Chapter 4

Revolution in Military Affairs and the Strategic Environment of East Asia

The history of mankind is dotted with revolutionary changes in military affairs. They include the emergence of national armies in the Napoleonic era and *blitzkrieg* mounted by Germany during World War II. Now, another one called "Revolution in Military Affairs" (RMA), a product of rapidly developing information technology, known as info-RMA is emerging.

Factors that have triggered an info-RMA are the high-tech weapons and information revolution that demonstrated their power by the Gulf War in 1991 and the air raid in the Kosovo Crisis of 1999. Spearheaded by the United States, this movement is designed not just to equip troops with new weapons and information but to improve the efficiency through organizational and tactical reforms based on advanced information technology (IT), such as precision-guided munitions or advanced sensors. In September 2000, the Office of Strategic Studies of the Defense Agency of Japan drew up a report on RMA. Other major countries in the region (China and Russia) are also studying steps to be taken to realize an RMA.

With a view to keeping up with the advance in info-RMA, the United States and its allies are discussing its impact on the interoperability and U.S. forward deployment forces. It is necessary for Japan to cope with these changes.

1. What Is Info-RMA?

(1) RMA Demonstrates Its Power in the Gulf War and the Air Raids on Yugoslavia

Debate about the RMA was touched off by the 1991 Gulf War, where a nature of war of the new era was manifest.

During the campaign, U.S. stealth aircraft F-117 *Nighthawk* infiltrated the airspace above Iraq without being detected by its early-warning radar network; the laser-guided bombs fired from the platform of these attackers hit key targets with pinpoint accuracy; the *Tomahawk* cruise missiles launched far from the frontline

gave a crippling blow to the strategic facilities in Iraq. In the ground campaign, E-8 Joint Surveillance Target Attack Radar System (JSTARS) tracked a convoy of Iraqi tanks from the air, and night vision sensors traced the movement of Iraqi soldiers even during the night, enabling the U.S.-led coalition forces to mount an attack on the Iraqi Army. In addition, various types of high-tech weapons systems were used in combat, helping the coalition forces led by the United States to crush the Iraqi Army and liberate Kuwait with minimum casualties. Scenes of crippling damage inflicted on the troops and military installations of Iraq by these high-tech weapons were reported almost real time by television, which impressed the world how dramatically the conduct of war has changed.

The bombing of Yugoslavia by NATO aircraft in 1999 delivered a shock as devastating as that carried out in Iraq. During the air bombing campaign, Joint Direct Attack Munitions (JDAMs), guided not by their platforms but by the Global Positioning System (GPS) and designed to hit targets with pinpoint accuracy, were used. In addition, stealth aircraft and cruise missiles were employed. NATO forces also used non-lethal weapons, such as electronic conductible carbon-fiber "bombs" that crippled transformer substations by shorting the wiring. Thus NATO forces finally achieved their objectives with zero casualties on their part. With the realization of a profound change in the conduct of war, the concept of RMA is attracting growing attention worldwide.

(2) Emerging Theory of Info-RMA

Arguments about the RMA actually date back much earlier than generally thought — to the end of the 1970s in the Soviet Union. The Soviet Union by that time had discovered that NATO's military capability had been multiplied by improved performance of computers and sensors brought about by an advance in information technology, and that the conduct of war had undergone a revolutionary change. Then the United States pressed ahead with re-

search into military information technology that led to the development of precision-guided munitions (such as *Tomahawk* cruise missiles) and information gathering and processing systems (such as JSTARS). And the havoc these high-tech weapons wrought on targets during the Gulf War and the Kosovo conflict has heightened interest in the RMA. In the belief that another revolutionary change in military affairs is at hand, the United States started in the mid-1990s systematic exploration of RMA. *A Report of the Secretary of Defense to the President and the Congress 1999* points out that "the dawning of the Information Age has given rise to a new RMA sparked by leap-ahead advances in information technologies and information processing capabilities." The report calls it an "information-based RMA."

