The Nature and Content of a New-Generation War

Col. S.G. CHEKINOV (Res.),
Doctor of Technical Sciences
Lt. Gen. S.A. BOGDANOV (Ret.),
Doctor of Military Sciences

Abstract. The authors make an analysis of print publications put out by the Russian Ministry of Defense and other sources devoted to the country's security today and offer an insight into the nature and content of a new-generation war.

Keywords: mobile joint forces, age of high-tech warfare, information superiority, information and psychological warfare, reconnaissance and subversive operations.

Many home-ground military experts writing in print publications put out this year by the Russian Defense Ministry and elsewhere in the national press offer their own visions of how this country can be made secure militarily, the kind of future warfare they call a new-generation war, and, perhaps the most puzzling issue, what the Russian Armed Forces' makeup must be. Many of them insist that a future war will in no way look like wars of the past century, and even wars fought only recently. Some of them are justified in their views that the Russian Armed Forces' weapons system does not fit completely the role it will have to play in future wars and that, for this reason, it must be restructured and its make-up reworked.

Quite a standout among them all is an article by the Chief of the Russian Armed Forces' General Staff who writes that "... the 'rules of war' themselves have changed significantly. Nonmilitary options have come to play a greater role in achieving political and strategic goals and, in some situations, are greatly superior to the power of weapons. The role of mobile joint forces operating in an integrated reconnaissance and information environment is rising through the use of new opportunities now available to control and logistic systems. New information technologies have reduced appreciably the distance - physical, temporal, and informational - between the troops and their superiors. Remote engagement
of the enemy ‘at arm’s length’ is turning into the principal tactic to achieve the goals of a combat action or an operation. Adversary targets are now attacked at any point of enemy territory. Differences between strategic, operational, and tactical actions, and between offense and defense are leveling off. High-precision weapons are used on a growing scale. Weapons based on new physical principles and robot-controlled systems are going into service in large quantities."

Fitting well into this context is an article by Army General M.A. Gareyev, President of the Academy of Military Sciences, who writes: “Nations have always struggled with one another with the use of armed forces and warfare capabilities, including intelligence and counterintelligence, deception and stratagems, disinformation, and all other refined and devious stratagems the adversaries could think up. It has always been held that any confrontation without resort to arms is struggle and pursuit of policies by physical force and armed violence is war. Some of our … philosophers, though, maintain that all nonmilitary practices are a contemporary development and suggest, on this assumption, that following these practices is nothing short of war.”

Yu. Ye. Gorbachov’s article titled “Cyberwar Is Already On” merits special mention here. The author believes that rapid development of information technologies in the late 20th and early 21st centuries, and widespread use of information in society and the leading countries’ armed forces have changed significantly the nature, methods, and techniques used by state and government political and economic agencies, affected social relationships and the nature, methods, and techniques of military operations, and created new information threats and challenges.

With reference to publications by military experts in the Military Thought journal, Yu. Ye. Gorbachov argues that the latest information technologies, modern weapons and equipment, and the potentialities of intelligence and electronic warfare technologies, automated control systems, and communications facilities have had a strong effect on troops employment options and conduct of military operations in our day. The new content and character of armed warfare derive today from the network-centric environment in which military operations are controlled – information and electronically guided fire operations (transformed EW and computer network operations) are conducted along with aerospace operations, and air force operations that follow a systemic pattern. No goal will be achieved in future wars unless one belligerent gains information superiority over the other.

Another of Yu. Ye. Gorbachov’s statements that has not escaped our attention is that the growing significance of struggle for information superiority makes employment of joint forces specific in many ways. Formerly fought in a three-dimensional environment, armed struggle has expanded from the ground, sea, and aerospace into an entirely new environment – information. The outcome of a war and, accordingly, the decisive role of any one of these environments will depend on the developments in the battlespace and the belligerents’ actions.

In the mid-1990s, Russian military experts displayed enormous interest in several points argued by V.I. Slipchenko in his famous book on sixth-generation
The main objective of sixth-generation wars, the researcher writes, is to “destroy the enemy’s economic potential...,” and “keeping the man outside of the battlespace is what makes future wars and armed struggle cardinally different.”

An analysis of publications by Russian military experts writing on national security and the character and content of new-generation warfare, and the experience of military conflicts of the last few decades, including those associated with the Arab Spring revolutions in North Africa and the Middle East, offer enough evidence that the early 21st century is really the beginning of a new “military age” for humanity – an age of high-tech wars.

