states. Another fear is that rogue members of Russian society (willing to sell secrets to the highest bidder) may be an even greater threat. However, this may be a moot point if 90 per cent of this information is already available for public consumption.

Neither side can afford to wait much longer. New technologies are continually appearing that may make the future even more difficult to manage and unstable. The US is awaiting the arrival of asynchronous transfer mode (ATM) systems, which will revolutionize the way soldiers communicate. As one recent discussion concluded:

> What will technology provide during the next century? Is it quantum computing? Is it molecular or DNA computing? ... The key question is: what technologies, if any, will complement and/or replace the predictable silicon technology.[39]

Quantum computing uses the principle of superconductivity to increase the speed of computing and to reduce the heat that arises from millions of processing procedures (even small amounts of heat affect chips where size is measured in fractions of a micron). One Russian scientist working in America and sharing his discoveries in the field of quantum computing with his Russian colleagues estimated that by the year 2010 it will be possible to pack 64 trillion transistors on a chip instead of the 1995 figure of 64 million.[40] Clearly, this spiral will continue unchecked. It would only be prudent for both sides to establish a dialogue as soon as possible.

The use of IT has caused significant changes in the armed forces of both countries. General William Hartzog, commanding general of the US Army Training and Doctrine Command (TRADOC), reflecting on these changes, commented during the Task Force XXI Advanced Warfighting Experiment exercises at the National Training Center that:

> I don't think I've been involved in 34 years in anything even closely approaching this ... I don't think we have ever had as large, complex or holistic a look at things.

> There are lessons that we will pick out from this that we woulf have never seen in any other kind of exercise or experiment...[41]

The armed forces of both Russia and the US have weighed carefully the impact of IT on their operations, as the discussion above indicates. They are also monitoring the impact of IT on the security interests of their respective states, and adjusting policy and organizational arrangements accordingly. However, keeping pace with rapid advancements in IT will be a continuous and difficult proposition.

One of the ways to bring about an understanding of IT's impact on the civilian and military components of both countries, and at the same time lower the fears associated with technological advancements, is to develop an agenda for cooperation. The discussion above suggests several areas that require immediate attention.

First, both sides need to develop a common terminology in order to discuss with both precision and understanding the meaning and impact of IT on military -pol iti cal affairs. This should be the simplest phase for cooperation but, as peace operations have shown, it may be one of the most difficult. It took over three years for the two countries to develop a set of definitions to explain Russian and US concepts of peacekeeping, peace enforcement, and peace making. Today, these definitions are continuing to undergo change and modification, and there is no coordinating mechanism to update them. This only encourages misunderstanding. Without a doubt, Russian and US policy makers need to come to a common understanding of IT and IW terms. Otherwise, how will the sides be able to cooperate on, say, computer crime without unwittingly violating a legal issue for the other side?

Second, there must be an agenda to institutionalize the legal norms for not just Russia and the US but for all nations regarding IT and IW. What would constitute an information attack? What are the cyberspace borders that a country can consider as violations of sovereignty? What is considered to be IT theft in cyberspace? Are there IT developments that should be curbed or limited, and included in an IT non-proliferation agreement? There are literally hundreds of such questions to answer.

Third, an IT/information operations hot line should be established. The need for such a line was evident a few years ago when a student in St. Petersburg broke into the computer data base of Citicorps Bank and stole millions of dollars. As is well known, many such attacks go unreported today because banks do not want their clientele to know that their system is not 100 per cent safe. If this hacking occurs in the nuclear codes of either side, then the scale and consequence of the problem increases substantially. An information hot line would allow immediate notification between the two countries of a serious problem.

Fourth, discussions on the impact of IT on the military art of Russia and the US, especially in the areas of greatest concern (for example, the Russian understanding of the boundaries of the initial period of war), would be an invaluable undertaking. A good place to start work on this issue would be private military-political discussions or even a conference at the highest levels. Both sides could express their concerns and fears to sensitize one another to the impact of new IT developments on their national security policies. Such cooperation can only help reduce the

likelihood of misunderstanding and can quickly move important concerns to the top of the agenda. It will no longer be an excuse to admit if only I had known what my action meant to you.

Fifth, it is important to recognize that soon both sides will have the ability to use holograms and other IT manifestations that will offer the opportunity to completely fool one another both on the battlefield and through the airwaves, whether it be TV or radio, and the press. Both sides should begin initial discussions on these issues before they are overtaken by rapidly changing technological developments. A hacker simulating an incoming ICBM nuclear attack on the radar screens of the military of either Russia or the United States is but one manifestation of this threat.

