Shen Weiguang

Information Warfare

A New Challenge

The 20th century has been an extraordinarily turbulent chapter in military history. It has brought forth two world wars, and has witnessed a military revolution that began with classic infantry and cavalry combat and culminated in mechanized warfare. … Now, at the end of the 20th century, after barely having had time to pause and reflect on these events, we are already faced by a completely new form of war looming on the horizon: information warfare.

The transformation of Mechanized War into Information War has already begun

Since the fall of the Iron Curtain and the end of the Cold War–that is, since the dissolution of the two great power blocs–international military strategy has undergone a historically significant transformation that has lessened the danger of an outbreak of a world war in the classic sense. The chief emphasis of international relations and the main focus of general attention has shifted to economic affairs. International strategic relationships are no longer characterized by a face-off of two superpowers and an arms race; rather confrontation now takes place in the form of competition in business and disputes over cultural values.

Just as mankind was going about celebrating the end of the Cold War and beginning to call traditional military values into question, Western military powers under the leadership of the United States set in motion a new military revolution.

Any analysis of information warfare must be conducted in light of this military revolution, since only in this way is it possible to come to grips with the entire scope of this form of war. After all, the historical background is the basis without which innovation cannot emerge.

Every new age is the product of a technological revolution, and a technological revolution is the prelude to a new age. This is a law that applies to all social changes and developments; it is determinative of the logic of social occurrences. Humanity's military actions–its wars–have conformed to this pattern since time immemorial.

The technological revolution brought about by the smelting of iron enabled agriculture to advance, made possible the development of weapons of war, and ultimately triggered the revolution in the art of warfare engendered by the use of firearms.

The invention of the steam engine marked the beginning of the Industrial Age. Tanks and heavy artillery assumed their place on the battlefield. This meant the beginning of mechanized war–yet another historical quantum leap.

Microelectronics and the computer have led to the third wave of the technological revolution: the Information Age with its war of invisible projectiles and the latest military revolution.

This military revolution had already been foreseen in the late 1970s in the former Soviet Union. Marshal Orgakov, then chief of the Soviet Army's general staff, and several prominent military theoreticians predicted that the development of new non-nuclear technologies would lead to a revolution in the military field. They then went about incorporating computer-based information technology into military applications, and focusing increased attention on

targeting systems such as those for precision guided missiles. They proceeded under the assumption that an army equipped with these new technologies–which were then still in the development stage, and which would shake the foundation of accepted scientific postulates–would most probably be in a position to produce weapons with considerably more destructive capability than nuclear warheads. This would bring about a military revolution. Following the Gulf War in 1991, numerous American generals held the view that American military technology combined with Soviet military thinking had made victory possible in that war. This is an objective assessment of the fact that the military leadership of the former Soviet Union had been the first to recognize this latest military revolution.

Nevertheless, the initiative for the implementation of this military revolution proceeded from the Americans. Large-scale research efforts on the technical side of information warfare are currently underway in the US, and a wide variety of measures have been instituted to enable information warfare to actually become a reality. These include:

— theoretical research in the field of information warfare and the establishment of a strategy for its conduct,

— the set-up of an integrated C4ISR system (command, control, communication, computer, intelligence, surveillance, reconnaissance),

— top-secret research on aggressive information warfare,

— research on defensive measures, and

— simulations of information warfare.

Chinese military theoreticians were also among the first to deal with this international military revolution and information warfare. In 1983, Chinese researchers began to take up the revolutionary changes brought about by these new technologies. Over the course of this research, Plan 863 was implemented to create a positive research climate in the high-tech sector. Along with these efforts, theoretical research in the military field also began to yield initial successes.

As far as the term information warfare is concerned, this was employed for the first time in China. I began dealing with the concept of information warfare as early as 1985, and formulated the term "information warfare" (Chinese: *xinxi zhan*) in a scholarly paper. In April 1987, China's leading military publication, *Jiefangjun bao* ("Newspaper of the People's Liberation Army"), published an article entitled *Xinxizhan de jueqi* ("The Harbingers of Information Warfare") which elaborated on the results of my research. In 1990, my book *Xinxizhan* ("Information Warfare") was released by Zhejiang Daxue Press.

The Gulf War broke out shortly thereafter, and the military began to pay increasing attention to high-tech warfare. In China, various official military research establishments, non-government organizations, and army institutions have repeatedly held conferences dedicated to this military revolution, and have also been active on a broader basis to increase awareness of the significance, composition, unique features, and historical background of this revolution, as well as the actual ramifications it has for the military field.

As far as the concept of "information warfare" is concerned, there are a wide variety of definitions in use throughout the world. However, if we regard its fundamental meaning, all of

these definitions have a few aspects in common: the goal of an information war is the attainment of informational supremacy; information warfare is a form of combat that can be both offensive as well as defensive; the target of an attack is either the information system and its infrastructure or the process of information transfer itself. Information warfare can thus be described as follows: information warfare is a conflict in which two hostile sides struggle to attain supremacy in the acquisition, control and deployment of information, whereby the essential means employed are informational measures and equipment.

