Military and Strategic Affairs

Volume 4 | No. 2 | September 2012

INSS
המכון למחקרי ביטחון לאומי
THE INSTITUTE FOR NATIONAL SECURITY STUDIES
INCORPORATING THE JAFFEE CENTER FOR STRATEGIC STUDIES
TEL AVIV UNIVERSITY
אוניברסיטת תל-אביב

Military and Strategic Affairs

Volume 4 | No. 2 | **September 2012**

CONTENTS

Military and
Strategic Affairs

The purpose of *Military and Strategic Affairs* is to stimulate and enrich the public debate on military issues relating to Israel's national security.

Military and Strategic Affairs is published three times a year within the framework of the Military and Strategic Affairs Program at the Institute for National Security Studies. Articles are written by INSS researchers and guest contributors. The views presented here are those of the authors alone.

The Institute for National Security Studies is a public benefit company.

Editor in Chief
Amos Yadlin

Editor
Gabi Siboni

Graphic Design: Michal Semo-Kovetz, Yael Bieber
Tel Aviv University Graphic Design Studio

The Institute for National Security Studies (INSS)
40 Haim Levanon • POB 39950 • Tel Aviv 61398 • Israel
Tel: +972-3-640-0400 • Fax: +972-3-744-7590 • E-mail: info@inss.org.il

Military and Strategic Affairs is published in English and Hebrew.
The full text is available on the Institute's website: www.inss.org.il

Dilemmas of Warfare in Densely Populated Civilian Areas

Moshe Tamir

This essay attempts to present operational perspectives on conducting warfare in densely populated areas. It also distinguishes between three types of combat within this general category, with the goal of shedding light on this complex type of warfare.

The first type relates to standoff warfare, a situation in which the enemy is located in one sphere and one's own forces are in another. In this case, one's forces do not control the enemy's sphere but direct massive firepower towards it. Examples of such situations are IDF activity in Lebanon over many years and current activity in the Gaza Strip. In situations of this sort it is imperative to take into account not only the capabilities and means of one's own forces, but also the civilian population residing in the area of conflict.

The second type of warfare in densely populated areas relates to warfare in urban areas. In such situations, the attacking force must maneuver, i.e., take control of urban areas containing not only enemy forces but also civilian populations. The most prominent example of such warfare in recent years is Operation Defensive Shield. Operation Cast Lead and the Second Lebanon War are other examples of situations in which IDF forces had to take control of densely populated urban areas. This type of situation is marked by intense friction in civilian surroundings. The IDF is experienced in both standoff fighting and urban combat, but operating with civilians is qualitatively different.

Brig. Gen. (ret.) Moshe ("Chico") Tamir was the commanding officer of the Gaza Division. This essay is based on a lecture delivered at the December 2011 conference "Challenges of Warfare in Densely Populated Areas," sponsored by INSS and the International Committee of the Red Cross.

The third type reflects a specific complex situation, where although one's forces have taken control of the area, they are forced to battle returning enemy cells. An example of this situation is Judea and Samaria since Operation Defensive Shield. The United States faces a similar situation in Afghanistan and Iraq, albeit both geographically and militarily more difficult than the situation that confronts Israel. Despite the Americans' range of capabilities and means, they have not managed to decrease the amount of hostile activity. In this type of situation, legally and morally the army becomes almost completely responsible for the civilians in the area, even if military rule has not been declared. In other words, the army needs completely different abilities and skills.

What follows are some examples of the various situations. In the context of the conquest of Tul Karm during Operation Defensive Shield, the IDF conducted a series of intensive actions within densely populated urban areas, operating massive force at the brigade and division levels. The possibility of the IDF operating effectively against terrorism within the population was limited because terrorist cells were almost completely integrated within the area. Any movement of the population was used to camouflage the movement of terrorist cells. Three or four attempts to overcome terrorism in Tul Karm failed because movement by tanks and armored personnel carriers very noisy. When the noise was heard, the terrorist cells would scatter to the suburbs and villages at the city's outskirts, and when IDF forces would reach key locations in the city, only old people and innocent civilians would be left. Once the forces were withdrawn, the terrorists would return to the city and a week later would again attack cities in the heart of Israel. The enemy was well organized in orderly terrorist cells that would sit back while the IDF was in control of the area and attack at a later time.

The IDF studied the failed attempts, drew the necessary conclusions, and then operated in a simple, effective manner. Some sort of relatively small distracting action would be carried out within the city, sending the terrorists fleeing into the refugee camps on Tul Karm's outskirts. At the same time, large IDF forces would surround the refugee camps. This created a situation in which the fight was contained in a very small area. The idea was to press the enemy into surrender, and it proved successful. Using this pattern, some 500 terrorists were surrounded and forced to surrender. The operational achievement was striking.

The experience in the Jenin refugee camp differed. The complexity of the situation and the conditions on the ground required the IDF to enter the camp again and again in order to clear it of hostile activity. Every IDF entry was meant to deal with only a certain part of the camp, so the terrorist cells would simply move and operate from a different location, not unlike the movement of a liquid inside a closed system: pressure on one side causes the liquid to move far from the pressure point. Only effective pressure on several points at once forces the liquid to the center. In such an operation of occupying an area the most important aspect is to fortify and protect the attacking force. In addition, the IDF applied the tactic of leveling the ground and using non-precision fire to cover the attacking forces.

At the time of all these actions, the houses were full of civilians. As such, the attacking force faced complex challenges, in its drive to minimize harm to the civilian population. Early assessments were that the number of non-combatant casualties would be high, but the results were less devastating and relatively few civilians were harmed. However, such data and assessments are of no importance to the commanding officer in place who has to decide whether or not to launch an attack in the heart of a civilian population and risk causing non-combatant casualties. The rule of thumb in fighting in densely populated civilian areas is a ratio of one civilian casualty to two terrorist casualties. The ratio rises significantly when the choice of tactic is use of ground troops. The moment ground troops go in, the complexity is even greater and the ratio between civilian and terrorist casualties is commensurately higher. The success of the mission of taking such an area depends on the attacking force's determination, i.e., clearing the area effectively, patiently, and consistently. The occupation of an area in the heart of the civilian population is an important achievement in this type of asymmetrical fighting.

As Operation Defensive Shield ended and areas were brought under control, the regular brigades were charged with identifying and destroying the terrorist infrastructures. The Golani Brigade was put in charge of the Jenin sector, a particularly active and complex area that sent many operatives to carry out acts of terrorism in the heart of Israel. Unlike other sectors, not only the city center but also the more rural area around the city served as a terrorism operations base. In addition, it appeared that the terrorist organizations prepared themselves for an IDF occupation and were ready well in advance. The Golani Brigade was supposed to carry out

two missions: one, to secure the area and prevent terrorists from leaving, and two, to destroy terrorist infrastructures. The second was successfully accomplished; in five and a half months of activity, the brigade managed to shatter the infrastructures almost completely. But the first and more complex mission was not fully achieved, and during this period the terrorist organizations still managed to send several terrorists into Israeli territory.

Another factor is the presence of Israeli settlements within the sector, a factor complicating the fighting even more. Many tend to compare this type of IDF activity to that of the American army. In Baghdad there was an area called the Green Zone. Civilians, including American contractors and foreign citizens working for international organizations, resided in this area. Defensive procedures were very rigid there in terms of procedures for opening fire on the one hand, and in terms of defending against an incursion on the other. The situation in Israel is different: in many cases, there is no distinction between civilian and military areas, e.g., a military force stationed in the city of Sderot takes heavy fire from the Gaza Strip. This fire does not distinguish between the military force and the residents' homes, schools, and the children attending them. I believe, therefore, that we must change the rules and the international laws of war. The international law for a regular army opening fire does not distinguish between defending military forces and defending civilians. From the perspective of international law, it is impossible to punish people who fire at civilians with disproportionate and inaccurate standoff fire. Every such action intended to defend the civilians under attack is prohibited. This approach creates an absurd situation when the enemy is a terrorist organization with the a priori intention of killing civilians. The tactic of Hamas, as predicted by the IDF, was opening fire at precisely 7:45 AM, when Israeli schoolchildren waited for their school buses. This situation is not similar to fire aimed at American soldiers stationed on bases in Iraq or even at civilian contractors who operate there to serve these soldiers.