This view is shared by Vice Premier Dmitry Rogozin who writes that “…so big a country is difficult to defend with what it has now if traditional approaches are taken to developing weapons and military and specialized equipment. New approaches have to be applied – robotics, automated weapon control systems, effective intelligence and communication systems, and much else besides.”

We know from the history of wars and military art that new weapons and specialized and general-purpose military equipment have always had a significant impact on the content of armed struggle in wars and military conflicts and, in the first place, on the need to address new operational tasks. Attainment of operational objectives in new-generation warfare will be influenced significantly by efficient new military technologies and weapons based on new physical principles. New weapons that are expected to be developed will have a greater killing power, range, accuracy, and speed, and intelligence, reconnaissance, control, communications, and information warfare will have greater potentialities. Deployed to the battlespace, they will alter radically the character and content of armed struggle in new-generation wars.

Intensive fire strikes against seats of national and military power, and also military and industrial objectives by all arms of the service, and employment of military space-based system, electronic warfare forces and weapons, electromagnetic, information, infrasound, and psychotronic effects, corrosive chemical and biological formulations in new-generation wars will erode, to the greatest extent possible, the capabilities of the adversary’s troops and civilian population to resist. It is also expected that untraditional forms of armed struggle will be used to cause earthquakes, typhoons, and heavy rainfall lasting for a time long enough to damage the economy and aggravate the sociopsychological climate in the warring countries.

These effects will certainly modify the character of tactical, operational, and strategic actions and give rise to new, and alter the content of existing, operations on every scale. New forms and methods of employing joint forces in operations and engagements will evolve.

New forms and methods of combat were first used by the U.S. armed forces in the early 1990s during the war against Iraq when they gave practical content to the “global scale, global power” concept. Years later, in 2003, military actions in Operation Iraqi Freedom were conducted in the spirit of the Joint Vision 2020.
The Gulf War may be called the first war of a new age – the age of high technologies. In a sense, it was a turning point giving a kind of vision of the future. An invisible line was, in fact, drawn under the traditional wars of the past, with their orderliness, armies millions strong, and continuous positional frontlines, with one belligerent’s immense numerical superiority over the other playing the decisive role.

In the Gulf War that broke out in the early 1990s, the Iraqi army employed its outdated inflexible positional standoff strategy that was no match for the new forms and methods of warfare used by the U.S. and its allies. This strategy eventually contributed to the Iraqis’ disastrous defeat. The Gulf War was a practical demonstration of the truth that **technological superiority in weapons could cancel the enemy’s numerical advantage** in weapons long come of age. It was the first time in the history of wars that formidable ground forces half a million strong did not put up a fight in an effort to win. They were only fully deployed in the last days of the war when the Iraqi army was as good as finished by air and missile strikes that went on for weeks.

In their war against Iraq, the Americans used an “electronic knockdown” before the first shot was fired. It proved to be a very effective strategic move to begin the war – an utterly untypical way to engage the enemy in the preceding decades. The Gulf War started with a massive attack by some of the latest EW weapons that went on around the clock. The electronic operation was launched in parallel with an aerial offensive by the air force and sea-based cruise missiles, reinforced with reconnaissance strike aircraft, artillery barrages, and remote-controlled aerial vehicles. The electronic and aerial offensive left the Iraqi forces no chance to retaliate and knocked out the Iraqi air force and air defense control system.

**The first war of the new high-tech age was different from any war that preceded it in many critical respects:** there were no clear dividing lines between the opponents’ forces; the warring sides’ flanks were exposed; their operational orders of battle had large undefended gaps, their combat elements separated by a considerable distance from one another; the attacker had an overwhelming superiority achieved by high-tech weapons; long-range high-precision weapons were used on a mass scale, particularly at a time when the Coalition forces were taking the strategic initiative and winning absolute superiority in the air; the Coalition forces were striking regularly and selectively at the enemy forces’ key targets, vital economic facilities of military significance, and civilian and military control centers, and destroying life support systems anywhere on enemy territory to force the defender to lay down the arms.