In 1985, I defined information warfare as follows: in the broadest sense, information warfare is a conflict in which combat-ready military (as well as political, economic, cultural and technological) units employ force to occupy the infosphere and dispute each other's access to information resources. This refers chiefly to activities whereby a state employs information for the purpose of attaining its strategic objectives. A practical illustration of this sort of information warfare is, for example, the end of the Cold War. In a narrow sense, this concept means the confrontation of two adversaries in the infosphere which takes place during the course of a war, and which is an essential feature of modern warfare. Here, it is possible to differentiate between strategic and tactical information warfare, whereby the former refers to a war beyond the "field of battle" on which actual armed conflict is taking place–that is, activities which take place in a conflict-producing political atmosphere, in the new "sphere of warfare." The target of an attack is the mind, the opponent's thought processes and, above all, that realm in which decisions are reached. Tactical information warfare, on the other hand, is conducted on the field of battle–that is, the command-and-control warfare, the war to achieve control over relevant pieces of information, whereby information itself constitutes the essential instrument of war. The objective is to attack the enemy's reconnaissance and information-gathering systems and to influence, knock out or modify the enemy's decision-making powers and the activities depending upon them. The manifestations of information warfare are highly diverse: psychological warfare, intelligence activities, strategic competition, theoretical deterrence, potential measurement of strength, electronic warfare, weapons systems designed to destroy the enemy's information infrastructure, computer virus wars, high-precision warfare, covert activities, etc. The chief feature which distinguishes the battlefield of information warfare from that of a conventional war is that it lies in an "invisible space." Information warfare is without physical form or bloodshed.

Information warfare encompasses six aspects: namely, acquisition, application, protection, use, concealment and administration of information. It has six essential characteristics:

— An information war is one which the warring parties conduct in the infosphere.

— Its objective is to achieve informational supremacy.

— The most important goal is to disrupt, weaken, sabotage or destroy the enemy's C4I system (command, control, communication, computer, intelligence).

— In information warfare, informational weapons and systems are the most important means of waging war.

— Information warfare very closely approximates real-time war; since it makes use of information systems, the theater of war is considerably expanded while, at the same, the concentration of military forces decreases correspondingly and the duration of hostilities can be reduced.

— The essential method of waging information warfare is the corruption of information.

In information warfare, supremacy in the informational sphere is one of the essential factors that are decisive for victory or defeat; it is a multiplier of power. Expressed in concrete, "battle field" terms, superiority in the informational sphere means the capability of using information in a timely, comprehensive and precise manner; the side enjoying superiority is thus in a position to use information at will. Viewed from a strategic perspective, this primarily means that techniques for the transfer and dissemination of information are exploited to the utmost in order to not only subvert the enemy's morale, but above all to disrupt and paralyze the general functioning of the opposition's political and economic systems.

A new View of War

The emergence of the Information Society alters conventional forms of warfare and, at the same time, vehemently calls into question the traditional conception of the nature of war.

Until now, war has been the continuation of politics–the ultimate form of hostility employing violent means to solve conflicts between social groups. Information warfare, however, is no longer just the continuation of politics; it is no longer waged only between peoples, states, social classes and political groups, but rather provides the preconditions which enable apolitical groups as well–and even individuals–to assert themselves and to accomplish their goals. Firms, religious sects, terrorist cells, tribal guerrilla bands, drug dealers or other criminal gangs can start a war. Any social group or private individual can launch an attack via computer, gaining access to systems linked to the Internet and using it to trigger a certain type of war. All that is necessary is mastery of the computer technology necessary for communication and availability of a computer and an Internet link-up via telephone. Therefore, it is necessary to perform a concrete analysis and investigation of political background factors before establishing the essential nature of such a war.

In the Information Age, distinguishing features with respect to the nature of war are also undergoing transformation. In conventional war, two chief categories were recognized: just and unjust wars. Any type of resistance against oppression and exploitation or to counter external aggression, and every war whose goal was social progress, was considered a just war. On the other hand, every war to suppress a revolution, one whose objective was aggression or external expansion, or a war seeking to hinder social progress was regarded as unjust. In the Information Age, however, many defining characteristics of war have become vague and undefined since it is often no longer possible to categorize certain armed conflicts, military actions or limited local wars as "just" or "unjust." The nature of war is thus growing increasingly complex.

The boundaries separating the preparation for and the conduct of war are also becoming less distinct in the Information Age. States striving toward hegemony prepare for war on a practically continual basis, and could therefore launch a war at any time. Campaigns to influence public opinion, counterespionage and Internet surveillance are actually nothing more than a modified form of military invasion; they are already a part of the conduct of warfare.

In the Information Age, informational deterrence constitutes a new variety of deterrence. Similar to atomic, biological and chemical weapons which display an extremely high lethal capability as well as considerable deterrent potential, the new methods and possibilities of

information warfare also contain a high deterrent potential and could, under certain circumstances, prevent the escalation of a war.

In the Information Age, information is a strategic resource of equal importance to material goods or energy; the information industry already constitutes one of a state's most important industries. Information has become a factor of production which has developed exponentially in relation to other factors of production. With respect to individual countries, regardless of whether they currently find themselves in the Agrarian or the Industrial Age, this means that they must orient themselves on the Information Age–either directly or by skipping one developmental stage. In the military field, the Information Age generates information warfare just as the era of heavy industry brought forth mechanized warfare. Regardless of one's current opinion on this issue, this is a matter of an inescapable historical development.

New forms of War call for Doctrinal Changes

In the military field, "information" also means "intelligence agency information." Although such information was previously just as indispensable to the military as it now is, men waging war in the past were forced to rely exclusively on the human brain to acquire and process information, to reach decisions, to issue orders, or to deploy and monitor armed forces. Only once it has become a matter of course that this entire process is managed by the human brain together with computers and networks can we speak of true information warfare.

The changes brought about by the development of mechanized warfare into information warfare manifest themselves first and foremost in a change in the form of war.