The Defense Agency of Japan has been studying the concept of RMA, and defined the concept as "the transformation in military affairs, including equipment, organization, tactics and training, designed to make a quantum leap in efficiently achieving military objectives, sparked by the application of advanced technologies to the military sphere, with information technology as its core." In other words, the RMA is not just equipping troops with new weapons or computerizing information. It is the transformation of the existing military by changing its organization and tactics on the basis of advanced information technology, and making a quantum leap in efficiently achieving military objectives by utilizing precision-guided munitions. A mere application of information technology to military affairs does not automatically lead to an RMA.

Characteristics of future wars fought by armies transformed by an RMA ("a post-RMA force") may be summarized as follows: Battle-space awareness capability is dramatically improved through sharing information real time among fighting units via a network equipped with advanced sensor systems (such as communications satellites and JSTARS) and a high-speed information processing system. The so-called "fog of war" will become thin, and each and every fighting unit will have instant access to precise bat-

tlefield information — its position and the situation surrounding it, as well as those of its enemy units. The fighting unit can hit the opponent with long-range precision-guided munitions, the minute it discovers military targets through such an information system. As attacks against enemy targets are launched by a platform most suitable for the given objective regardless of its affiliation, be it the army, the navy or the air force, a joint operational control can be established on a permanent basis. And the combat capability will be determined not by the performance of individual weapons (such as fighters and tanks) but by the capacity of its information system and precision-guided munitions supported by that system. It is conceivable that as robotics advances, unmanned aerial vehicles (UAVs) may be actively employed for the purpose of reconnaissance and surveillance of enemy troop movements and military installations or for such other simple but dangerous duties as the removal of land mines.

On the other hand, as the concentration of friendly troops increases the possibility of heavy casualties at a blow from enemy precision-guided munitions, fighting units have to be reorganized into more compact ones and located widely dispersed. However, these changes may impair the efficiency of operational control. In order, therefore, to organically employ widely dispersed units, they have to be commanded and controlled by a highly advanced information network. And by combining widely dispersed units and long-range precision-guided munitions by such a network, the firepower can be effectively concentrated on the opponent without physically concentrating friendly troops.

This can be accomplished only on the basis of an efficient flow of information through a centrally controlled network. And steps must be taken to check the enemy's interference of the information network of friendly forces. It follows that warfare takes on a new dimension — offense and defense of information — in addition to the conventional army, navy and air force. Therefore, not only the information system of the military but the computerized social in-

frastructure could become a target of an electronically guided attack. This raises the necessity to defend not just the information system on the battlefield but that of society as a whole, or conversely, the necessity to interdict enemy social infrastructure. And this has given rise, as a battle with the dimension of information added thereto, to the concept of "cyber-warfare," an electronically operated offense and defense fought in a virtual cyber-space created on a computer network.

2. Approaches Taken by Asia-Pacific Countries

(1) The United States Seeks to Integrate Information and Fighting Capability

The country that has a head start in tackling RMA is the United States. The heart of U.S. concept of RMA is "the system of systems." This is designed to bring about a multiplier effect by systemizing individual systems into an integral whole. During the Gulf War, the linkage of various systems — the reconnaissance and surveillance systems (such as JSTARS) and the precision attack system such as *Tomahawk* missiles — have achieved excellent military results. By drawing upon the lessons learned from that operation, the United States sought to fortify the linkage among various systems. Particularly, the United States sought to dramatically raise its combat efficiency by sharing real time "sensor to shooter" military intelligence gathered by Airborne Early-Warning and Control System (AWACS) and sensors of reconnaissance satellites and JSTARS with fighters and ground troops, and by instantly attacking enemy troops and military installations with precision-guided munitions.

In 1996, the Joint Chiefs of Staff (JCS) released *Joint Vision 2010* that described a future vision of U.S. armed forces. *Joint Vision 2010* did not use the term RMA, but the *Report of the Secretary of Defense to the President and the Congress 1999* referred to *Joint Vision 2010* as a conceptual framework of the RMA