At the start of the action in Jenin, the area was saturated with terrorist cells. High ranking terrorists wanted by Israel, trying to impersonate innocent civilians, were caught almost daily at one of the roadblocks in the sector. Terrorist cells were caught almost at random. But this pressure made the cells split into tougher, smaller, and more independent units, making it harder for the IDF to identify and apprehend them. Therefore, the IDF boosted its efforts, placing more roadblocks and leveling more extended

curfews. In such complex situations and lacking intelligence, there was no choice but to operate in ways that also harm civilians. These steps blocked traffic to schools, and made it hard for civilians to acquire basic foodstuffs and receive medical attention. Consequently, serious friction with the local population developed, and indeed, the damage to freedom of movement and the routine life of the civilians led to a boomerang effect: the civilian population supported the terrorist organizations even more strongly than before and opposition to the IDF grew. At the same time, the Jenin sector dispatched terrorists who carried out two attacks in which 32 Israelis were killed. A situation in which a military force is charged with preventing the dispatch of terrorists while operating within the civilian population is very complex. This asymmetry, with Israelis hostage to the terrorist organizations, complicates military operations.

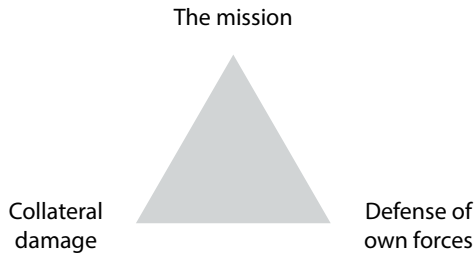
It was only long after Operation Defensive Shield ended that the correct conclusions were drawn about the most effective modus operandi for complex situations involving warfare in densely populated areas:

a. Gathering as much intelligence as possible.
b. Using infantry rather than armored personnel.
c. On the one hand, making life as easy as possible for the civilians, while on the other hand, fighting in a focused, uncompromising way against terrorist cells.

As for standoff fighting: The history of Israeli warfare on terrorism includes many commanding officers who felt this was the most effective way to fight within civilian populations. At present, the common understanding is that this is not the right method. Whatever the intensity of the fire applied, it will never be enough to render it unnecessary for the attacking force to use its infantry in the area and cleanse it. In addition, it is necessary to take the price the civilian population has to pay into account when operating heavy fire. Expelling the civilians is a tool not only to defend the population but also a means to motivate it to influence the regime. The methods of standoff fighting have failed over and over again. In asymmetrical warfare in densely populated areas there are no shortcuts.

Many speak of the tactic of deterrence in confrontations with terrorist organizations. However, one ought perhaps to relate to the situation as an equation with two players rather than as deterrence of the other side. In order to deter terrorist organizations from firing, the IDF first fought them in pinpoint fashion and created the rules for the fighting. When one of the

organizations would violate a rule, the IDF would take control over a civilian area and put the enemy's civilians into the same equation. However, this was at best a mixed blessing: taking control or any other extreme action would lead to terrorist organizations firing on Israeli citizens. As a result, Israelis became hostages of the situation. The IDF found itself caught in an impossible bind: on the one hand, an attempt to fight what proved to be an insufficiently effective tactical battle without full use of its military capabilities, and on the other hand, an attempt to minimize damage to the civilians on both sides. The only advantage of this situation is minimizing the harm to IDF soldiers because the activity is of relatively small scope. Nonetheless, the ineffectiveness made it hard to achieve the mission as a whole because it extended the duration of the fighting and therefore also added to the attrition of the force. It is therefore necessary to know when to change the rules of the game. One can clarify the complexity of the situation by means of the following figure:



Completing the mission, defending the force, and minimizing damage to the civilian population are the three points of the triangle. Concentrating effort on one point comes at the expense of the other two. All along, one must remember that the IDF is charged with one clear task: defending the citizens of Israel. When a decision is made to embark on an operation in order to fulfill this task, it stems from the fact that life for Israelis in a particular area has become unbearable and that one cannot allow the situation to continue without taking some action.

However, the task of defending the citizens of the state implies damage to the enemy's civilian population. Any fire of any intensity immediately affects the civilians on the other side; the extent of the effect on the civilians is determined by the intensity of the fire. The bombing of an entire neighborhood in the Gaza Strip in response to a mortar bomb fired

at Sderot creates a different effect than that created by using precision weapons with limited collateral damage. To be sure, such weapons are not always available and cannot always be used, but in general the key is to use weapons with the least potential for damage in densely populated areas and minimize the effect on the civilians.

Another component is defending one's troops, which prompts a very serious dilemma: to what level of risk can one's forces be exposed in order to minimize damage to enemy civilians? No military force in general, and the IDF in particular, is interested in targeting civilians or ignores the ramifications of firing on civilians. Nonetheless, foregoing support fire as described above in the case in Jenin will lead to fire directed at one's forces from the buildings located in the area of the battlefield, which house both terrorist cells and innocent civilians. The decision on how to act in such situations is a real dilemma.

In Jenin, for example, there was initially no plan to take control of the refugee camp, but the circumstances on the ground – including the enemy's resolve to fight without regard for casualties to its own civilians – dictated the IDF's methods of operation. This operation of force of such large proportions had commensurate results. The triangle sketched above is the key for operating force in asymmetrical warfare within densely populated areas. In complex situations of this kind, it is possible to operate most effectively and optimally only by being exactly in the center. The political and decision making echelons must internalize that without understanding this triangle, the fighting will not succeed and the mission will fail.

In this sense Operation Cast Lead was unusual. Hamas was patently unprepared and unorganized; in terms of functioning like an organization, it was still in its infancy and was certainly not ready for the force brought to bear against it. One must consider that this was a one-time occurrence; next time, the enemy will be much better prepared.

There are three key issues, then, in asymmetrical fighting in densely populated areas. The first is to understand the challenges. If the IDF as well as Israel's decision makers understand the challenges, they will be able to prepare better for this type of warfare. As a conventional army, the IDF is still captive to the paradigm of conventional use of force. It is imperative to change this way of thinking and paradigm and understand the nature of warfare in densely populated areas and prepare for it. A different way of organizing the force – from preparing operational units to operating more

effective means of contact with the civilian population – will ensure better results in the future. Some of the positive results of Operation Cast Lead stemmed from the lessons learned through less successful efforts during Operation Defensive Shield.

The second key issue is to instill behavioral norms and rules of engagement. The IDF is used to operating in the format of army versus army, a much simpler and straightforward format. When the civilian factor enters the equation, the attacking force must be prepared not only operationally but also mentally. The level of friction with the civilians and the complexity and difficulties described above often result in uncontrolled use of fire by soldiers towards civilians. Restraining the force and handling these responses are critical to success.

The third key issue in asymmetric warfare is intelligence. Commanding officers and decision makers must understand that when they look through their binoculars, the true picture of the battle is not the tank battalion they're seeing at a distance, rather the huddle of civilian houses in the background. Therefore, it is their responsibility to prevent fire coming from those houses. The picture seen through the binoculars, in which there doesn't seem to be an enemy, must – using the means currently at our disposal – be turned into a picture in which the enemy is defined as clearly as possible.

The success of Operation Cast Lead lay precisely in this picture of the battle. At first glance, all that was seen was a civilian neighborhood, but in practice, every soldier who participated in the mission knew very well how the enemy was organized within it: which building had mortar bombs underneath it and which house had an attic full of ammunition. This is the capability that determined the outcome.

Obligations of International Humanitarian Law

Knut Doermann

It is an understatement to say that armed conflicts fought in densely populated areas can and do cause tremendous human suffering. Civilians in particular have historically paid a high price in the form of death, injuries, and permanent disabilities. They have also paid indirectly through the effects of widespread damage to their homes, the impact on their livelihoods, and the destruction of the infrastructure that supplies the necessities of life. With modern conflicts increasingly fought in urban areas, civilians are increasingly caught in the midst of hostilities. Such a trend will surely continue into the future.

Urban areas are by nature complex environments, and military operations in or against such areas confront a variety of significant challenges. These include the co-mingling of combatants and military objectives with civilians and civilian objects, the fluid and often unconventional tactics used by defending combatants, and the risk of sudden interaction with civilians. Such factors may make it difficult for the attacker to properly identify enemy forces and military objectives. It may also complicate assessment of the incidental civilian casualties and damage that may result from operations. Managing the safety of one's own troops and minimizing the impact of the fighting on civilian populations in such situations is often a challenging task for every armed force.

Dr. Knut Doermann is Head of the Legal Division of the International Committee of the Red Cross (ICRC), Geneva. The views expressed here are those of the author and do not necessarily reflect those of the ICRC. Special thanks go to Louis Maresca, Legal Advisor, ICRC Legal Division. This essay is based on a lecture delivered at the INSS-ICRC conference "Challenges of Warfare in Densely Populated Areas" in December 2011.