Troops' freedom to operate depends on informational supremacy An armed force's freedom to operate on the field of battle is an indication of the extent to which it has assumed the initiative in war. Initiative is commensurate with freedom to operate. Information warfare opens up a fifth dimension; that is, the initiative in war is shifted away from supremacy on land, in the air, at sea and in outer space to informational supremacy. In other words, only when an armed force possesses informational supremacy does it enjoy freedom to operate. Informational supremacy, however, cannot be equated with technical superiority and is not totally dependent upon it; rather, to a greater extent, it depends upon novel tactics and upon whether commanders are capable of independent, creative thinking.

The war's objective is selected with a view toward disrupting the enemy's capability to make decisions. In past wars aimed at the conquest of territory, the guiding principle was the destruction of the enemy's effective strength, whereas, in information warfare, it is axiomatic to disrupt the enemy's decision-making processes to such an extent that he can no longer effectively coordinate his activities. Taking this one step further, we conclude that the chief aim of information warfare is to attack the enemy's systems of knowledge and belief.

Firepower is no longer deployed on a saturation basis, but rather with pinpoint accuracy. Mechanized warfare, which reflects the production methods of the age of heavy industry, is a highly schematized form of war. In this respect, it resembles industrial assembly line production; that is, it proceeds in a highly coordinated and orderly, as well as inflexible and rigid fashion. The Information Society transforms the traditional forms of assembly line production, just as information warfare does to traditional schematized warfare. The essential characteristic of information warfare is that it is waged with precision and speed: the pinpoint attack directed at targets outside of the field of vision has become the fundamental pattern for the deployment of firepower. "Carpet-bombing," saturation bombardment, has been

consigned to the past; "surgical" structural destruction replaces the traditional form of schematized war.

Specialized units and specialized warfare gain significance. Specialized units represent a special organizational form of an armed force. They are characterized by flexibility, high efficiency, and minimal size.

The chain of command becomes increasingly flattened out. In information warfare, commanders must operate with extremely high efficiency, and this increased efficiency can be achieved only by means of a reduction in the levels of command. Consequently, it is necessary to break down the traditional multilevel, pyramid-shaped system of command. Computerization and network link-up of troops calls for the dismantling of the traditional pyramid-shaped chain of command and its replacement by a flat structure. Just as firms have reacted to meet the demands of the Information Age, the armies of many states are currently in the process of loosening up the top-down structure of their rigid command and control systems and setting up a new system that is capable of unleashing the dynamism of a flat command hierarchy and empowering officers and troops actually present in enemy territory.

In a theater of war that can be precisely delineated only with great difficulty, full use must be made of the power of the people. Information warfare is a war waged by means of high technology and one in which the entire people takes part. Thanks to the establishment of a worldwide data highway, non-government organizations as well as private individuals can use computers and information systems linked to the Internet and thus participate in information warfare. Regarded from a strategic perspective, a theater of war consisting of information is extremely difficult to precisely delineate. Soldiers are no longer called upon to storm enemy positions in hand-to-hand combat and can no longer boast of their heroic deeds. Perhaps computer programmers will withdraw to their offices or homes to carry on the battle from there. In war whose fronts become increasingly unclear, general mobilization and the utilization of the power of the people assume particular significance. It is precisely the cohesion of the people as a whole that imbues this form of warfare with its power.

The strategy of "total victory" advocated by Sunzi achieves consummate effectiveness in information warfare. War is a continuation of politics; that it is a bloody form of politics was recognized very early by mankind. Over 2,500 years ago, Sunzi was already seeking a way to wage war without bloodshed, formulating his famous stratagems "to triumph without fighting" and "if the troops are unscathed, then the victory is all-encompassing." But it is only with the advent of the Information Age that these concepts achieve full applicability. We cannot assume that a future war will be child’s play, but if technological progress furthers the process of the civilizing of society, then the concept of violence and the concrete application of violence will also undergo change.

The application of stratagems will become more multifaceted. Even if information warfare is waged by means of various public and military communications networks and media, technology is not the decisive factor determining victory or defeat; rather, the decisions made by human beings are. Combatants carry out highly concentrated, decentralized actions and implement closely coordinated, autonomous decisions. Proceeding in this fashion, however, presupposes that the commander possesses great creativity. Not only has progress in information technology not diminished the human factor, it has rather amplified it and made even more clear that command is an art. Since the identity of the foe cannot be definitively established, the setting is undergoing constant change, the rhythm of battle accelerating and the quantity of information increasing, the course of a future war will become more complex

and more difficult to grasp. For this reason, broad latitude is accorded to the implementation of stratagems.

New Aspects of War

In the silent struggle of information warfare, the mental aspect takes on tremendous significance. If intelligence and courage were the decisive factors in the past, then today it is intelligence first and foremost. Since this form of war constitutes a test of strength on the intellectual level, it is extremely difficult to make up for strategic errors by means of tactical or operational undertakings because, in the case of a failure on the intellectual level, information and control systems–the army's central nervous system–lose their effectiveness.

An additional aspect is that a "soft" strike becomes more important that a "hard" one. Since the objective of information warfare is to gain control over the enemy's systems of information and knowledge–above all, the thinking of commanders and decision-makers–and, simultaneously, to provide for one's own needs, one might properly speak of a "soft" strike of system versus system. If matters do not escalate beyond such a soft strike, then the war can be concluded without bloodshed. Therefore, it is incumbent upon us to succeed in transforming conventional warfare in which "the enemy is destroyed and one's own side is spared" into a war in which " the enemy is brought under control and one's own side is spared."