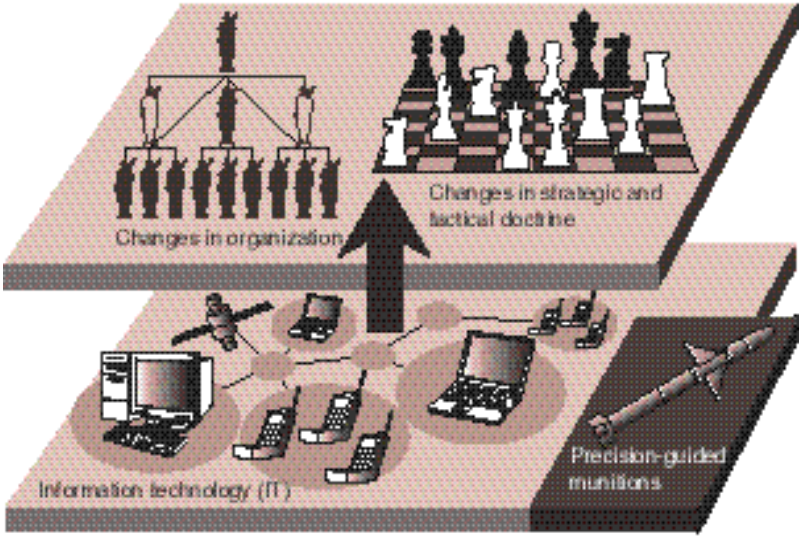
and characterized it as guidelines for RMA to be pursued by the United States. Assuming that the maintenance and strengthening of both forward deployment forces and power projection capability are still necessary in coming years, the *Report of the Secretary of Defense* stresses the importance of achieving information superiority by utilizing information technology and joint operations among the services.

It presents four new operational concepts — dominant maneuver, precision engagement, full-spectrum protection and focused logistics. It argues that to take and maintain a superior military position in full spectrum, ranging from peacekeeping to a large-scale conflict, these four concepts have to be realized. "Dominant maneuver" means combining highly advanced information gathering and processing capability, precision engagement capability and superb mobility, overpowering the enemy with a speedy execution of operations, and delivering a decisive attack against the nucleus of the enemy forces. "Precision engagement" presupposes real time availability of information concerning the strength of enemy troops and the battlefield environment gathered by taking full advantage of the information gathering and processing capability. Given that, precision-guided munitions carried by stealth aircraft are fired to accurately destroy enemy targets. "Full-spectrum protection" means to protect friendly troops and facilities by all means available at all levels of conflict — from peacetime to exigencies. It envisages the protection of targets not only against physical attack but against all other forms of attack, including attacks by biological and chemical weapons, and cyber-attacks against information systems. Last, "focused logistics" means to grasp real time data through an information network, concerning logistic support for troops deployed across the world, and keep them adequately supplied.

Under the guidelines set forth in *Joint Vision 2010*, all four services have published their info-RMA plans as follows:

Even before the publication of *Joint Vision 2010*, the U.S. Army

Chart 4-1. Conceptual Chart of Info-RMA



Source: Office of Strategic Studies, Defense Agency, *Info-RMA*, p. 6.

had been pressing ahead with a project called "digitalization of battlefield" designed to share information real time among its units by connecting them with a digital communications network. For instance, in August 1994, the U.S. Army Training Doctrine Command issued *Military Operations: Force XXI*. It showed the direction toward which the U.S. Army will move to cope with future wars under the assumption of a battlefield digitalization. In 1996, the army published *Army Vision 2010* on the basis of *Joint Vision 2010*. This applies the four concepts mentioned above to the ground operations and reviews the role of the army in joint operations described in *Joint Vision 2010*.

In 1998, the Army announced a new force structure plan geared to the progress being made in battlefield digitalization. This program envisages the digitalization of the existing heavy divisions by stages, starting in 1999 with the Fourth Mechanized Infantry Division stationed in Fort Hood, Texas. In the process, the personnel of a division will be reduced from 18,000 men to 15,700 men,

and its direct fire capability (including tanks) will be reduced. It is thought that the reduced direct fire capability and troop strength can be made up for by rapid mobility of troops and concentration of firepower that will be brought about by the digitalization of command and control. However, the Second Infantry Division stationed in South Korea will not be affected by the new restructuring divisions until 2009.