Finally, both Russia and the United States should have advisors sit together and discuss two documents: the Russian Federation Draft Doctrine on Information Security and the President's Commission on Critical Infrastructure Protection. The sides could discuss areas of concern and potential cooperation. Both nations should learn a great deal from such a process.

This chapter has focused on US-Russian bilateral relations. Certainly, US-Russian decisions concerning IT will influence other nations and vice-versa. These suggestions for expanding US-Russian bilateral cooperation in IT could easily be extended to include other nations. This is not only advisable, but necessary, as nations approach the interdependent security environment of the twenty-first century.

ENDNOTES

1. Information technology (IT) is defined as all aspects of managing and processing information, and is characterized by the domain and tools of its usage. Two major components of IT remain hardware and software but IT's tasks, constantly being redefined, include processing, operating systems, network operating systems, data communication standards, high-speed communications, networking applications, the Internet, object-oriented technologies, and database technologies. This definition is provided by The Center for Research in Electronic Commerce (CREC, University of Texas at Austin (1998) (http://cism.bus.utexas.edu/ram/collab/it.html).

2. Some of the more important US works on information war include George Stein, "Information Warfare," *Airpower Journal* (Spring 1995), pp. 3139; John Arquilla and David Ronfeldt, "Cyberwar is Coming," *Comparative Strategy*, No. 12 (1993), pp. 141-65; and Martin C. Libicki, *What is Information Warfare?* (Washington DC: Center for Advanced Concepts and Technology, Institute for National Strategic Studies, National Defense University, 1995). Important Russian works on information warfare include Vladimir S. Pirumov, "Several Aspects of Information Warfare," paper presented at InfoWarCon 1996 entitled "Defining the European Perspective" (23-24 May 1996), Brussels, Belgium; V. I. Tsymbal, "Concept of Information Warfare," Academy of State Management, Moscow, Russia (14 September 1995); and A. A. Prokhozhev and N. I. Turko, "The Basics of Information Warfare," report presented at the conference entitled "Systems Analysis on the Threshold of the 21st Century: Theory and Practice," Moscow, Russia (27-29 February 1996).

3. See Lawrence Freedman, "The First Two Generations of Nuclear Strategists," in Peter Paret, ed., *Makers of Modern Strategy* (Princeton: Princeton University Press, 1986), p. 762.

4. Unless, of course, the information strike is against a nuclear plant, causing a melt down and greater damage than a nuclear blast.

5. "New Trends in Power Deterrence," *Armeyskiy sbornik,* No. 9 (September 1995), pp. 12-19 in *FBIS- UMA* (17 January 1996), p. 11.

6. Ibid., p. 12.

7. I. Panarin, "Troyanskiy kon XXI veka" (Trojan Horse of the 21st century), *Krasnaya zvesda* (8 December 1995), p. 3.

8. Georgiy Smolyan, Vitaliy Tsygichko and Dmitriy Chereshkin, "A Weapon That May be More Dangerous Than a Nuclear Weapon: The Realities of Information Warfare," *Nezavisimoye voyennoye obozreniye* (Supplement to *Nezavisimaya gazeta),* No. 3 (18 November 1995), pp. 1-2 in *FBIS-UMA* (6 December 1995), pp. 31-35.

9. Aleksandr Pozdnyakov, interviewed by Vladimir Davydov, "Information Security", *Granitsa Rossii,* No. 33 (September 1995), pp. 6-7 in *FBIS-UMA* (13 December 1995), pp. 41-44.

10. M. Boytsov, "Informatsionnaya voyna" (Information Warfare), *Morskoy sbornik,* No. 10 (1995), p. 70.

11. Pozdnyakov, "Information Security," p. 43. These viruses are Trojan horse, forced quarantine, sensor, and overload, and are described in the article.

12. B.P. Pal'chun and R.M. Yusupov, "Obespecheniye bezopasnosti komp'yutorynoy infosfery" (Providing Security in the Computer Infosphere), *Vooruzheniye, politika, konversiya (Armaments, Policy, Conversion),* No. 3 (1993), p. 23.

13. See Timothy L. Thomas, "The Threat of Information Operations: A Russian Perspective," in Robert L. Pfaltzgraff, Jr. and Richard H. Shultz, Jr., eds., *War in the Information Age* (Washington/London: Brassey's, 1997), pp. 69-73. For further discussion concerning these military considerations (initial period of war, and so forth) see pp. 61-80.