Furthermore, information warfare shifts in the direction of a people's war. The essential differences between a conventional war and an information war are that:

First, the target can be any individual citizen, but anyone can also participate in the war, and those involved could just as easily be regular army troops as young people.

Secondly, many pieces of equipment that are deployed on the "battlefield"–for instance, computers or optical instruments–are widely available commercially and were, in fact, originally developed for civilian use, and third, the war is no longer waged in traditional theaters of war by the force of arms, but rather permeates the entire society. Information warfare is a people's war in the truest sense of the word.

Fourth, information warfare calls into question traditional concepts of attack and defense. Indeed, considerable importance is attributed to the attack; nevertheless, defense is even more important. As a comparison of offensive and defensive information warfare reveals, one reason for this is that the attack is often concentrated on a single point whereas the defense encompasses an entire sphere and must defend against attack from all directions. With respect to defense, it is no simple matter to locate the attacker in the domain of computers. Moreover, the hidden threat emanating from such an attack is difficult to grasp, a timely prediction of it is problematic, and the results of defensive measures are hard to assess in advance. Furthermore, the conduct of information warfare as this is currently being discussed relies to a high extent upon electronics, which increases the vulnerability of national networks in the case of an information war. To this can be added the fact that in the Information Age, a preventive strike is more efficient than defense alone.

Fifth, strict definitions and conclusions are no longer possible in information warfare. Over the course of the continual improvement of information infrastructure, the boundaries between concepts that in the past were quite clearly defined (for example, public and private good, war and criminality) have become increasingly fuzzy. If an information war breaks out in a network-linked information system, borders such as those between states and regions lose

their function. It is hard to ascertain where a threat is coming from; indeed, it is even difficult to establish who has been attacked and who bears responsibility for that aggression. On the other hand, it is highly problematic to discriminate between the various levels of hostile action which can range from criminal activities to the conduct of war. In the future, the damages that could be inflicted by computer crime might exceed those that would result from a military attack, whereby the traditional division of responsibility between the government and the military as well as among the individual government ministries (e.g. the ministry for internal security, the intelligence agency, and the various law enforcement bureaus, etc.) suffer diminished effectiveness.

Sixth, there is one feature shared by conventional and information warfare: namely, that the nation which possesses the ultimate weapon–such as the atomic bomb–has the capability of delivering a first strike or a retaliatory attack. The same applies to information warfare; here as well, there are a series of key technologies for both offensive and defensive purposes. It is impossible maintain superiority in all areas of modern weaponry which are undergoing change on a day-to-day basis; nevertheless, they ought to be part of a nation's arsenal to be actually deployed or used as a deterrent. In the future, a series of directives should be issued which regulate information warfare and which all parties to a conflict must abide by. Information warfare is merely a test of strength; it cannot be permitted to be detrimental to the well-being of humanity as a whole, and especially not to human beings themselves. I am convinced that those who make some future decision that proves injurious to all of humanity or who issue such orders will turn out to be the first victims of such an attack. Social development, the consciousness of humanity, and technological progress are in a position to make good on this.

Changes in the Nature of an Attack

In the Agrarian Age, an army that had sufficient manpower available to protect its territory created an infrastructure which guaranteed the military security of that territory. In the wake of the rapid developments of the Industrial Age, it has become impossible to guarantee the military security of a nation solely by equipping the armed forces with state-of-the-art technology such as tanks, warships, missiles armed with atomic warheads, etc. Rather, a state also had to possess certain economic resources and a fast, comprehensive system of military mobilization. In the Information Age, military security has been confronted by a previously unknown challenge.

Information warfare pursues goals which differ from those of conventional war. In the Agrarian Age, the aim of war was to destroy the opposing army, whereas in the Industrial Age, the objective was not only to destroy the opposing army but also to demolish the military potential that enabled the enemy to continue to wage war. In the Information Age, the primary targets of attack are the opposing state's computer systems which link together political, economic and military installations as well as all social institutions.

The Gulf War has been characterized as a primal form of information warfare or as a war of the "third wave"–not because computerized weapons were used to fight it, but because military thinking underwent a major transformation as a result of it. Allied troops went about their selection of targets differently than in the past and first attacked the enemy's information systems by means of informational weapons.

In the Information Age, the boundaries between preparation for war and the waging of war are gradually becoming blurred. Heretofore, every aggressor who wished to start a war, and

every defender who wanted to repel an invasion, had to make involved preparations including training of the populace, setting up a comprehensive system of mobilization, formulation of war policies and plans, the development and production of new weapons and the installation of the infrastructure of war. Warfare itself was a constant process of gunfire and bloodshed. Above all during the Industrial Age, a war of this kind bore a certain resemblance to assembly line production. In information warfare, preparation for and conduct of war blend together. States striving for hegemony are occupied with preparatory tasks virtually on a daily basis, precisely as if they would be waging war. In going about this, they make use of the most diverse methods: bribery of foreign weapons producers, and sale of virus-contaminated chips to nations they want to get under their control or which they regard as potential enemies; or the purchase of weapons factories in order to equip the weapons with contaminated software, etc. This sort of preparation for war has revised the actuality of a formal military invasion and has become part of the conduct of war itself.

Such developments suggest the following conclusions: in the Information Age, the chief military threat does not consist of enemy troops menacing the state's borders or carrying out an ominous military build-up; rather, this threat is posed by a sudden attack from the net. This is an attack on the "central nervous system" of the state and the military, an attack carried out "face to face." The target nation does not even know who the foe is, where the threat has come from, or when the war actually began.