In spite of these challenges, there is an important body of international law that applies in these situations, regulating the behavior of combatants and protecting those not taking part in the hostilities. The rules on the conduct of hostilities that will be addressed in this article are mainly found in the 1977 Additional Protocol I (AP I) to the Geneva Conventions. These rules apply in international armed conflicts, and since their adoption have become customary international humanitarian law (IHL) – and thus are also binding on states that have not ratified the AP such as the United States and Israel. Most of them are also widely accepted as customary law applicable in non-international armed conflicts.

These rules are complemented by additional rules relative to specific weapons. These rules were meant and drafted to be applied in all types of situations, including warfare in urban settings. This is also the reason why they are formulated in a fairly general and abstract way, in order to cover all situations and all methods and means of warfare. Therefore they are a priori capable of and appropriate in dealing with developments in modern warfare that arose after the rules were adopted. Furthermore, the rules were negotiated in the 1970s against the backdrop of guerrilla warfare and asymmetries in warfare, and as such, these issues affected the negotiations. These rules were also developed with awareness that there may be situations where the other side will violate the rules. Moreover, since international humanitarian law is not built on a legal concept of reciprocity, the rules must apply even when violations have been committed by the other side. The rules provide a degree of appreciation, which is necessary in volatile, complex combat situations, for commanders who sometimes have to make decisions in a matter of seconds. Compliance with the rules is assessed based on the information available to the commander at the time of deciding on an attack and an assessment of what a reasonable commander with that information should do in such a situation.

The Rule of Distinction

Considering the legal framework more specifically, the starting point is the fundamental IHL rule on distinction, that is to say, the requirement that the parties to an armed conflict must at all times distinguish between civilians and combatants as well as between civilian objects and military objectives. From this fundamental rule of IHL flow a number of specific obligations aimed at protecting civilians from the dangers arising from

military operations. These rules regulate the conduct of hostilities, and they contain requirements for all parties to an armed conflict and all operations undertaken in attack and in defense.

Two questions arise in any discussion of the laws regulating the conduct of hostilities. First, it must be determined who can legitimately be attacked, and second, which objects can be legitimately attacked. International humanitarian law distinguishes between two categories of persons. The first category encompasses members of the armed forces, meaning those who conduct the hostilities on behalf of the parties to an armed conflict. This category includes the regular and irregular armed forces of states, and also the members of an organized armed group fighting on behalf of a non-state party in a non-international armed conflict. Civilians, the second category, are defined as those persons who are not members of the armed forces of a party to the conflict. Only members of the armed forces and of organized armed groups are legitimate targets of an attack. It is absolutely prohibited to attack civilians or the civilian population. Civilians are entitled to protection from direct attack unless and for such time as they directly participate in hostilities. The notion of direct participation in hostilities as it relates to civilians only comes into play when they are carrying out an act cumulatively fulfilling the following three requirements:

a. The act must be likely to affect adversely the military operations or military capacity of a party to an armed conflict, or alternatively, to inflict death, injury, or destruction on persons or objects protected against direct attacks.
b. There is a direct causal link between the act and the harm likely to result either from that act, or from a coordinated military operation of which that act constitutes an integral part.
c. The act is specifically designed to support one party to the conflict against another.

Any person who is neither a direct participant in hostilities nor a member of an organized armed group as defined above is entitled to the full protection accorded to civilians.

The question of who belongs to organized armed groups and who can be seen as participating directly in hostilities, and thus loses protection against direct attack, has been debated for years. At a certain point the International Committee of the Red Cross (ICRC) engaged in an expert process to clarify this issue and subsequently published an interpretive guide that clarified

the question.[1] In the view of the ICRC, the term "organized armed group" refers exclusively to the "armed" or "military" wing of a non-state party to an armed conflict, namely its armed forces in a strictly functional sense – in other words, those who are charged with the conduct of hostilities on its behalf. Only persons assuming a continuous combat function (i.e., a continuous function involving their direct participation in hostilities) can be regarded as belonging to an organized armed group and as such can be legitimately attacked.

A reliable determination of membership in an organized armed group (i.e., continuous combat function) or of direct participation in hostilities may not always be straightforward. This is particularly true in an urban setting where various actors intermingle and where places to hide or positions from where to launch an attack abound. Such a context normally demands rapid military decisions and actions. Thus, the determination of membership or direct participation in hostilities may not be an easy task for military forces. It is therefore all the more crucial that all feasible precautions be taken to determine whether a person is a civilian, and if so, whether he or she is directly participating in hostilities. In case of doubt, IHL mandates that a person is presumed to be a civilian and protected against direct attack.

It is important to bear in mind that once a person has been identified as assuming a continuous combat function for an organized armed group or as a civilian directly participating in hostilities, the attacker is not automatically free to attack this person. Indeed, an attack against such a person may still be prohibited under other rules of IHL. For example, such an attack would be prohibited under the rule of proportionality if it would lead to excessive incidental civilian casualties and/or damage.

Concerning the question of what objects can be attacked, the rule of distinction prescribes that only military objectives can be attacked. According to customary international law, military objectives are limited to those objects that by their nature, location, purpose, or use make an effective contribution to military action; and in addition, whose total or partial destruction, capture, or neutralization, in the circumstances at the time, offers a definite military advantage.

With regard to the first of those two criteria, a close link must be established between the potential target and "an effective contribution to military action." The term "military action" denotes the enemy's war

fighting capabilities. This nexus is established through the four criteria outlined in the rule, namely its nature, location, purpose, or use. "Nature" refers to the intrinsic character of an object. For example, a weapon system or a missile launching site are objects that make an effective contribution to military action by their very nature. Objects that are not military by nature may also make an effective contribution to military action by virtue of their particular location, purpose, or present use. However, it is important to keep in mind that the contribution must be effective, and must also be directed towards the actual war-fighting capabilities of a party to the conflict. This second point follows from the reference in the definition to "military action." If an object merely contributes towards the war-sustaining capability of a party to the conflict, i.e., its general war effort, it does not qualify as a military objective.

Regarding the second criterion, namely that the total or partial destruction, capture, or neutralization of the target in the circumstances ruling at the time offers a definite military advantage, an object is a military objective if an attack on it would bring about "a definite military advantage." It follows from the word "definite" that the advantage must be concrete and perceptible, and not merely hypothetical or speculative. From the word "military," it can be inferred that the anticipated advantage must not be of a mere political nature. Even when the military advantage is derived from the "attack as a whole," it bears emphasis that the "attack as a whole" constitutes a finite operation with defined limits and must not be confused with the entire war effort. Finally, the military advantage to be gained must be evident "in the circumstances ruling at the time." If the destruction of a given object does not yet offer or no longer offers a definite military advantage, the object would not constitute a military objective and must not be attacked.

Again, it is important to bear in mind that once an object has been identified as a military objective on the basis of these criteria, the attacker is not free to launch an unrestrained attack on this object. Indeed, even if a military objective has been properly identified, an attack may still be prohibited under other IHL rules, in particular if it would lead to excessive incidental civilian casualties and/or damage to civilian objects. In densely populated areas and other circumstances, whether or not an object constitutes a military objective must be assessed on a case-by-case basis in view of the ruling circumstances at the time. Sweeping or

anticipatory qualifications of an object are not allowed. For example, it would clearly be contrary to IHL if all objects somehow related to, owned by, or associated with a party to the conflict were collectively considered as military objectives.

When assessing whether or not something is a military objective, one difficult issue is the question of dual use objects, which are often found in densely populated areas. A dual use object is an object that has simultaneous military and civilian functions. One example is the electricity power grid, which is used by the military to operate air defenses and is also used to power hospitals and other civilian activities. If the standards relating to military objectives mentioned above are applied, even a secondary military use may turn a civilian object into a military objective. However, such use must be carefully verified and any attack would need to be consistent with other rules on the conduct of hostilities.

Indiscriminate Attacks and the Rule of Proportionality

Among such rules are the prohibition of indiscriminate attacks and the rule of proportionality. Indiscriminate attacks are those that are not directed at a specific military objective; that employ a method or means of combat which cannot be directed at a specific military objective; or that employ a method or means of combat whose effects cannot be limited as required by IHL; and consequently, in each such case, are of a nature that strike military objectives and civilians or civilian objects without distinction.