The U.S. Navy announced *Forward from the Sea* in 1997 in which the navy made it clear that it will attach importance to littoral operations, not ocean operations to which it used to attach the highest importance in the Cold War years. The principal operational concept of the navy is network centric warfare. This is a digitalized version of the data-link system, designed to enhance combat efficiency by sharing real time information among navy vessels and aircraft through a network. In this system, information concerning enemy targets picked up by sensors of other vessels or unmanned aerial vehicles will be shared real time with a vessel, which in turn can launch an attack on such enemy targets on the basis of information received from such friendly vessels or aircraft. The U.S. Navy calls this capability "cooperate engagement capability."

The U.S. Air Force has been operating an information network system called "Joint Tactical Information Distribution System"(JTIDS) since the late 1980s. The JTIDS furnishes its units with information concerning orders from the central command and control or the position of enemy and friendly aircraft, and helps improve combat efficiency. For instance, even if an aircraft deactivates its radar to avoid the risk of being detected, it can receive radar information real time from an AWACS, on the basis of which it can attack enemy aircraft, or it can get information concerning enemy or friendly troop movements that is out of its radar coverage.

Therefore, it may be said that the U.S. Air Force was equipped with elements of info-RMA, and it announced Global Engagement as early as 1996, in which it lists five elements — rapid global mo-

bility, precision engagement, global attack, information superiority and agile combat support — as important capabilities the air force should have to realize its future vision set forth in *Joint Vision 2010*.

In *Operation Maneuver from the Sea* announced in 1997, the U.S. Marine Corps describes new type of amphibious operations that employ tactics different from the conventional ones that land large units of Marines by landing craft, build a beachhead and then let them advance inland. The objective of the new amphibious operations is to make a surprise attack on key points of an enemy country by taking advantage of the Marines' high mobility in such a way as to cripple the fighting capability of, and demoralize, enemy troops. Playing a key role in this new type of amphibious operations is the tiltrotor aircraft MV-22 Osprey that has the vertical takeoff/landing capability and a larger carrying capacity at a faster speed than a helicopter. It is thought that by operating Ospreys from an amphibious ship off the coast, the Marine Corps can deploy its troops in an enemy country via air without landing them ashore and overpower enemy targets located inland.

After the air raids on Yugoslavia in the spring of 1999, several ideas were proposed to reflect the experience the Operation Allied Forces had had. Particularly, the U.S. Army was unable to deploy its troops rapidly and its ground troops had no chance to engage the enemy. From this experience, the army has become painfully aware of the limitations of its rapid deployment capability. To redress the situation, Army Chief of Staff Eric K. Shinseki unveiled a new *Army Vision* in October 1999, in which the army established a goal of acquiring the capability of deploying its troops to any part of the world within 96 hours. Under the *Army Vision*, the existing divisions will be reorganized into medium brigades that have the firepower of a heavy division and the rapid deployment capability similar to that of light units and the caterpillar vehicle units (such as M1A1/2 Abrams main battle tanks) will be replaced by wheeled vehicles. And as the first step, the army has decided to reorganize

the heavy brigade of the Second Infantry Division stationed in Fort Lewis, Washington.

In May 2000, the JCS announced *Joint Vision 2020*. As *Joint Vision 2010* did before it, the 2020 version centers around the four operational concepts and stresses the necessity of maintaining and strengthening the forward deployment force and the power projection capability, and for improving the fighting power by integrating the services by taking advantage of advanced information technology. However, while *Joint Vision 2010* stressed the importance of technological superiority, *Joint Vision 2020*, given the possibility of the United States losing its technological superiority, points out the necessity to secure its superiority not just by relying on technology but by striving to improve the competence of its personnel, change the organization of its armed forces and refine its doctrine. It is worth noting that it discusses the above mentioned concepts in greater detail, systematically incorporating information operation capability into them. And following the publication of *Joint Vision 2020*, the air force released its own *Vision 2020*, and the Marine Corps *Strategy 21*.

(2) Allies Seek Interoperability with the United States

America's allies have to address two problems relating to RMA. One of them is how to go about engineering an info-RMA on their own and the other is how to maintain the interoperability with that of the United States. Particularly important for America's allies is how to maintain the interoperability without falling behind the RMA of the United States.