Political Security and Media

In evaluating the security of a state, its political security must also be taken into consideration. Politics is the totality of all activities of the various classes, political parties and social groups, whose goal is to provide for the common welfare, to organize and consolidate the authority of the state, and to govern the country by means of state power. All of this is unthinkable without information. Information strengthens the cohesion within a state and the power of a state, but it is also a weapon that can break down the cohesion of a state and threaten a regime.

In an agrarian society in which productivity is underdeveloped, individual regions of the land are not in constant contact with each other, and there is only a limited exchange among the inhabitants, the dissemination of information was essentially a matter of verbal communication and postal stations. The flow of information from the battlefield to society at large was therefore highly limited and quite slow, which made it easier for government authorities to exert control, to insulate themselves, to erect monopolies and to establish a highly centralized form of administration. A regime could thus maintain stability and security over a relatively long period of time.

In the Industrial Age, the situation is completely different. Due to the development of information media, the expansion of the quantity of information, and the acceleration of the information flow, the number of human beings capable of exerting an influence on politics has grown tremendously. This aspect has a most favorable effect on the process of increasing democratization; on the other hand, political conflicts become more numerous and political insecurity rises correspondingly. Since nowadays, the communications media are essentially controlled by the ruling class, subversive activities–of both domestic and foreign origin–manifest themselves primarily in the form of a struggle for the mastery of public opinion.

In the Information Society, social, political and economic life in its entirety is transferred into computer networks. On one hand, this makes political processes more transparent and raises the level of democratization; on the other hand, however, political security is subjected to an

unprecedented level of pressure. The development of a symbolic economy of information leads to a dramatic increase in the number of channels between the various classes and social groups, between different regions and states.

The globalization of media systems radically weakens the influence of previously monolithic media, publications and technologies. Consequently, the information monopoly of governmental groups is broken up, and social groups and individuals get the opportunity to participate directly in the political events of their country or of any other land. In this decentralization process, political power undergoes an almost imperceptible shift.

Furthermore, the boundaries between national and international politics become blurred in the Information Age. The political security of a state is subjected to a varying degree of influence and pressure from international politics. At the same time, the rapid development of information technology makes more economical and more practical ways and means available to states striving to achieve hegemony to play power politics. The political security of Third World nations is thus confronted by a new challenge.

The Threat from the Economic Sector

Politics is the concentrated manifestation of the economy; the economy, in turn, is the basis for the existence of any class, nationality, state and political group. Based on the precept of "peace and development," economic security has become the quintessential question of national security.

In an autarkic agrarian society, the economy was essentially self-sufficient and independent. Except for climatic factors, there were hardly any external influences on economic security. A large-scale intensification of production and a very precise social division of labor was instituted during the Industrial Age. At long last, the portals of these lands were opened to commercial wares which had been excluded up to this point, and closer international economic relationships developed. The production of an auto might now involve a design created in America, the chassis might be manufactured in Europe, with Asia contributing the motor and assembly taking place in Africa, whereupon the finished product is brought to market. On one hand, this furthers cooperative effort; on the other, the economic security of the individual states is somewhat threatened.

In the Information Society, the economic security of individual states faces an even greater challenge. Developed countries already find themselves in an Information Society, or at least in a postindustrial or pre-information society. "High geopotential outdoes low geopotential" is a rule that applies to economic competition. It is thus a historic necessity to solidly ensure the short-term and long-term economic security of a state by quickly creating productive structures, the backbone of which is the information industry.

The integration and simultaneous regionalization of the global economy leads to a high degree of dependence and fragility on the part of the economies of individual states. In the hard-nosed competition of the information industry, considerable differences in the field of technology can emerge among the developed nations as well, whereby the mutual interdependence is strengthened even further. This interdependence of national economies constitutes a threat to the economy of each individual state–the greater the dependence, the greater the threat.

In the Information Society, computerization and telecommunications lead to a fusion of previously discrete sectors such as finance, marketing, goods, technology, labor, industrial facilities, services, leisure and production. An assessment of the current state of technology makes it apparent that these computerized networks are highly vulnerable and can easily be attacked by hackers. If a hostile nation initiates organized, targeted criminal activities in the Internet, then this can result in the collapse of the targeted state's economy. This scenario is by no means pure science fiction. Evidence exists that certain states are already working on the development of so-called superviruses and electromagnetic impulses which could attack, at some desired point in time, systems such as banks, securities exchanges, air traffic control, telephone, television, power plants and electric power networks, etc., and thus paralyze a nation's economy.

The question of a country's "economic security" comprises an evaluation of a wide variety of threats both foreign and domestic which confront its economic system; indeed, these threats could even stem from the economic system itself.

Cultural and Ecological Aggression

Social security is intimately interrelated with political and economic security.

Culture is the "glue" of society, the foundation that ensures social stability. Culture created by human beings permeates all spheres of social life, bringing forth social norms and social systems. Human beings living at a particular time and making up one people all live in a certain cultural model.

The development of information technologies and media accelerates the dissemination of cultural conceptions and the process of reciprocal cultural absorption and fusion. At the same time, though, there are also individuals who employ modern network technology in order to distribute, for example, a "pornographic culture." This constitutes, without a doubt, an attack upon the moral and cultural norms and values of a traditional culture. Chaos on the cultural level can ultimately impair social security. In the transition to an Information Society, a nation can also be subjected to social shocks, whereby such upheavals can assume even greater proportions in developing countries. But regardless of whether a nation is still an agrarian society or is already an industrial one, no nation can proceed along its path of development in quiet isolation during the Information Age. A land has a chance to survive only in an atmosphere of openness to the outside world.