In an area where civilian objects and military objectives are mixed, the attacking party must assess with particular care which objects are civilian objects and which ones are military objectives. Only those objects that qualify as military objectives can be directly attacked with weapons that are capable of being directed at them and that have effects that can be limited as required by IHL. Attacks by bombardment or any method or means that treat a number of clearly separated and distinct military objectives located in a city, town, village, or other area as a single military objective containing a similar concentration of civilians or civilian objects are prohibited under IHL.

Once a legitimate target of an attack has been properly identified, the rule of proportionality must be assessed. This rule prohibits attacks "which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which

would be excessive in relation to the concrete and direct military advantage anticipated." Again, direct attacks against civilians and civilian objects are prohibited. The rule of proportionality, therefore, only becomes relevant when military objectives are the intended targets. Note that it is not only excessive civilian casualties and injuries that are prohibited by the rule of proportionality, but also excessive damage to civilian objects. This fact is often overlooked or forgotten.

The damage to civilians must be balanced by the military advantage that will be gained by a particular attack. Weighing the military advantage against the civilian damage is often very difficult, particularly because they are not easily comparable. How can one weigh something concrete in terms of loss of life and destruction against something that is more relative, such as the military value of an operation? Yet despite all the uncertainties in the interpretation of the rule of proportionality, there are nevertheless very clear limitations set by the rules. Only the "concrete" and "direct" "military" advantages can legitimately weigh in the determination as to whether the consequence of an attack would be excessive. Hypothetical, indirect, and long term political advantages must be excluded from the calculation of military advantage. Simply winning the war cannot be considered a criterion for calculation of proportionality. When assessing the incidental damages to civilians and civilian objects, the foreseeable reverberating effects of the attack on the civilian population must also be taken into consideration. For example, if attacks are launched against electrical grids or telecommunications infrastructures, which may be military objectives in a particular situation, these may potentially cause incidental damage to the future wellbeing of the civilian population, through the death of patients in medical facilities or the long term disruption of electricity supplies. Such consequences must be factored into the equation.

There is much debate regarding the use of certain explosives in densely populated areas. Certain weapons, by virtue of the way they function or because of their substantial explosive power, may be more likely to have indiscriminate effects and an increased likelihood of causing excessive incidental civilian casualties and damage to civilian objects when used in densely populated areas. Weapons that have a significant degree of inaccuracy or that have a wide destructive radius may not be much of a concern on an open battlefield far away from civilian installations, but their use against military objectives positioned in an urban setting and in the

vicinity of civilians or civilian objects may be troublesome. The ICRC has therefore expressed concern about the use of high explosive air dropped bombs, artillery, mortars, and munitions containing white phosphorus in urban areas. The concern about high explosive air dropped bombs, artillery, and mortar shells is generally due to the difficulty of directing such weapons at specific military objectives, and their potentially wide explosive footprint. Their use in densely populated areas raises serious concerns under the prohibition of indiscriminate attacks and the rule of proportionality, among others. The attacking army is obligated to take all feasible precautions to avoid and minimize incidental civilian casualties and damage to civilian objects. This also applies to the choice of weapons and means of warfare. Alternatively, more discriminative weapons and means of attacking military objectives located in densely populated areas must be chosen instead of, for example, free flight projectiles fired by artillery or mortars. In light of this and despite the absence of an express legal prohibition for specific types of weapons, the ICRC believes that explosive weapons with a wide impact area should be avoided in densely populated areas.

Precautions Required of Both Sides

In the conduct of military operations, constant care must be taken to spare the civilian population, individual civilians, and civilian objects. The particular precautions required by IHL include doing everything feasible to verify that targets are military objectives and taking all feasible precautions in the choice of means and methods of warfare with a view to avoiding and in any event minimizing incidental civilian casualties and damages to civilian objects. In densely populated areas, special attention must be paid to the type of weapons and munitions used in order to spare, as much as possible, civilians and civilian infrastructure.

Advance warning to the civilian population is one of the core precautions that must be taken prior to an attack. Effective advance warning must be given regarding attacks that may affect the civilian population, unless circumstances do not permit. The aim is to provide civilians with the opportunity to protect themselves. The main requirement in this regard is that an advance warning must be "effective." The effectiveness of a warning should be evaluated from the point of view of the civilian population that receives it. An effective advance warning will allow civilians to adequately

protect themselves. Generally, this would mean that the advance warning should be constructed so as to reach as many civilians as possible in the concerned area of the planned attack. It should also be in a language that the civilian population understands and it must give civilians enough time to evacuate. In addition, such a warning should not be issued prematurely or in an untimely fashion, so as to lead the civilian population to believe that the threat of an attack is no longer real.

Advance warnings do not relieve an attacker from the obligation to take other precautionary measures. Indeed, as mentioned above, effective advance warnings amount only to one of several precautions prescribed by IHL. The fact that a warning has been given does not mean that an attack may automatically proceed. An assessment of distinction and proportionality must still be made, and the attacker is obliged to take precautions in order to avoid and in any event to minimize the incidental loss of civilian life, injury to civilians, and damage to civilian objects. In particular, even if advance warnings are given, experience shows that often a number of civilians remain in the area. It is not permissible to consider everyone who remains in an area after advance warnings to be legitimate targets.

Several of these obligations to take precautions are not absolute, but depend on what is "feasible" at the time. Thus, again, certain discretion is given to those who plan or decide upon an attack. According to various interpretations, feasible precautions are those that "are practicable or practically possible taking into account all circumstances ruling at the time, including humanitarian and military considerations." In this context, it is debatable what weight should be given to the understandable aim of ensuring the safety of the attacking side's armed forces ("military consideration") when an attack is launched. To the ICRC, it does not seem appropriate to resort to such considerations as a justification for not taking any precautionary measures in the implementation of the rules of distinction or proportionality and thereby exposing the civilian population or civilian objects to a greater risk. There would also certainly be no justification to resort, for example, to indiscriminate fire in violation of the mentioned IHL rules in order to avoid exposure of one's troops. While national regulations may require military commanders to protect their troops, under IHL combatants may be lawfully attacked. This is the corollary of their right to directly participate in hostilities. Civilians – as

long as they do not participate directly in hostilities – as well as civilian objects must not be made the object of an attack. Thus, the provisions of IHL clearly emphasize the protection of civilians and civilian objects.

The side that is the object of an attack also has obligations under international humanitarian law. It must also take necessary precautions to protect civilians and civilian objects under their control against the effects of military operations. Such precautions include removing them from the vicinity of military objectives or avoiding the location of military objectives within or near densely populated areas to the maximum extent feasible.

In addition, under no circumstances may civilians be used to shield military objectives from attack or to shield military operations. It is a well-established rule of IHL that the use of human shields is prohibited and constitutes a war crime. Therefore, the party facing an attack is prohibited from abusing the obligations of the attacker not to target civilians and civilian objects by using the civilian population, individual civilians, or civilian objects to shield a military objective. This rule also covers the transferring of civilians to the vicinity of a military objective as well as placing military objectives in or near civilian areas.

What is the consequence for the commander ordering an attack if human shields are nevertheless used? The use of human shields does not necessarily prevent him from proceeding with the attack. However, any violation of the prohibition on using civilians as human shields does not release the attacker from his obligations with respect to the civilian population and individual civilians, including the obligation to take the required precautionary measures. Can voluntary human shields be considered direct participants in hostilities with the consequence that they lose protection against direct attack and would not count in the proportionality equation? The fact that some civilians voluntarily and deliberately abuse their legal entitlement to protection from direct attack in order to shield military objectives does not, without the fulfillment of other conditions, entail the loss of their protection and their liability to direct attack independently of the shielded objective. This, in the view of the ICRC, would only be the case if they create a physical obstacle to military operations of a party to the conflict. This scenario may become particularly relevant in ground operations, such as in urban environments where civilians may attempt to give physical cover to fighting personnel supported by them or to inhibit the movement of opposing infantry troops.

Even if voluntary human shields are not directly participating in hostilities, they will be particularly exposed to the dangers of military operations through their presence near legitimate military objectives, and therefore incur an increased risk of suffering incidental death or injury during attacks against those objectives.