Another distinction of the campaign against Iraq was that reconnaissance, fire, electronic, and information warfare forces of different branches and arms of the service were integrated the first time ever into a shared spatially distributed reconnaissance and strike system making wide use of modern information technologies and automated troops and weapons control systems.
The potentialities of orbiting satellites were used on a wide scale in the Gulf War, the first time as well, at the strategic, operational, and even tactical (division, brigade, and battalion) levels. Orbiting satellites played a special role in the war. They were frequently the only source providing online intelligence at any time of day and night, in any weather, whatever the geographic position of targets.

Field manuals of ground forces in most all foreign countries (NATO countries, in particular) make a strong point that their armed forces must be ready today to unleash the full potential of their combat power – nuclear and conventional arms, weapons and specialized equipment, and electronic warfare capabilities. In fact, they put EW capabilities next to nuclear and conventional arms, that are transformed, in a network-centric troops control environment, from a combat support activity into an important type of combat operations.

By drawing on an analysis of armed conflicts and local wars fought in the past few decades, with reference to the views acknowledged military experts have on future warfare, these authors venture their own viewpoint on the character and content of a new-generation war. As we see it, introduction of the latest information technologies to develop effective modern weapons, reconnaissance, EW, and communication capabilities, and automated control systems has altered significantly the patterns of manpower employment and conduct of military operations, and is going to have a decisive impact on the development of new patterns. This is a natural process from the historical viewpoint. Back in the 1920s, A.M. Zayonchkovsky, a professor at the M.V. Frunze Military Academy and a Russian military theorist, wrote that the forms and methods of armed struggle tend to change from time to time. It is very important to find the causes and identify the principal trends in changes because they will give a insight into the way in which armed struggle will be fought in the future.  

A new-generation war will be dominated by information and psychological warfare that will seek to achieve superiority in troops and weapons control and depress the opponent’s armed forces personnel and population morally and psychologically. In the ongoing revolution in information technologies, information and psychological warfare will largely lay the groundwork for victory.

Asymmetric actions, too, will be used extensively to level off the enemy’s superiority in armed struggle by a combination of political, economic, information, technological, and ecological campaigns in the form of indirect actions and nonmilitary measures. In its new technological format, the indirect action strategy will draw on, above all, a great variety of forms and methods of nonmilitary techniques and nonmilitary measures, including information warfare to neutralize adversary actions without resorting to weapons (through indirect actions), by exercising information superiority, in the first place.

Interstate differences preceding new-generation warfare will be resolved by relying on a combination of political, economic, scientific, engineering, religious, cultural, information, and humanitarian capabilities of a country to integrate it into a peaceful environment, develop its diversified relationships that
promote trust and cooperation, scale down military confrontation, and put up barriers to power politics. These nonmilitary actions will help lessen and remove military hazards and threats by the opponents entering into peace treaties and taking other amicable steps. Nonmilitary measures serve to reduce the possibility for the aggressor to engage in hostile activities against other countries, give it an unflattering image in public opinion, make sensational denunciations of its aggressive plans, and so on.

Beyond a shadow of a doubt, the aggressive side will be first to use nonmilitary actions and measures as it plans to attack its victim in a new-generation war. With powerful information technologies at its disposal, the aggressor will make an effort to involve all public institutions in the country it intends to attack, primarily the mass media and religious organizations, cultural institutions, nongovernmental organizations, public movements financed from abroad, and scholars engaged in research on foreign grants. All these institutions and individuals may be involved in a distributed attack and strike damaging point blows at the country’s social system with the purported aims of promoting democracy and respect for human rights.

In their propaganda efforts, these organizations can obtain information to engage in propaganda from servers of the Facebook and Twitter public networks watched over by the American special services. The propaganda program is controlled from a center at the U.S. Air Force Base in MacDill, Florida, that employs 50 operators, each controlling up to ten “influence agents” registered in different countries and conducting information warfare in the spirit of traditional state erosion technologies. In the estimates of British experts, this program is run at a cost of $2.76 million, giving a credible legend and safeguards against disclosure to each of these information warriors. What is more, these public networks are banned from reaching out to U.S. audiences, for which purpose they are not permitted to use English. They can only use Arabic, Urdu, Pashto, Farsi, and several other languages spoken in target countries.

Advanced countries already use the new strategy for preparing and conducting new-generation warfare that differs significantly from war strategies of the 20th century. The changes that have since occurred in all things military have compelled the U.S. armed forces to develop a new concept – the Network-Centric Warfare, or NCW. In substance, the NCW concept is not a system of views on the conduct of a modern-day war (armed conflicts) as such; rather, it is a concept of control over combat operations as a new way of directing armed forces in 21st century operations.