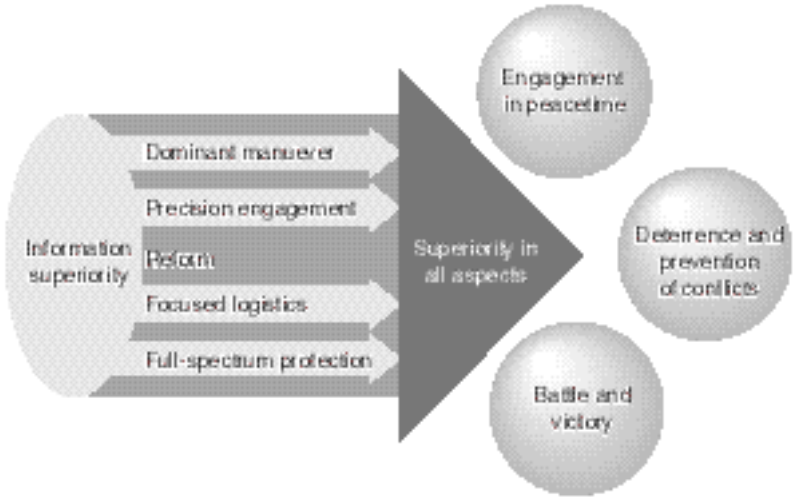
Japan has established a New Central Command System and an Integrated Defense Digital Network under the Mid-Term Defense Program (FY1996-2000) to strengthen the information and command communications capability of its Self-Defense Forces, but its systems and networks have been established not exactly with an RMA in mind. In September 2000, the Defense Agency (the Office of Strategic Studies) has issued a booklet titled *Info-RMA* that

spelled out its basic concept on RMA. However, the question as to whether the Self-Defense Forces will seek to develop an info-RMA will be considered in coming months.

Info-RMA of the JDA states that a policy aimed at achieving an info-RMA could become an important option in view of the four elements — (1) armed forces reformed with an info-RMA will be superior to a conventional one, (2) an info-RMA helps an armed forces minimize its casualties during campaign, (3) information technology of Japan is at a high level by world standards, and (4) the United States, an ally of Japan, is actively pursuing info-RMA. *Info-RMA* points out that as the RMA policy of the United States is primarily designed to maintain its forward deployment capability and strengthen its power projection capability, it is incompatible with the exclusively defense-oriented policy of Japan.

Given the difference in policy direction between Japan and the United States, *Info-RMA* of the JDA points out the direction toward which the RMA of this country should be developed on the

Chart 4-2. RMA Pursued by the United States



Source: Joint Chiefs of Staff, Department of Defense, *Joint Vision 2020*.

basis of six factors: — the consistency with Japan's defense policy, ensuring the interoperability between Japan and U.S. forces, the necessity to cope with the pre-RMA force, the diversifying role of the defense capability, the emergence of new weaknesses caused by the computerization of society, and the strict restriction on defense budget. With these factors in mind, *Info-RMA* enumerates seven principles to be observed in building an RMA. They are Information (information sharing through establishment of an information network), Jointness (joint defense capability), Speed and Mobility (increasing the speed of decision-making and maneuver), Efficiency (increase in units' combat efficiency), Flexibility (organizational flexibility), Protection (protection, redundancy and invulnerability), and Interoperability (bilateral operations with the U.S. forces).

One country that has been studying the feasibility of an RMA ahead of other U.S. allies is Australia. In *Australia's Strategic Policy*, its government states that "The so-called Revolution in Military Affairs (RMA) or the information revolution — much of which is being driven by commercial developments in the civil sector — is changing the nature of warfare all over the world." That said, the Australian government says that given its strategic environment, its first priority is to improve maritime surveillance capability by exploiting information technologies, and sets priorities in the order to defeat threats in its maritime approaches, the maintenance of its capability to mount attacks, and building ground forces. Areas to which it attaches particular importance are the improvement of the surveillance capability covering the huge area of its territory and maritime approaches, the enhancement of the capability of command, deployment and mobility to use its relatively small force to maximum effectiveness, the establishment of an information technology base, and the building-up of an efficient and effective military strength through access to cutting-edge military technologies of the United States.