The Asymmetric Nature of Modern Armed Conflicts

Significant disparities between the military capacities of the belligerent parties, or in other words, asymmetric warfare, bring significant challenges for the application of IHL, in particular its rules on the conduct of hostilities. For instance, a belligerent party that is weaker in military strength and technological capacity may, when under attack, be tempted to hide from modern sophisticated means and methods of warfare. Consequently, it may be led to engage in practices prohibited by IHL, such as feigning protected status, mingling combatants and military objectives with the civilian population and civilian objects, or using civilians as human shields. As for the militarily superior belligerent, it may be tempted to relax the standards of protection of civilian persons and civilian objects in response to constant violations of IHL by the adversary. For example, confronted with enemy combatants and military objectives that are persistently hidden among the civilian population and civilian objects, an attacker – who is legally bound by the prohibition of disproportionate attacks – may, in response to the adversary's strategy, progressively revise his assessment of the rule of proportionality and accept more incidental civilian casualties and damage.

The ICRC has observed that in a number of recent conflicts, there is an increased pressure on the military to protect its forces due to the reluctance of the states' constituencies to tolerate casualties and capture of their soldiers on the battlefield. In this context, it is debatable what weight is to be given to the legitimate aim of ensuring the safety of the attacking side's armed forces when an attack is launched. In any case, this consideration cannot lead to circumventing the principles of distinction, proportionality, and precaution. Nor does force protection take on increased weight in asymmetric warfare because of the military or political goals of the adversary. For instance, considerations of force protection cannot override the principle that when there is a doubt whether a person is a civilian or not, he or she must be considered to be a civilian. Also, as stated before, force

protection cannot lead to indiscriminate firepower by troops as a measure to avoid the exposure of its own forces. In this context, it must be borne in mind that new technologies can in some cases reduce the risk for the attacking force's soldiers, but might also in some cases – in particular in densely populated areas – increase the risk of incidental civilian casualties and damage, such as, for instance, the use of air strikes, the use of indirect fire, or the use of white phosphorus munitions to create smokescreens.

The real danger in asymmetric conflicts is that the application of IHL will be perceived as detrimental by all the parties to a conflict. This will ultimately lead to all-around disregard for IHL and undermine its basic tenets. In light of this, it is perhaps logical to ask, where does IHL go from here? What are the best ways to address the challenges raised by the waging of war in densely populated areas and the asymmetries in warfare? The ICRC believes that the challenges posed to IHL by asymmetric and urban warfare cannot a priori be solved by developments in treaty law. It must be stressed that in such circumstances, it is generally not the rules that are at fault, but the will or the ability of the parties to an armed conflict – and of the international community – to enforce them, in particular through criminal law.

Conclusion

The ICRC recognizes that today's armed conflicts, especially asymmetric ones and those fought in densely populated areas, pose serious threats to the rules derived from the principle of distinction. It is crucial to resist these threats and to make every effort to maintain and reinforce rules that are essential to protecting civilians, who so often bear the brunt of armed conflicts. The rules themselves are as pertinent to "new" types of conflicts and warfare as they were to the conflicts or forms of warfare that existed at the time when they were adopted. The fundamental values underlying the rules of the conduct of hostilities need to be safeguarded and are timeless. While it is conceivable that developments in IHL might occur in specific areas, such as in relation to restrictions and limitations on certain weapons, a major rewriting of existing treaties does not seem necessary for the time being.

At the same time, there is an ongoing need to assess the effectiveness of existing rules in protecting civilians and civilian objects, to improve the implementation of those rules or to clarify the interpretation of specific

concepts on which the rules are based. However, this must be done without disturbing the framework and underlying tenets of existing IHL, whose aim is precisely to ensure the protection of civilians. Despite certain shortcomings in some of the rules governing the conduct of hostilities, mostly linked to imprecise wording, these rules continue to play an important role in limiting the use of weapons. Any further erosion of IHL may propel mankind backwards to a time when the use of armed force was almost boundless. The challenge is to examine and interpret how the rules of international humanitarian law should be applied in particular circumstances, but the values and principles inherent in international humanitarian law must remain unchanged, and be defended and upheld in the future.

Notes

1 See the ICRC interpretive recommendations in Nils Melzer, *Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law* (Geneva: International Committee of the Red Cross, 2009).

Operation Unified Protector: Targeting Densely Populated Areas in Libya

Christian de Cock

A War is a War is a War?

Although at first sight many issues related to targeting densely populated areas seem similar, regardless of the type of conflict and the area where hostilities take place, it should be recalled that what works in the framework of one operation does not necessarily work in another operational context.[1] This can be illustrated by two contemporary conflicts in which air assets play or played a major role: Afghanistan and Libya. Air operations conducted in the framework of International Security Assistance Force (ISAF) are similar but not identical (and thus different) from those conducted during Operation Unified Protector (OUP). This is based on the fact that different criteria impact on the execution of air operations, including: the strategic end state, the nature of the enemy forces, the classification of the conflict, the mission-specific air operations, the presence of ground forces, and the rules of engagement (table 1). It is crucial to be aware of those differences, because otherwise there is a risk of applying the wrong standards or the wrong rules of engagement to the wrong conflict. What worked for Operation Unified Protector worked in

Lieutenant Colonel (GS) Christian de Cock is Chief of the International Law Section at NATO. He served as a legal advisor assisting BEL air crews in NATO missions in both Afghanistan and Libya. The views expressed in this paper, which is based on a lecture delivered at the December 2011 conference "Challenges of Warfare in Densely Populated Areas," sponsored by INSS and the International Committee of the Red Cross, are those of the author in his personal capacity and do not intend to reflect the views of the DG, the Ministry of Defense, or NATO. A more detailed analysis of the conflict in Libya by the author will be published in the upcoming *2012 Yearbook of International Humanitarian Law* (T.M.C. Asser Press).

Libya (at that time) but doesn't necessarily work in Afghanistan, and vice versa. This is a logical consequence of the differing surrounding conditions in which the air crews had to operate in Afghanistan and Libya. In sum: every conflict is characterized by its own dynamics, despite the similarities to other conflicts.

Table 1. ISAF vs. OUP: Comparison of Parameters

Criteria	Afghanistan: ISAF	Libya: OUP
Strategic end state	Stable and secure environment	Protection of civilians
Classification of conflict	Non-international armed conflict (NIAC)	International armed conflict (IAC)
Boots on the ground	Yes	No
Enemy forces	Non-state actor	State actor (Libyan armed forces)
Type of warfare	Irregular/asymmetric warfare	From regular to irregular warfare
Air operations	Close air support (CAS)	From defensive counter air (DCA) to offensive counter air (OCA)
Rules of Engagement	Reactive/offensive	Offensive

End State

First of all, the strategic objectives in Afghanistan and Libya were different. While in Afghanistan the strategic objective was/is to create "a secure and stable environment,"[2] in the Libyan Unified Protector mission the strategic objective was "to protect the civilians and civilian populated areas under attack or threat of attack" by the Libyan armed forces and associated forces.[3] It is important not to lose sight of these strategic objectives, as the importance of strategic objectives is not purely academic.[4] Strategic objectives are important because even in situations where the use of force is authorized by implemented rules of engagement (ROE),[5] the tactical advantage to be gained from an attack can have tremendous consequences on the strategic level.[6] Those strategic objectives are translated into a

military end state where decisive points will be defined in the operational planning process. But in order to achieve those decisive points, e.g., gaining and maintaining air superiority, accurate rules of engagement are needed to allow the armed forces to conduct the operation in accordance with the mandate and to achieve, at the end of the armed conflict, the strategic objectives established by the UN Security Council resolutions.

Boots on the Ground

The operations in Libya and Afghanistan were also different in terms of the type of war that was waged, the nature of the enemy, and the capacity of the NATO forces that were engaged. In Afghanistan ground forces were available so an aircraft could be guided to a military objective by qualified forward air controllers. For example, the Joint Terminal Attack Controller (JTAC) could help lead that aircraft to the military objective and strike that military objective. That was not the case as far as the operations in Libya were concerned. NATO had no boots on the ground.[7] Consequently, aircrew could not rely on JTAC to positively identify ground targets and the assessment of the ground commanders with regard to the combat development (CD) to be expected from the attack. Other means were used to make such determinations, and experience proved that these processes met the standards to comply with the requirements of the law of armed conflict.

Irregular Warfare Used by a Non-State Actor

Another difference between the two operations is that the ISAF in Afghanistan is fighting an asymmetric war against a non-state actor (NSA) that deliberately refuses to comply with the laws of armed conflict. This made ISAF a counterinsurgency operation, and this meant that the means and methods of combating those non-state actors had to be adapted significantly to achieve the final objective. Today, the conflict in Afghanistan can be classified as a non-international armed conflict (NIAC).