The network-centric warfare concept arose immediately in the wake of rapid advancements of information technologies and development of high-precision weapons and weapons based on new physical principles. Armed with the NCW concept, American planners want to use information attack at the outset of a new-generation war to disable all elements of the adversary air defense system – control posts, communication centers, radar stations, antiaircraft missile batteries,
and the air defense aircraft control system. In their estimates, a loss of up to 50% of control system capabilities would have an adverse effect on the enemy’s strategy and force him to discontinue resistance – the end goal of the NCW concept.

In a network-centric warfare environment developing on the guidelines of the NCW concept, U.S. forces’ operations at any level (tactical, operational, and strategic) will be directed regardless of where the forces are deployed across the world, whatever combat missions they fulfill, whatever strength they have, and however they are structured. Actually, a “network-centric environment” comprises information and communication elements bringing the armed warfare forces and weapons into one system.

It may be assumed, with a large measure of probability, that defeating the enemy’s main forces and destroying the economic potential of the country attacked, and also overrunning its territory are the principal objectives of a new-generation war fought in a network-centric environment. The full range of military, economic, political, diplomatic, and IT measures, blended with effective psychological information activities, may be used to achieve these objectives.

The new environment in which international armed conflicts will be resolved in the future suggests that the attacker will make plans for a new-generation war (international armed conflict) in advance and take wide-ranging measures to conceal his preparations for an attack, the D-day, and the nature of impending operations. Misleading the opposing country’s political and military leaders about the attacker’s intentions is an effective way of achieving his objectives. He can do this by launching a disinformation effort to conceal the commencement date and scale of operations he is about to go ahead with.

Strategic operations can only achieve their goals in new-generation wars if the attacker wins information superiority over his opponent. Information superiority was a major contributing factor in the operations the U.S. and its allies undertook in the Persian Gulf area in 1991, against former Yugoslavia in 1999, Afghanistan in 2001, and Iraq in 2003.

A special operation to misinform and mislead the enemy’s political and military leaders in a new-generation war may include large-scale carefully coordinated measures carried out through diplomatic channels by government-controlled and private media and top government and military agencies by leaking false data, orders, directives, and instructions. High-ranking political and military officers will make public statements for greater effect of the disinformation effort.

In the run-up to his special operation, the attacker will presumably make wide use of nonmilitary (indirect) moves and techniques, including targeted cyber-attacks against the communications systems of the enemy’s control bodies at all levels. Decisive battles in new-generation wars will rage in the information environment, in which the attacker’s computer operator manipulating the “intelligent machines” at a distance will be the key figure in the battlespace.

Encrypted data flowing in public communication channels will be among the coveted targets for cyber-attacks. A quantum computer may turn into a tool of
The Nature and Content of a New-Generation War

destruction and a 21st century bomb for cyber-attacks to succeed. It will easily crack all codes and gain free, and virtually instant, access to all networks supporting the operation and security of government and military control agencies.\textsuperscript{12}

The new time frame of new-generation blitz wars will be created by information technologies operating within the nanosecond range. Speed, synchronization, and concurrency will decide success or failure of operations. Computers, telecommunications, and satellite communications will permit troops and fire strikes to be controlled in real time.

Months before the start of a new-generation war, large-scale measures in all types of warfare – information, moral, psychological, ideological, diplomatic, economic, and so on – may be designed and followed under a joint plan to create a favorable military, political, and economic setting for the operations of the allies’ armed forces.

Powerful information pressure (in the form of an information operation) will be applied, in accordance with the joint plan, through all media on the population of the country to be attacked militarily and on the public in the rest of the world. As the information operation gets under way, the world public will be induced to accept the need to fight tyranny and restore democracy in the country to be attacked soon. Actually, however, the principal aim of the invasion is for the aggressor states to resolve their political, military, and economic problems.

Acting on their detailed and fully funded information operation plan, the aggressor states will impose rigid censorship and constraints on all media. As a result of these measures, information the attacker’s political and military leaders find acceptable and necessary will be dispensed to the population of the country to be attacked by the aggressors and to the world public.