The 1998 *Defense White Paper* of South Korea states that the

rapid computerization of information brought about by marked development of information technology has had a profound impact on the military and is raising interest in the emerging RMA. Particularly, South Korea has to contend with the threat posed by North Korea and unpredictable dangers to its security in coming years. And it points out that such being the outlook, it is necessary to transform the structure of its defense capability from the present large-scale material-based one to an information-based one. And its government plans to overhaul its defense structure in two stages: During the first stage from 1998 to 2003, it will have to use existing equipment continuously, mainly because of fiscal constraints while building defense capability to provide against future warfare. During the second stage starting in 2004, it will build defense capability largely based on an information system necessary to overcome unpredictable dangers in coming years. In addition, the South Korean government set up an RMA Planning Group in April 1999 to carry out research into the emerging RMA. However, the group has not come with any specific policy recommendation as yet.

Another problem is to keep the interoperability with the United States. The importance of this problem came to light during the bombing of Yugoslavia. Due to the large technology gap, no NATO ally other than the United States could carry out precision bombing missions or without the support of the United States.

The runway destroyed at a Yugoslav air base by a NATO air raid (USDOD Photo)

According to a report issued by the U.S. Department of Defense, 47 percent of the direct bomb-

ing missions during the air raids on Yugoslavia were carried out by NATO allies. However, 71 percent of support activities that were indispensable to carrying out bombing missions were provided by the U.S. Air Force. They include aerial refueling, control of Airborne Early-Warning and Control System (AWACS) to prevent confusion among friendly aircraft and near-misses with civilian aircraft flying in the area, battle management that allocates bombing targets, assessment of bombing results, surveillance of the movement of ground troops of Yugoslavia, choosing the next targets and support for electronic warfare. Moreover, as NATO allies either had no or only a limited number of precision-guided munitions, attacks of targets that required precision-guided munitions had to be carried out by the U.S. forces. What is more, as only the United States had the all-weather land attack capability, including nighttime bombing and stealth attack capability, the bombing of all important targets had to be carried out by the United States.

It was only the U.S. forces that had high-performance sensors such as unmanned reconnaissance aerial vehicles, electronic information gathering aircraft and JSTARS, which is indispensable to the surveillance of ground troops, to say nothing of reconnaissance satellites. Therefore, NATO allies had to rely almost entirely on the U.S. forces for military intelligence.

Even when military intelligence was shared among the countries participating in NATO's action against Yugoslavia, there arose another serious problem. NATO had 1,200 STU-IIs (secret radios), of which only 72 were deployed in the southern theater. And it is said that as a majority of them were used in Bosnia, only a few of them were available for use in the Kosovo. What is worse, as these STU-IIs were not interoperable with the STU-IIIB used by the U.S. forces, communications between the U.S. forces and other NATO allies were seriously hampered. In addition, the command and control network of the U.S. forces and that of other NATO allies were not interoperable, making it impossible to share secret intelligence.

It is feared that such problems could occur in the future between

the United States and its Asia-Pacific allies. As U.S. allies in the Asia-Pacific region, except South Korea, do not have the permanent command such like NATO, problems of a joint operation in the region may not be limited to the disparity in precision attack capability and the difficulty of sharing military intelligence. For Japan to effectively provide the U.S. forces with rear area support pursuant to the 1997 Guidelines for Japan-U.S. Defense Cooperation, it must work out an interoperability of the emerging RMA in anticipation of digitalization of the logistic support system that the U.S. forces are expected to undertake in coming years.

(3) China and Russia Seek to Narrow the Gap between Them and the United States

In China, also, interest in the emerging RMA runs high, and the *Chinese Defense White Paper of 1998* touched on it. Acknowledging that the development of high-tech weapons has brought about a profound change in the military field, it points out that many countries are attaching great importance to the qualitative aspect of military capabilities.

In China, opinions are supposedly divided into three schools of thought — the school of people's war, the school of high-tech warfare and the school of cyber-war. While acknowledging that the emerging RMA could dramatically change the way in which future wars will be fought, those belonging to the school of people's war take the position that it is impossible for China to follow the path of RMA given the country's low existing technological level. That said, in the belief that Western countries are quite sensitive to incurring war casualties, they argue that China should continuously employ the people's war strategy to fight against the RMA pursued by the United States. In other words, their thinking is based on the idea that China could counter an enemy force armed with an RMA by inflicting heavy casualties.