In Operation Unified Protector, at least when NATO operations began, the conflict pitted the Libyan armed forces against the coalition forces. According to the traditional principles of warfare, this was an interstate armed conflict between two or more states.[8] Later, however, the Libyan armed forces changed their tactics and their strategy from traditional warfare to irregular warfare. They stopped wearing uniforms and began

using vehicles that were difficult to distinguish from civilian vehicles. This made it much more difficult for NATO to distinguish between the armed forces, mercenaries, and other individuals affiliated with Libyan armed forces and the civilian population. This of course did not alter the classification of the conflict, which was still international in character. The point is that even in the context of an international armed conflict, NATO and NATO-led forces were confronted with irregular warfare from regular forces, and consequently, the approach that had to respond to this new phenomenon was somewhat similar to the tactics and procedures used in traditional counterinsurgency campaigns. When regime forces were forced to flee and the Transitional National Council took power after the fall of Tripoli, the conflict between NATO/NATO-led forces and the former regime troops became a non-international armed conflict.

This was also the case in Afghanistan. When Karzai took office in Kabul, the conflict in Afghanistan shifted from an international armed conflict (IAC) to a non-international armed conflict. In Libya, from a targeting perspective, this change in government made no difference as far as dynamic or deliberate targeting issues were concerned. Coalition forces continued to apply the standards of the law of international conflict, even though from a legal point of view, the situation evolved from an IAC to an NIAC. In other words, there was no legal consequence of this change, since coalition forces continued to apply the rules of international conflict in the context of a non-international armed conflict. The legal framework for the intervention was based on the law of international armed conflict, which is basically customary international law, the Geneva Conventions, and the Additional Protocol I (AP I).

Impact of Air Missions

The air missions in Libya were also quite different from the missions that were carried out in Afghanistan, influenced by, inter alia: the objectives of the operations, the availability of ground forces to assist aircrew in their missions, and the type of targets to be pursued. In most cases, the air missions in Afghanistan can be classified as "close air support" missions in order to support the ground forces. In Libya, air operations ranged from defensive counter air to offensive counter air missions. From a targeting point of view, ISAF air missions were flown more "dynamically," while Operation Unified Protector combined "deliberate" and "dynamic"

missions. In the beginning, the focus was rather "deliberate" and shifted later to more "dynamic" missions. Additionally, the deliberate targeting process had to be shortened in order to keep on track with the operational pace.

The operation had three main objectives. The first goal was the protection of civilians and civilian populated areas under attack or threat of attack, which was to be accomplished without a foreign occupation force. The second objective was to enforce the no-fly zone. There was not necessarily a direct link between the enforcement of the no-fly zone and the protection of the civilian population. In practice, it was not always clear whether a particular engagement was part of the second objective, the no-fly zone, or whether it was part of the first objective, the imperative to protect civilians and civilian populated areas. The third objective was the embargo.

Regarding the OUP strategic objective of protection of the civilian population and civilian populated areas under attack or threat of attack, one of the issues that arose was whether or not the objective was limited to *jus ad bellum*. Was it necessary to have a direct and causal link between the military objectives planned by NATO and the strategic objective of protecting the civilian population? In other words, each time the crew decided to strike a particular target did they need a direct link to the protection of the civilian population, or was this strictly the overall strategic objective and the end state? Different views exist on the interpretation of this wording in the UNSC Resolution. The protection of the population as a strategic end state permitted the striking of targets, even if they were not directly attacking the civilian population. Other issues arose from the wording of UN Security Council Resolution 1973.

It is important to note that NATO did not support the rebels against the forces of Colonel Qaddafi. The mandate was clear in this respect. NATO and the coalition of the willing (before NATO assumed responsibility for the implementation of UNSCR 1973) were engaged to protect the civilians and the civilian population. Although some indirect effects of this intervention did benefit the rebels in their internal armed conflict against the regime forces, there was no deliberate support for the rebels in their fight against the regime forces. Consequently, the conflict in Libya was not an "internationalized" internal armed conflict. From a legal point of view, there were two armed conflicts on Libyan territory: a non-international

armed conflict between the rebels and the regime forces, and following the implementation of UNSC Resolution 1973, an international armed conflict between NATO-led countries and the Libyan armed forces. There was a coexistence of two different armed conflicts, and the NATO nations did not consider themselves involved in an internationalized non-international armed conflict. This also results from the wording of the mandate, which did not mention the opposing parties in the respective operative paragraphs of the resolution. The mandate had to be implemented in an impartial way and the Security Council resolution was construed broadly, so that if the rebels attacked civilians or civilian populated areas, NATO could engage rebel forces as well. The second aspect that confirms that NATO did not support the rebels is the fact that NATO gave Qaddafi forces the opportunity to retreat and return to their barracks. Had they taken this opportunity and had rebel forces attacked them, then the regime forces would have had an inherent right to defend themselves and the coalition would not have interfered in this internal struggle.

In conclusion, there were two different parties, the rebels and the regime forces, regulated by the law of non-international conflict. Until the fall of Colonel Qaddafi's regime, there was an international conflict between the different nations of the coalition and the regime forces of Colonel Qaddafi. Later, the IAC turned into an NIAC when the National Transitional Council became the governing authority in Tripoli.

Direct Participation in Hostilities

Mercenaries who on an individual or organized basis assisted the Libyan authorities in suppressing civilians, mainly in the eastern part of Libya, were considered to be directly participating in hostilities. From an international humanitarian law (IHL) perspective, if an individual is a member of an organized armed group, and if he/she participates in hostilities, then he/she becomes a legitimate military target. Organized armed groups acting as armed forces of non-state actors are legitimate military objectives for the entire duration of the conflict, unless they leave the group or become *hors de combat*.

Some human rights advocates argue that these individuals can only be targeted if they have a "continuous combat function," as suggested by the ICRC Interpretive Guidance on the notion of direct participation in hostilities. This is false. If these individuals are members of an organized

armed group, they are a legitimate military target on a 24/7 basis for the entire duration of the conflict, whether they perform a combat, combat support, or even combat service support function (unless they become *hors de combat*). This principle also determined the way in which mercenaries and other persons who directly participated in hostilities, without being a member of the Qaddafi armed forces, were considered in terms of targeting. They were considered legitimate military targets. Furthermore, individuals or groups who were not directly attacking the civilian population at a certain point but were known to be a future threat to civilians could also be targeted without violating international humanitarian law.

Voluntary Human Shields

Civilians who give up their immunity to deliberately and voluntarily shield military objectives from attack are directly participating in hostilities, and while they participate directly in hostilities they lose their immunity from attack. The military objective they are trying to protect can be attacked, and the voluntary human shield should not be factored into the proportionality analysis.

Three basic views exist on this particular issue. IHL advocates argue that even voluntary human shields remain civilians, and consequently they may not be attacked and should be accounted for in the proportionality analysis. At the other end of the spectrum, some argue that those who engage in voluntary shielding are directly participating in hostilities and thus are liable to attack. Finally, the middle position is that they are not directly participating in hostilities, but on the other hand, should not figure in the proportionality analysis.

Human Rights Law and Targeting

The role of human rights in the law of armed conflict is controversial. Proponents of human rights have tried to introduce principles such as the right to life within the context of the law of armed conflict (LOAC) for the purpose of targeting and the use of force.

Human rights law cannot be applied in the targeting process. In the conduct of hostilities in international armed conflict, the *lex specialis* is the law of armed conflict, which unambiguously determines who can and cannot be targeted. If the enemy combatant (the term is used here in a generic way) is not *hors de combat*, he/she remains a legitimate target on a

24/7 basis for the entire duration of the armed conflict. There is no place for human rights in the conduct of hostilities with regard to the principle of distinction or the principle of proportionality.

The proportionality analysis under human rights law is totally different from proportionality in the law of armed conflict, as enshrined in the AP I. The proportionality analysis in human rights law is a strict proportionality analysis in the framework of the right to life provision, which can be found in the different regional human rights conventions such as the European Convention on Human Rights. The European Court of Human Rights should embrace its essential mission, which is the safeguarding of human rights in a human rights context. In a situation of peace or an emergency situation, the right to life provision applies, and a court must apply this provision. But if the court is dealing with an international human rights issue in the context of an armed conflict, then there is no place even under Article 2 for the right to life provision, which distorts LOAC to the point that it makes no sense.

Targeting Process

Once the war began, the key missions for coalition air forces were essentially to enforce the no-fly zone in order to gain and maintain air superiority, prevent (artillery and armored) attacks on civilian areas, and enable humanitarian assistance missions to enter Libya. NATO-led air forces had an unprecedented ability to execute these missions and the ability to paralyze the Libyan air force. The systematic suppression of Libyan air defense systems allowed NATO to achieve air superiority shortly after the first days of the operation.