According to the theory of the self-organization of systems not in a state of equilibrium, a system undergoing a process of development which is currently in a stable stage of quantitative change must necessarily be in the controlling position; if, however, the system approaches the critical point of quantitative change, then it finds itself coincidentally in the controlling position. This means that the deeper a reform goes, the more numerous are the random factors.

In the Information Age, wealth accumulates faster than in the Industrial Age, whereby the gap between rich and poor constantly expands and endangers social security.

In discussing the question of social security, we must not underestimate the problematic issue of ecology.

The advent of Information Society by no means provides relief from the pollution and hazards caused by Industrial Society. Quite the contrary: new sources of contamination are added to previously existing ones since the development of information technology is accompanied by new forms of environmental pollution such as contamination by electromagnetic radiation. Those western countries that have attained a high level of industrial development and in which the information industry is rapidly evolving have–due to necessary restructuring measures–transferred industrial sectors with a high pollution potential out of their own territories and relocated them in developing countries where they have caused severe environmental damage. The hard facts of economic development already enable us to perceive quite clearly that the development of a state and its ecological security are tightly interwoven. Security is the guarantee for development, but development, in turn, provides the preconditions for security. Along with scientific and technological development and the onset of the Information Age, an ecologically intact environment will be a key issue of social and, indeed, national security.

A Few Thoughts on the War of the Mind

Every war has its point of origin in the mind. Those who plan wars and issue orders, and those who translate those plans and orders into practice, are all beings whose actions are controlled by thought processes in the human mind. All past and future wars have their source in the minds of men. If we wish to limit and abolish wars, then we must, on one hand, search for an answer in the objective world. On the other hand, we must also seek the cause in subjective human factors; that is, first and foremost, we must analyze and eradicate the causes of war in our mode of thinking.

The human brain wages war–regardless of whether consciously or unconsciously, regardless of whether as the outcome of one's own initiative or not, regardless of whether actively or passively, though always following a bitter struggle: the battle of thoughts in the human brain. The war of thinking includes both the war within an individual's brain as well as the battle between different brains. The basic unit in the war of thinking is: human brain + external brain (thought storage unit) + electronic brain (computer).

If one proceeds under the assumption that total information warfare constitutes the highest stage of information warfare, then the war of thinking is the lowest stage of information warfare and simultaneously the most minute entity in the structure of information warfare. Every information war is composed of innumerable larger and smaller wars of the mind.

A future world war–total information warfare–begins with a war of thinking. The duration of such a war, who wins and who loses–all of this depends on the extent of the victory or the destructiveness of the defeat in the war of thinking.

The most bitter, most interesting and most decisive phase of such a future war is the war of thinking. If it were possible to limit the war to this domain, then the combatants could decide already at this stage who wins and who loses.

Will war ever become extinct? The answer is no. Since the dimensions and the content of the concept of "war" are undergoing incessant transformation, war will remain a constant companion of mankind. As long as human beings think, as long as they have a mentality, war will never die out. Naturally, war's form and content will constantly change, and traditional forms of war will continually be replaced by new ones, just as mechanized warfare has been succeeded by information warfare, whereby the half-life here as well becomes ever shorter.

The 21st century will be the one in which the war of thinking, the "war of the mind," will unfold to the fullest.

"Firewall" and "Information Frontier"

The domain of information is brimming with energy and power. The regionalization of finance and trade, and the swift progress being made by the process of globalization have necessitated a rapid increase in the quantity of information. All over the world, 10 billion units of information are transmitted every day; the annual "information output" comes to approximately 72 billion units, and this figure is rising by 10-15% each year.

Regarded from the perspective of national security, the concept of national borders gradually becomes less clear with the worldwide expansion of networks. This nullification of boundaries has direct consequences for national "sovereignty" with respect to communications, information, and the ability to maintain state secrets. The Internet–that world-spanning network that exerts the greatest influence, boasts the largest number of users and provides the richest content–is a new continent that knows neither borders nor treaties; it is a world that is only gradually taking shape, and one whose final form has not yet been established. In this *terra incognita*, information warfare is still a complete novelty that is indeed developing rapidly but is not yet defined in all details. In the Information Age, war's primary targets are a nation's computer networks which link together its political system, economy, armed forces, and other spheres of society. Thanks to modern technologies, these can be attacked invisibly and with tremendous speed via a number of different channels simultaneously and in a wide variety of ways, so that the enemy can be "defeated without a fight." Therefore, if one invokes traditional theories oriented on a formal, physical concept of space in order to explain the "territory of information" and to define the "frontier of information," one encounters many vague issues. Therefore, what is needed is a new way of thinking, a new theory, a new perspective in order to even begin to define the significance of the term information frontier in a scientific way.

My opinion is that the information frontier is a boundary without either form or rules which separates the "information territories" of individual states or political groups from one another. An "information territory" cannot be divided up according to traditional geopolitical concepts such as sovereign territory, airspace, territorial waters or even territories claimed in "outer space," but rather only according to an "information dissemination sphere" subject to certain political circumstances. The boundaries of the information territory and the security of the information frontier affect the prosperity of a people and a state in the Information Age. Individual states all over the world are presently in the process of annexing their information territory and defending this invisible border. Thus, a bitter struggle for domination of the territory of information is currently underway. The future strength of a nation's economy depends upon whether it can open up and exploit this territory and ensure the security of its borders.