Heavy propaganda is designed to spark discontent among the defender’s population and armed forces personnel at the current government agencies’ activities. The propagandists expect to depress the moral and psychological feelings of the civilian population and armed forces personnel to a level where they give up resistance and the civil administration and military control systems are unbalanced. The onset of chaos, loss of control, and demoralization among the population and the defending army’s personnel must give the aggressor and his allies an opportunity to fulfill their political, military, and economic objectives in the campaign within a short space of time without significant loss of life.

Depending on the obtaining situation, the aggressor may use nonlethal new-generation genetically engineered biological weapons affecting human psyche, moods, and will to intensify the effect of mass-scale propaganda to drag the target country deeper into chaos and further out of control.

At around the same time, the attacker will most probably attempt to intimidate, deceive, and bribe government and military officers, to blackmail them and induce top commanding officers of the target country’s armed forces to abandon fulfillment of their service duties and, in this way, to manipulate their behavior. Much will be made of the discontent of the aggrieved population segments.
Undercover agents will be planted to encourage the discontent to commit unlawful acts, and to stoke up chaos, panic, and disobedience. The agents will be supplied with considerable funds, weapons, and materials to go on with their subversive activities. If the country flying out of control has Islamist radicals among its population, destabilizing propaganda will be directed at them in the first place. Arrival of international bands of militants is to be expected to make the situation in the country still worse and to step up subversion.

Before the outbreak of war, nonmilitary measures, such as establishment of no-fly zones over the country to be attacked, imposition of blockades, and extensive use of private military companies in close cooperation with armed opposition units, may be applied as new methods of interstate warfare.

**The start of the military phase will be immediately preceded by large-scale reconnaissance and subversive missions** conducted under the cover of the information operation. All types, forms, methods, and forces, including special operations forces, space, radio, radio engineering, electronic, diplomatic, and secret service intelligence, and industrial espionage will be used to detect and map the exact location of key government and military objectives vital to the country’s sustainability, designate targets for fire strikes, make digital topographic maps of enemy territory and load them remotely into onboard homing systems, and monitor the efficacy of fire strikes.

Hours before the start of war (launch of high-precision missiles from the ground, sea, air, and space), the attacker may schedule a mass attack by the latest EW technologies to administer an “electronic knockdown” (electronic operation) that may go on for up to two full days, depending on the way in which the operational-tactical situation develops. The electronic offensive will blend with an aerial offensive, massive launching of high-precision missiles from all platforms, reconnaissance and strike missions, remotely controlled aerial vehicles, and robot-controlled weapons.

**Most probably, the attack will begin with an aerospace operation several days long.** On day one, the attacker will attempt to direct his air strikes and high-precision missiles launched from the ground, sea, air, and space in a network-centric environment to destroy or heavily damage the opponent’s key military and industrial capabilities, destroy enemy government and military control centers, his political and military leaders, and communications centers, knock out power and water supplies, and ultimately force the target country to sue for peace. The aggressor will take every possible measure to prevent retaliation by the defender and avail himself of the early hours of aggression to disorganize the defender’s air force and air defense system.

This possibility will require the defender to plan in advance and enforce continuously all appropriate measures to repel enemy aerospace strikes on the scale of the country’s common aerospace defense system and to protect effectively every single military and economic facility.

**While the aerospace operation is on, the defender must anticipate attack by enemy military robots.** Walking, crawling, leaping, and flying robots and robot-
controlled systems capable of engaging in combat activities independently will be used along with unpiloted aerial vehicles in the ongoing military operations.\(^{13}\)

Robots will be used in a new-generation war to conduct reconnaissance and collect data, coordinate combat operations of different arms of the service and units, repair weapons and equipment, build defenses, destroy enemy hardware, clear mines, and deactivate and degas contaminated areas. Groups of robots will be used in hazardous areas in place of ground troops, naval forces (in deep sea and on the sea surface), and conduct military operations on their own.

It is very probable that an attacker will achieve his political and military goals in a new-generation war before he deploys his ground forces. The aggressor will, most likely, send them into enemy territory only after he has assured himself that his missile and air strikes, long-range artillery fire, and weapons based on new physical principles have wiped out a majority of the defending units, destroyed government and military control centers, key military, industrial, and economic targets, and wrecked the stability of the defending country's government administration system. Ground troops will be used in special operations to mop up the enemy's surviving centers of resistance and fighting units.