14. Grigoriy S. Utkin, "Synthetic Environments and Virtual Reality: The Russian View," paper presented at the seminar entitled "Military Applications of Synthetic Environments and Virtual Reality" (16-18 September 1997), Stockholm, Sweden.

15. John M. Shalikashvili, *National Military Strategy of the United States of America: Shape, Respond, Prepare Now: A Military Strategy for a New Era* (Washington DC: Government Printing Office, 1997), p. 9.

16. Ibid., p. 17.

17. Tsymbal, "Concept of Information Warfare."

18. General Dennis J. Reimer, "The Army and the Cyberspace Crossroads," *Defense Issues,* Vol. 12, No. 33 (http://www.dtic.mil/defe...nk/pubs/ di97/dil233.html).

19. "Powerscene: An Overview," Cambridge Research Associates, Inc., McLean, Virginia (November 1995). Also see Timothy L. Thomas, "Virtual Peacemaking: Conflict Prevention Through the Use of Information Technology" (September 1997), paper under consideration for publication in *Parameters.*

20. Douglas Pasternak, "Wonder Weapons," U.S. *News and World Report* (7 July 1997), pp. 38-46.

21. James K. Morningstar, "Technologies, Doctrine and Organization for the RMA," *Joint Force Quarterly* (Spring 1997), pp. 37-43.

22. James Schneider, "Black Lights: Chaos, Complexity, and the Promise of Information Warfare," *Joint Force Quarterly* (Spring 1997), pp. 2628.

23. Robert Steele, "Virtual Intelligence: Conflict Avoidance and Resolution through Information Peacekeeping," distributed at conference entitled "Virtual Diplomacy," US Institute of Peace, Washington DC (2 April 1997).

24. Andrew Gilligan, "Army goes to war with platoons of holograms," *The Sunday Telegraph,* London (I I May 1997), p. 5.

25. *Russian Federation Draft Doctrine on Information Security* (13 August 1997) in *FBIS-SOV Q* September 1997).

26. Aleksey Okhskiy, "FAPSI: Only Powerful Organizations are Capable of the Comprehensive Protection of Information," *Sevodnya* (8 September 1995), p. 3 in *FBIS-SOV* (28 September 1995), p. 20.

27. Vladimir Markomenko, "Invisible, Drawn-Out War," *Nezavisimoye voyennoye obozreniye* (16-21 August 1997), p. 1. Markomenko lists the functions of Russian IW (electronic warfare, electronic surveillance, hacker warfare and psychological warfare) and describes them in this article.

28. A. A. Prokhozhev and N. 1. Turko, "The Basics of Information Warfare," report at the conference enitled "Systems Analysis on the Threshold of the 21st Century: Theory and Practice," Moscow (February 1996), p. 251.

29. Utkin, "Synthetic Environments and Virtual Reality: The Russian View," p. 11.

30. Ibid.

31. Ibid., p. 12.

32. INTERFAX (14 February 1996) in *FBIS-UMA* (28 February 1996), p. 64.

33. Andrey Fonotov, "Science and Technology Policy," *Rossiyskaya gazeta* (8 August 1996), p. 6 in *FBIS- UST* (8 August 1996).

34. Barbara Starr, "U.S. Puzzle Palace Seeks New Clues to Combat Old Threats," *Jane's Defense Weekly* (3 September 1997), pp. 35-36.

35. "Report of the Defense Science Board Task Force on Information Warfare-Defense, Office of the Under Secretary of Defense for Acquisition and Technology," Washington DC (November 1996).

36. Alvin H. Bernstein, "Conflict and Technology: The Next Generation," National Defense University, unpublished paper.

37. *Russian Federation Draft Doctrine on Information Security.*

38. Stanislav Leonidov and Denis Kirillov, "Microsoft Increases Pressure on Russian Market," *Moskovskiye Finansovyye Izvestiya (14* October 1997), p. I in *FBIS-SOV* (9 January 1998).

39. Juris Hartmanis, "Roundtable: The Future of Computing and Telecommunications," *Issues in Science and Technology* (Spring 1997), p. 72.

40. Vladimir Pokrovskiy, "A Russian Scientist is Making a Quantum Computer but No One Knows in America or Here," *Obshchaya gazeta* (30 October-5 November 1997), No. 43, p. 14 in *FBIS-SOV* (9 January 1998).

41. Dennis Steele, "AWE: Testing Soldiers and Equipment," Army (June 1997), p. 28.