The ability to rapidly target and re-target proved to be crucial in achieving the mission objectives, especially when regime forces transformed their fighting tactics from regular to irregular warfare. One of the major concerns was that the 72-hours deliberate targeting process could not (always) keep pace with the dynamics of the battlefield, because the planning to execution cycle was too long and the process did not react quickly enough to changes in the scheme of maneuver. Shortening the 72-hours targeting cycle and pushing the targeting planning cycle closer to execution helped keep the Prioritized Target List more current (and relevant) during Air Task Order execution. A guiding principle of the air campaign was to achieve maximum effect with minimum force. The use of precision guided munitions was the

key, helping NATO achieve its objectives more quickly while minimizing civilian casualties. Precision weapons were used against targets in (densely) populated areas where the aim was to destroy single targets while leaving neighboring buildings intact. Because no ground troops were deployed during OUP, unmanned aerial vehicles (UAV) were of utmost importance.

One of the central lessons learned during OUP was that the mandate should be very clear so that operators do not have any doubt as to what they can and can't do in the context of an armed conflict. It is the responsibility of the legal advisors to assist the operational staff in interpreting and translating those rules of engagement so they can be applied in day-to-day operations. Pilots must receive clear instructions as to what they can do and can't do in prosecuting targets. In dynamic targeting in Libya, the targets were categorized according to the level of civilian or collateral damage that resulted from the strike. The higher the expected collateral damage, the higher the authority needed to engage that target. In order to protect pilots against prosecution for their actions during such an operation, the pilots' decision making authority was restricted to basic levels of lower collateral damage levels, with no nearby collateral damage concerns within the range of their ordinance (type GBU 12 and 38). All other targeting decisions, that is to say exceeding the collateral damage levels delegated to the aircrew, had to be dealt with within the Combined Air Operations Center (CAOC), which is essentially what was done during Operation Unified Protector as well. In dynamic and in deliberate targeting, if the level of collateral damage exceeded the aircrew-delegated CD authority levels, the decision to strike was transferred to the Combined Air Operations Center (CAOC) for further consideration. This is because at the CAOC, additional intelligence was available that could be used to assess the collateral damage concerns, such as, inter alia, live feed from UAVs (if and when available). The live feed was sometimes used to assess whether the targeting and prosecuting of a particular target still complied with the LOAC requirements. Intelligence and UAVs proved to be crucial, especially where C^2 nodes and other targets were located in urban areas.

Conclusion

Operation Unified Protector was conducted successfully by NATO and NATO-led forces in order to achieve the strategic objectives in accordance with the UNSC mandate. Different issues arose in the context of this

operation, both legally and operationally. From a legal perspective, the conflict was an international armed conflict until the National Transitional Council took power following the fall of Tripoli. Despite some ambiguities in the wording of the mandate, NATO succeeded in conducting air operations and protecting civilians and civilian populated areas under attack or threat of attack.

The presence of mercenary activities raised some questions on the issue of direct participation in the hostilities. Civilians affiliated with the regime forces involved in attacking and threatening to attack the civilian population are directly participating in the hostilities and are liable to attack during the entire conflict, unless they become *hors de combat*. Although the issue of voluntary human shields did not arise during OUP, there were some discussions on the use of involuntary human shields by the regime, in which case they could not be attacked. Even assuming that the incidental damage in attacking the military objective they were shielding was not excessive in relation to the military advantage to be gained from the attack, it would have been illogical and contrary to the percieved end state (and mandate) to do so, since NATO's mission was the protection of civilians. The main focus of the operation was to prevent the attacks and the threat of attacks on civilians.

OUP has undoubtedly been the most intense NATO air campaign since Operation Allied Force during the Kosovo conflict in 1999. It has proved that air assets are critical parts of every modern operation and can contribute to the success of a military campaign. In all phases of OUP, constant care was taken to comply strictly with the Security Council mandate and the imperatives of the law of armed conflict. When requirements changed and pro-Qaddafi forces shifted their tactics from regular to irregular warfare, NATO-led forces proved to be capable of responding rapidly and adequately to these changing circumstances. The use of precision guided weapons, coupled with hi-tech intelligence, surveillance, and reconaissance (ISR) assets, was crucial to the fulfillment of the mission. Using precision laser-guided and satellite-guided munitions made every strike count. With a minimum of collateral damage, the air strikes enabled NATO to enforce the mandate. Operation Unified Protector offered convincing proof that airpower is flexible enough to take the lead in many different types of conflict. In targeting enemy forces, NATO forces strictly adhered to their obligations under the law of armed conflict. Targets were

positively identified prior to prosecution, and all feasible precautions were taken in order to minimize the damage to civilian property and the civilian population.

Notes

1 The title of this section is based on H. Summers, "A War is a War is a War is a War," in L. B. Thompson, *Low Intensity Conflicts: The Pattern of Warfare in the Modern World* (Lexington: Lexington Books, 1989).
2 UNSCR 1386 (2001) and subsequent UNSC resolutions.
3 Associated forces include mercenaries.
4 UNSCR 1970 and 1973 (2012)
5 The rules of engagement are basically the translation of strategic objectives from a military and political level into the operational and the tactical level.
6 Better known as the "strategic corporal" dilemma.
7 UNSCR 1973 did not prohibit the deployment of ground forces. The only restriction contained in the resolution pertained to the interdiction of occupying in part or in total the territory of Libya.
8 Article 2 GC.

Multi-Layered Defense and Initiated Attack in Defending the Homeland

Uzi Eilam

Introduction

The end of the twentieth century witnessed a dramatic transformation of the battlefield, and classical warfare between armies and states became relatively rare. Warfare on the modern battlefield is usually asymmetrical, fought between a state and a non-state enemy, or between two non-state entities. Armed groups target civilians in order to change a state's modus operandi and policies. This type of warfare is commonly known as terrorism.[1] The shock of the 9/11 attacks in the United States, and subsequent attacks in Europe, Iraq, and many other places around the world have thrust the world into a new reality. The threat of explosive devices and suicide attacks has been joined by the threat of rockets and missiles and the threat of cyberspace warfare. This new reality demands an improved response to the complex and dynamic threats of terrorism, specifically, a comprehensive approach and the investment of significant resources that can generate an effective response.

Over the years Israel experienced waves of attacks resulting in many casualties. Terrorism was on the rise elsewhere in the world as well, especially in Western Europe, but until recently did not reach the point where it was defined as a threat requiring special measures. France, which for many years thought it was immune to Islamic terrorism, learned the hard way that it too was a terrorism target. The attacks on March 19, 2012 in Toulouse, in which four Jews – a teacher and three schoolchildren – were killed and three French soldiers were murdered by one terrorist showed the French that the threat, in all of its severity, is present there as well. Unlike

Brig. Gen. (ret.) Uzi Eilam is a senior research fellow at INSS.

other European countries, the United Kingdom, which for many years was the target of Irish Republican terrorism, developed its own methods for domestic use to confront the threat. On the other side of the Iron Curtain, Russia failed in its war in Afghanistan, which it invaded in late 1979. The blood-soaked campaign against guerilla fighters who adopted terrorism as a successful method ended with Russia's humiliating withdrawal from Afghanistan. The 9/11 attacks were based on the creative notion of training terrorist pilots. The hijackings of the planes were accomplished without the use of firearms, and the hijackers, who boarded those planes in groups of five, aroused no suspicion.

Security services have long been aware that the various terrorist organizations help one another. The Irish underground, the Japanese Red Army, the German Bader-Meinhof gang, Fatah, and other Palestinian organizations found a common denominator and made use of the same training camps in Libya and Lebanon, and later also in Afghanistan.

In recent years, terrorists have also used the threat of nonconventional terrorism – atomic, biological, and chemical. The chemical threat was realized when canisters filled with the nerve gas sarin were used in the March 20, 1995 attack on the Tokyo underground.[2] The attack, carried out by the Aum Shinrikyo (literally "the unadulterated truth"), killed 12 and injured many. Nonconventional terrorism hangs like a sword of Damocles above the head of humanity.

At first, the fight against terrorism focused on tactical and ad hoc solutions. Israel built a defensive line through the Jordan Valley and put the Jordan Valley Brigade in charge. The response to the threat of Israeli airplanes being hijacked was the creation of a whole network of physical security on the planes themselves, including specially trained security personnel. Until the 9/11 attacks, the United States did not see the need for physical security and skilled security personnel on aircraft, methods adopted by Israel following the years of airplane hijackings.