Still, the end goals of a new-generation war cannot be attained unless ground forces are committed. To have them fulfill this purpose, ground forces must be continually improved and equipped with the latest weapons, particularly high-precision weapons and EW capabilities.

It is our strong belief that a new-generation war will be fought by the rules and customs of the side that is best prepared to put the recent breakthroughs in warfare economics and technologies to a practical test. Accordingly, economically advanced countries are seeking to prevent a potential adversary from achieving superiority in warfare technologies over themselves. They achieve this goal by continuously improving their military technologies, creating efficient economies, developing and consistently fulfilling their programs for improving the design of their weapons and hardware on the basis of the last word in technologies and producing them in quantity. Little surprise, then, that a growing number of Russian military theorists name *overwhelming superiority of either of the warring sides in military technologies* a hallmark of new-generation wars.

We have researched some of the recent armed conflicts and have reasons to suggest that a new-generation war will fall into an opening and a closing periods. The *opening period* will be the pivotal and critical time of the war, and will break down into a targeted information operation; an electronic warfare operation; an aerospace operation; continuous air force harassment; the use of high-precision weapons launched from various platforms; long-range artillery, and weapons based on new physical principles to strike at enemy targets in all areas, practically the full length and width of enemy territory.

The aggressor will use this time to destroy critical government and military control centers, key military-industrial complex facilities, knock out the country and armed forces management system, and to prevent orderly deployment of the
defender’s forces to the theaters of operations in an effort to ward off aggression. The defending country’s political and economic system made ungovernable, its population demoralized, and its key military-industrial complex facilities destroyed or damaged beyond repair, the victim of aggression will not be able to switch its economy over to meet the country’s war needs and beat off the aggressor. As a result, the attacker will achieve the military and political aims of its campaign within the shortest possible time frame.

In the closing period of the war, the attacker will roll over the remaining points of resistance and destroy surviving enemy units by special operations conducted by reconnaissance units to spot what enemy units have survived and transmit their coordinates to the attacker’s missile and artillery units; fire barrages to annihilate the defender’s resisting army units by effective advanced weapons; airdrop operations to surround points of resistance; and territory mopping-up operations by ground troops.

Realities of our day dictate an urgent need to prepare Russia for possible new-generation wars without further delay. It is a first priority for this country because its defense and economic potential has waned significantly over the past two or three decades.

Every effort must be made to repair deteriorating relations between states before a new-generation war breaks out, preferably beginning with nonmilitary options, such as a combination of political, economic, scientific, engineering, information, diplomatic, and humanitarian opportunities of a country to be integrated into the world community and versatile relations to be developed with it by confidence-building measures and expansion of its cooperation with other countries, to ease military confrontation, and to put up barriers to power politics. These nonmilitary options will lessen, and ultimately remove, military hazards and threats by peace treaties and other initiatives, reduce the aggressor’s choices in his hostility to other countries, give him an unfavorable image, and expose his aggressive plans.

Where nonmilitary efforts produce little effect, a country must be ready to use every kind of power containment to persuade the potential aggressor that the costs of his attack will be higher than the expected results. The enemy may be swayed in his resolve by demonstration of the readiness (in response to a threat of attack) of a Russian defensive force to be deployed to the area of anticipated aggression; a strongly worded statement with a warning of immediate nuclear retaliation against the threat arising to the country’s sovereignty and integrity during the war and of unrestrained use of high-precision weapons to destroy the enemy’s nuclear power plants, chemical industry plants, and major hydropower projects on the potential aggressor’s territory; and preparation and conduct of an information operation expressly to mislead the enemy about Russia’s readiness to fight off aggression.

We are almost certain that as a new world order is put in place, armed force will, in the short term, continue to play a major role in the efforts economically
advanced countries and their allies will be making to achieve their political objectives. To avoid making the same historical mistake yet another time, the Russian Armed Forces must be ready to fight new-generation wars in the medium and long terms and to use indirect, arm’s length forms of operations.14

Information superiority and anticipatory operations will be the main ingredients of success in new-generation wars. The intensity of military operations will peak from the start, with the attacker entertaining the hope of striking a first surprise and most powerful and crippling blow. A country preaching a defensive doctrine may get the short end of the deal in the face of a surprise attack by an aggressor.

NOTES:
10. Military Thought, # 1, 2011, pp. 100-111.