The world is now in the process of transforming itself into a world of "network capitalism." In light of the liberalization of the market in the Internet, the protection of the information territory's borders is becoming a matter of national security.

From the Border of the Nation-State to the "Border of the Fifth Dimension"

Information territory is an unavoidable product of the Information Society; the "information frontier" is the result of changes in the form and development of war.

In addition to the four realms of war–land, air, sea and outer space–information warfare as a new form of war opens up a fifth dimension. However, since the war of the four dimensions is open to the war that comes from out of this fifth dimension, we are compelled to investigate the form of this new theater of war–to explore this new territory–and to look into the significance of the term "frontier."

The history of warfare has repeatedly shown that every time a new form of warfare has been developed, a new sphere of war has been brought into play, and the emergence of a new dimension of war has also led in every case to the establishment of a boundary of this new dimension. The dimension of war dictates the dimensionality of the territory of a state. The capability of a state to put up resistance in a dimension of war determines the level of security of the boundary corresponding to this dimension. Without this capability of putting up resistance in a particular dimension during a war, the result in actual fact is the loss of that particular boundary and even the loss of the corresponding defensive capability. Dominance in a high dimension determines multidimensional security, and the security of a high-dimensional territory is determinative with respect to the security of lower-dimensional or multidimensional territories.

Defensive Measures–Where and How?

Setting up a strong "mental line of defense"

All of us living in a computerized society–and this applies to individuals, states and political groups–are in danger of sinking in a sea of information. If we fail to master the art of "swimming," we risk drowning in that sea. It is not enough to gain access to that sphere in which information is obtained and to disseminate one's own information; rather, one must implement measures to enable the information thus acquired to be filtered and organized in order to be able to sort out and dispose of harmful or undesirable information, as well as to maintain the security of one's own information and to employ useful information with the greatest possible efficiency.

On the field of battle as well, information is becoming the most important weapon, and since an attack is ultimately aimed at knowledge and reliance, the enemy can be made to abandon resistance. The mental line of defense is the first to be affected; it is the primary target of an attack. For this reason, everyone–the state as well as each individual citizen–must erect his own invisible "mental line of defense." The task of the state is to develop laws and moral norms which regulate this territory of information, to promote the intellectual and spiritual culture of the nation by exerting a positive influence on public opinion, and to preserve and protect the political and cultural independence of the state. It is the responsibility of individual citizens, on the other hand, to absorb information selectively and to be on guard against harmful informational attacks.

Constructing an effective "Network Frontier"

Once a society's computer networks attain a high level of comprehensiveness, the weaknesses of those networks become apparent. Those nations that are on the leading edge of network technology and are fully committed to setting up such networks expand their information frontier at the expense of other nations and thus constitute a threat to the "informational sovereignty" of other countries. On the other hand, there are cases of "network sabotage"–such as hackers who gain illegal access to networks–which, in the worst case, can mean the destruction of various networks. "Net war" research is being conducted and simulations

carried out at present in a number of nations. Since the trend is for increasing quantities of information to be transmitted via networks, competitive conflicts will also be played out in the net some day, and conflicts in the area of national security will manifest themselves not only in the form of information warfare within the military field, but also in the form of a general conflict in the net that encompasses all spheres of society–politics, the economy, diplomacy, science and technology, culture, education and ideology. Conflicts in the realm of information and at the information frontier are thus certain to occur.

As an upshot of network-based deceptive maneuvers, future conflicts at the "network frontier" will manifest themselves in the form of disruptions, threats, and the total collapse of the enemy. Attempts will be made to use various means to penetrate the enemy's network and to "capture" information; conversely, efforts will also be undertaken to employ deception and other means to prevent the foe from penetrating one's own net. Intimidating information will also be disseminated via the net which is likewise designed to stop a hostile attack. The objective of all of these measures is to attack and destroy the enemy's network frontier and to make an attack on his part impossible.

States possessing highly developed information technology have already carried out successful efforts in this area. Politically, they have gotten away from placing exclusive emphasis upon the performance of computers and networks, and have turned their attention to questions of security, intactness, user-friendliness, precision and continuity. Many western countries have established unilateral or multilateral rules and norms designed to effectuate a long-term increase in the security of the net, and have invested enormous sums in the development of new technologies aimed at protecting the net–such as anti-virus technologies, technologies designed to prevent information from "leaking out," and other security technologies. Nevertheless, western experts warn of highly vulnerable points in these networks. Parallel to the development of computer networks, it would be highly advisable to consider the establishment of a "net frontier." On one hand, we ought to use these worldwide networks effectively and to their full extent, and correspondingly make positive information available in them. Moreover, we should set up our own information sphere and strengthen the influence of our own information. If, on the other hand, an effective "network border" is to be set up, then those backbone information networks which are directly involved in a state's political, economic, and military security must also be made subject to unified state regulation, be constructed in unitary fashion, and wherever possible be comprised to a certain extent of Local Area Networks. In this way, features that make the net easier to use can be prevented from causing its security to be diminished. Appropriate measures must also be taken with respect to other networks, such as the installation of firewalls, "protective barriers," or platforms that screen information in order to prohibit the dissemination of information that is damaging to the state and to defend against an attack aimed at the state. Furthermore, similar precautions must also be taken to protect other computer-equipped networks such as utility, telephone and television systems.