Those belonging to the school of high-tech warfare proposes building military capabilities almost symmetrically to match the

RMA pursued by the United States. While acknowledging the underdevelopment of its information technology, they maintain that determined efforts should be devoted to the modernization of China's Navy and Air Force. Mindful of the lessons they learned from NATO's air raids on Yugoslavia, they stress the importance of strengthening China's air defense capability. Given the fact that the major thrust of China's military buildup is directed toward coping with limited war under a high-tech environment by drawing upon the lessons learned from the Gulf War, the thinking of the school of high-tech warfare seems to be gaining consensus within the military establishment of China.

Those belonging to the school of cyber-war propose that China should wage a cyber-war in case of an attack by an enemy force armed with an information-based RMA currently pursued by the United States, instead of a frontal confrontation or the traditional methods proposed by the school of people's war.

What keeps the United States on the alert is this China's potential cyber-war capability. For instance, *Strategic Trends in China* published in 1998 by the Institute for National Strategic Studies, the National Defense University of the United States points out the importance China attaches to high-tech information warfare and predicts that China will acquire the capability to challenge information systems of other countries by 2015. On the other hand, however, it says that there is little evidence of major attention paid to other dimensions of the RMA such as networking sensors and precision-guided munitions, and dispersing its combat units across the country. If the thinking of this report is correct, it means that China is applying the results of its information revolution to military affairs by a method different from that of the United States.

The policy proposed by the school of people's war and the school of cyber-war is called "asymmetric conflicts." These schools argue that while the United States seeks to strengthen the conventional combat capabilities in the name of RMA, China can neutralize the military superiority of the United States by an entirely different

asymmetric approach, instead of countering by strengthening conventional combat capabilities.

It appears that Russia is attempting to use information technology to enhance jointness in operation and is trying to carry out measures to build cyber-war capabilities from the standpoint of national security. However, whether the Russian government is pursuing any concrete concept on RMA is still unknown. The *National Security Concept of the Russian Federation* published in 1997 makes no mention of factors relating to information-based RMA. Perhaps, Russia is too preoccupied with the rebuilding of its economy. However, it appears that aware of the disparity of its precision-guided attack capability with that of the United States demonstrated during NATO's air raids on Yugoslavia, Russia is trying to narrow the technological gap by its tactical nuclear force.

3. Impacts of RMA on the Region's Security

(1) The Future of U.S. Relations with Its Allies

As noted earlier, NATO's air raids on Yugoslavia in 1999 brought the disparity in combat capability between the United States and its allies to the fore. As information-based RMA gathered momentum, the disparity in combat capability has widened, and this is likely to touch off a change in the political and strategic relations of the United States with its allies.

It is said that U.S. allies have relied heavily on the United States for the supply of strategic intelligence gathered through reconnaissance satellites and signal intelligence (SIGINT). If a U.S. ally wants to improve its combat efficiency by fully utilizing the results of the RMA, it will, as it did during the air raids on Yugoslavia, have to rely on the United States not only for the supply of strategic intelligence but for gathering military intelligence on the theater and battlefield levels. It might be able to supplement its intelligence needs to a certain extent by installing a network of sensors on its own, but it will not be easy to create an intelligence gather-

ing and processing capability matching that of the United States.

Thus far, U.S. allies have relied heavily on nuclear deterrence provided by the United States, and they are highly likely to rely on the United States also for using their conventional forces effectively. In 1996, Joseph Nye and William Owens pointed out in their article in *Foreign Affairs* that an "information umbrella" of the United States is likely to supersede the nuclear umbrella. Indications are that this is indeed happening.

(2) The Future of Forward Deployment Force

Some observers who have participated in the debate over RMA divide the development of RMA into two stages and predict that the forward deployment capability of the United States will outlive its relevance and become unnecessary in the future. According to them, information sharing among, and application of high technology to, the existing organization and operations currently pursued by the U.S. armed forces are defined as the first stage of RMA. And the use of unmanned and stealth aircraft, and the extension of their flight distance are defined as the second stage. As long-distance bombing by unmanned aircraft will become the major vehicle of future wars, there will be no need to deploy ground troops to forward positions.

However, U.S. ground troops stationed in the allied countries will take on political significance as evidence of the U.S. commitment to the defense of allies. Moreover, in the case of a conflict, dispatching U.S. ground troops will be a means of last resort. No matter how much progress a country may have made in engineering an RMA, it cannot dramatically improve the speed of its transport or vessels to deploy its ground troops to areas of conflict. Therefore, it is necessary to maintain certain units of ground troops in an area adjacent to one threatened with conflict. Such being the circumstances, forward deployment forces will be necessary from the political and strategic standpoint, notwithstanding the progress being made in RMA. And a big change in the composition of forward de-

ployment forces is inconceivable at least in the foreseeable future. However, the possibility that the United States may try to reduce its forward deployment force to generate funds to cover the expenses necessary to carry out an RMA cannot be ruled out.

(3) Response to Asymmetric Warfare

The lessons the Gulf War and the air raids on Yugoslavia convinced some countries that they could not defeat the U.S. forces with conventional weapons. And opinions arose in Western countries that adversaries of the United States might challenge its hegemony by mounting a terrorist attack on its weak point in non-military areas, instead of provoking the United States into a large-scale conventional war.

Typical of such tactics is a cyber-attack. Opinions are divided as to whether a cyber-attack has a decisive effect in determining the outcome of a conflict. And the question as to whether a cyber-attack will constitute a condition justifying the exercise of the right to self-defense under international law will become an issue yet to be thrashed out. For instance, when a country sustains a cyber-attack, can that country mount a cyber-attack in retaliation or exercise physical force in retaliation? Such questions will have to be discussed.

(4) RMA and Japan's Defense Policy

The United States, a country most actively involved in engineering an RMA, has been taking various measures to strengthen its rapid deployment capability and long-range precision engagement capability to maintain and strengthen its power projection capability (namely, an efficient armed intervention in regional conflicts). Given the importance of coalition operations to be conducted with the U.S. forces to defend the security of Japan, it is necessary for the Self-Defense Forces of Japan to go along with such U.S. policy. On the other hand, as Japan is basically committed to the exclusively defense-oriented policy, the assumption underlying its ap-

proach to an RMA is far different from that of the United States. Thus, equipment and capabilities required by the Self-Defense Forces will be different from those of the United States. "Exclusively defense-oriented policy" means that defensive force may not be employed unless and until an armed attack is mounted on Japan by another country, and that the extent of the defense forces retained and the use of these forces is kept to the minimum necessary for self-defense. The exclusively defense-oriented policy is thus defined as a passive defense strategy that is consistent with the spirit of the Constitution. The geographic scope within which Japan can exercise its defense capability is not necessarily limited to its territory, territorial waters and airspace. Generally speaking, however, Japan ought to prepare itself for a defensive battle in its own territory. It follows that Japan's defense capability has to be designed to protect its land and civilian property as less as possible from collateral damage. Therefore, it is imperative also for Japan to acquire RMA type capabilities that mount a precision attack on the basis of advanced capability for battle-space awareness. In fact, the development of these capabilities should be a centerpiece of Japan's future defense buildup programs. Particularly, since assumed battle-space will be limited to the areas surrounding Japan, it is possible to densely deploy sensors for gathering theater and battle-space intelligence. The direction toward which Japan should pursue an RMA will be to enhance the objective achieving efficiency of its defense capability under the assumption of a joint operation with the U.S. forces by utilizing the capability for battle-space awareness thus acquired, by attaching importance to precision attack capability, and by carrying out reforms of tactics, organization and others.

It is necessary to re-emphasize that an information-based RMA is not simply utilizing the fruits of the IT revolution in the military field. A revolutional change can become a reality only when the Self-Defense Forces change its equipment, organization and tactics in light of that strategic environment it is in. In this sense, the

RMA may bring about the most far-reaching reform in history of the Defense Agency and the Self-Defense Forces in the future. To accomplish this, it is necessary for the Defense Agency and the Self-Defense Forces to foresee the future trend and tackle its reform with an open mind.