Deployment of a Force to Safeguard Information

When territorial waters came into existence, navies were formed; with the creation of airspace came the creation of air forces; and the formation of armed forces in outer space has even been considered, at least theoretically. If an information dimension and an information border are erected, then a corresponding force to protect information is also required–that is, a unit completely different from conventional forces, possessing intensive and specialized knowledge and technological capabilities, and which would thus be composed of specialists in information warfare including scientists, information experts and military personnel. Its main

objective is to ensure the security of the information border, to defend against attacks targeting the state's information sphere launched by other states, political groups, or individual persons, and to prevent criminal activities of this nature within the state itself. It thus puts up informational resistance against an invisible enemy in the sphere of information. This would also be the special commando unit to wage information warfare, the elite troops whose task is to repulse an information attack and to go into action in case of an information incident. Such an information defense force would be a clear symbol for the formation of an armed force appropriate to the Information Age. The more underdeveloped a state is vis-à-vis information technology, the more consideration it ought to give to the creation of an information defense force in order to ensure the protection of information and thus the entire security of the state.

Re-establishing our Supremacy

Setting up a digitized armed force and waging information warfare–all of this seems to us to be matters for the far-distant future, but the theoretical preparations are already well underway.

With armed forces currently undergoing a process of development by rapid leaps and bounds, it is not necessarily the land that has the technological lead which is actually the one in the position of superiority, but rather that land that is in the lead with respect to its thinking. This situation offers both an opportunity and a challenge; whoever succeeds in taking advantage of the opportunity can also meet the challenge.

If we wish to achieve supremacy, we must abandon the familiar conception that gives primary consideration to technology, followed by strategy, with theory at the bottom of the list. In order for theory to actually assume the position of a forerunner, it must be ahead of its time.

Victory in a future war depends upon the efforts we make today. In order to attain a position of preeminent power, we must acquire a new body of knowledge. "Knowledge is power"–in information warfare, this maxim takes on a whole new meaning.

Knowledge and information are our weapons. The difference between this immaterial weapon and conventional, material weapons is that it is easier to distribute, no one has a monopoly on it, and anyone can share in it. If it is available to others, then I can also quickly gain access to it, assimilate it, and apply it. Moreover, it is considerably more economical to bring knowledge to bear than it is to acquire modern weapons systems. And besides, the deployment of modern weapons systems is possible only if the personnel operating them possess adequate knowledge.

Conventional armed forces must break down the barriers that are inherent in the force of habit; they must abandon their traditional conceptions and acquire new knowledge, since only then will they be capable of meeting this new challenge. If this process of renewal does not take place, the process of adjustment to new facts and circumstances cannot occur. Since these changes initially take place in human beings themselves, the first task is to "transform" these human beings.

Information warfare is a product of the revolution in the military field, and it will certainly call into question old military theories, antiquated methods of waging war and archaic organizational structures. According to the historically-operational law of the "negation of the negation," information warfare will first of all negate the mechanized warfare which is

characteristic of Industrial Society. Conversely, it will, under certain circumstances, adopt various aspects of the art of warfare as practiced in Agrarian Society. We can surely proceed under the assumption that the "Art of Warfare" of Sunzi or the strategies of guerrilla warfare will thus be amalgamated with the technology of this new age to allow an undreamed-of potential to unfold. Our primary task is thus to unite these two approaches.

Theory is indispensable to technology, and theory cannot be considered in isolation from technology. An essential principle of information warfare is the "differential principle." If an information-supported unit and a unit without informational support face one another on a battlefield, the former will be superior as a general rule, in that the information-supported unit enjoys, under certain conditions, a better overall view of the entire theater of war. In order to effectuate a change in this situation, one cannot rely solely on strategic thinking or the deployment of stratagems. Those in command must possess technical understanding and initiate close cooperation with technical specialists in order to "technologize" their strategic thinking. Even in the area of technology, one side cannot be in sole possession of total supremacy; and even if this were the case, this is not a situation this is fixed once and for all. Both superiority and inferiority are relative concepts, and neither side can be totally superior or totally inferior. It is an illusion to believe that it is possible to avoid an opponent’s strengths and to attack only his weak points, just as it is an illusion to concentrate on one’s own strengths and to ignore one’s weaknesses.

History teaches us that, on one hand, technologies can have a positive effect on mankind; on the other hand, technology also has its dark side. The latest computer and information technologies enable society and the military to be ever more closely linked and integrated by networks, and to thus achieve an extremely high level of efficiency. Nevertheless, a society and an army that are network-linked to a high degree also have considerable weaknesses. For this reason, network linkage and digitization must be accompanied by the establishment of a new order. Information warfare breaks up the order of mechanized war and thus itself requires a new technological order. If a conflict were to break out, this would then be considerably easier to resolve. Our research efforts in the field of waging war and improving our technological position should begin with this point. We should not imitate others and, in the process, fail to take into account our own capabilities.

To attain supremacy and to employ it to its best advantage, we must pay particular attention to the development of a military "soft science." An information war is a "soft" attack, a gentle injury, and needs this "soft science" as a basis and also as a guarantee.

The military soft science concerns itself with military theory, strategy, planning and organization. Research in this field encompasses the entire range of weapons, and transcends the boundaries of individual departments and disciplines. Information warfare is not just a virus war, an electronic or psychological war, a war of deterrence or political propaganda. It comprises a much broader scope and cannot be compared with any forms of warfare that have existed until now. It therefore requires not only the conventional "hard" technologies, but also–to a much greater extent–a guarantee provided by "soft" technologies.