If indeed the world is engaged in a global war on terrorism, what is the optimal way to defend against it? Should the response be focused on defensive aspects or should offensive ones augment defensive measures? Who are the enemies and where is the battle zone? This essay examines these questions from an historical perspective in order to draw conclusions and attempt to formulate some insights about the right strategy and most

effective tactics involving technology as a critical component in the response to this type of warfare.

The Terrorism Threat

An examination of the terrorism threat reveals a dizzying array of fields and methods. Some have been around for many years but have not yet been met with an appropriate response. The future is sure to bring threats that today are unimaginable. Here is a short survey of known threats:

a. *Aerial attacks*: Attacks on airplanes and attacks using airplanes offer a host of possibilities. The American aircraft that crashed into the Twin Towers in New York and the Pentagon in Washington on September 11, 2001 are extreme examples. As a lesson learned from those attacks, the United States now operates the Federal Air Marshal Service to secure passengers and airplanes. Firing shoulder-borne missiles at planes, as in the 2002 attempt to down an Arkia flight in Kenya, has not yet led to a decision to equip all passenger planes in the world – not even in Israel – with anti-missile defense systems. By contrast, passengers' shoes get special attention at many airports as the result of a foiled attempt to blow up a trans-Atlantic flight en route from Paris to Miami in December 2001 using explosives hidden in the soles of a terrorist's shoes. The world has not yet experienced damage to airplane systems via cyber attacks, but such a possibility is no longer in the realm of science fiction.

b. *Suicide attacks*: Suicide attacks by means of vehicles laden with explosives were seared into public consciousness beginning with Hizbollah's 1983 attacks in Beirut. Now, almost 30 years later, the same method of action is still used successfully in Iraq, Afghanistan, and elsewhere. In Israel, suicide attacks were the weapon of choice during the 1990s and early 2000s. Attacks on buses can be considered a special category of suicide attacks.

c. *Roadside bombs*: Roadside bombs are a familiar tool used by terrorist organizations. The wide range of bombs, locations, and methods of detonation (booby traps with sensors, manual detonation from afar, or electronic detonation from afar) make it difficult to develop a comprehensive response to this threat.

d. *Nonconventional terrorism*: For decades, the use of chemical and biological agents has been discussed as a possible terrorism threat;

the most prominent attack was Aum Shinrikyo's use of sarin on the Tokyo subway. The anthrax envelopes mailed in the United States in 2001, after the 9/11 attacks, brought the potential of the biological threat by terrorist groups to the fore. Because the investigation showed that the envelopes were mailed by a lone "bizarre" American scientist, the panic over chemical and biological attacks ebbed and preparedness for these sorts of attacks has dwindled.

e. *High trajectory weapons*: Rockets, artillery, and missiles are obvious means of terrorism and represent the firepower of terrorist organizations. The Russians began to sell their Katyusha rockets, developed during World War II, and Grad missiles, with a range of dozens of kilometers, all over the world.[3] The Qassam rocket, manufactured in local Hamas workshops, now has a range of more than 10 km. The Second Lebanon War showed Israel and the world at large the impact of high trajectory weapons used massively by a non-state entity against a civilian population. Iran and Syria have worked to restock Hizbollah's arms depots with an arsenal of rockets and missiles of all sorts and ranges, and this is currently one of the most important challenges facing Israel.
f. *Cyberspace terrorism*: Today most civilian activity is communications and computer based, from simple economic and social transactions, through emergency and medical services, to basic infrastructures of water, electricity, gas, and communications. Almost all activities are computerized and linked in one way or another to communications networks and the internet. The potential for damage in the realm of cyberspace, already colossal, is only growing as the technology develops further. Information security is currently an inseparable part of using the internet. Cyberspace terrorism capabilities are becoming more sophisticated all the time, and defending computer systems from harm has become a matter of exerting continuous, daily efforts.

Special attention must be paid to threats that could result in severe strategic damage, e.g., harm to infrastructure facilities, the paralysis of financial centers, the shutting down of energy installations and governmental centers, and damage to communications networks and databases. Such damage could be created through physical means, such as explosives, or by cyber attacks, liable to be much more dangerous and comprehensive. Interfering with transportation routes has significant economic implications, and to no small degree means the undermining

of world order. Terrorist activity can occur on the ground at the airport soon after takeoff using shoulder borne anti-aircraft missiles, or in the air, during the flight. The same is true of naval routes, the theater of most international trade; it too constitutes a strategic threat. Such activity, should it expand and succeed, is liable to entail paralysis of the global economy. The threat of high trajectory weapons – starting from ranges of several kilometers and ending with ranges of hundreds and even thousands of kilometers – is considered a strategic threat that will exist in the future. On the basis of Israel's experience, an almost certain outcome of the success of this threat is a significant paralysis of the economy and serious damage to the routines of all civilians in the nation under attack.

Learning the lessons after the shock of 9/11 while also considering the range of threats and challenges outlined above leads to the assessment that the threat is much greater than it was in the past and requires a systematic, comprehensive response.

The Response

In terms of the terrorism threat, the current situation may be likened to a global epidemic. Some would define the widespread reach of terrorism and the war on it as World War III. The French philosopher and sociologist Jean Baudrillard has even claimed that the war on terrorism is World War IV (Baudrillard considered the Cold War to be World War III).[4] Current methods of action to combat terrorism must confront the inherent asymmetry of the battle. The process of formulating the response must involve a sober, realistic analysis of the threats and identification of those that lack an adequate response. The response must consist of a combination of offensive and defensive components, based to a large degree on technological initiatives and capabilities. The decision by the United States and its allies to act in Afghanistan, America's targeted assassinations, and the ongoing effort that resulted in the elimination of Osama Bin Laden are evidence of the change that has occurred in thinking about the response. The use of offensive components requires the formulation of different tactics than those used in the past and reliance on technologies that will help confront various situations in the war on terrorism in the coming years.

Similarly, it is necessary to reexamine one of the IDF's fundamental premises – to move the war onto enemy territory – and consider whether

this principle remains relevant in this type of warfare. When speaking of a non-state organization operating out of defined territory, it is still possible to apply this principle, and examples in Israel are Operation Defensive Shield, the Second Lebanon War, and Operation Cast Lead. However, by contrast, fighting against decentralized terrorist organizations and cells is more complex. Moving the fight onto the court of an enemy using rockets and missiles requires different approaches when the threat is short range (dozens of kilometers) or when the threat is long range (hundreds of kilometers). We are already witnessing differences in the various components of the tactical response, e.g., the use of unmanned and armored combat vehicles against anti-tank missiles. Warfare against terrorism within the country's own borders is prosecuted primarily by means of focused intelligence. The use of bombs at roadsides and inside buildings, where forces are likely to operate, requires early identification of preparations to place these bombs in order to foil such attacks. It is crucial to attain relatively safe passage in the face of anti-tank and explosive device threats in enemy territory on the way to neutralizing the enemy's networks of artillery rockets and missiles. Contemporary urban warfare requires the identification of the enemy while maintaining the safety of troops moving through the urban landscape. Wars of the future will make extensive use of unmanned platforms to gather intelligence, operate ammunition, and identify enemy systems by drawing enemy fire at unmanned tools. An important component in these systems of warfare will be encrypted communications systems adapted to the new type of urban warfare, including use on the ground of effective systems to distinguish between friend and foe.

Technology for Defensive Systems

The need to supply a response requires the full use of technological capabilities. In this field, states usually have a relative advantage over terrorists and non-state entities. Some of the critical capabilities needed are:

a. *Means of discovery and sensing*: Sensors, especially those capable of identifying explosives at a distance, are an important need still awaiting a full response. At border crossings and airports in the United States advanced imaging technologies and X-rays systems operating on the backscatter method are already in use.[5] In addition, millimetric

wave imaging systems are also in use. These systems do not identify explosives but do identify suspicious objects carried by people. It seems that the use of trained dogs is a reliable method to discover certain types of explosives. Distance sensing of materials that power explosive devices is still awaiting a solution. An inseparable part of future sensor systems is to be found in cheap, reliable moving robots that would carry the sensors to wherever they are needed. Neutralizing explosive devices used by terrorist organizations leads to a search for alternatives to the chemicals used to put the explosive devices together. The challenge is to develop pesticides, insecticides, and herbicides based on chemicals that would be useless in constructing explosives.

b. *Identification and incrimination*: In recent years the use of biometric identification has expanded. The traditional opposition to the use of the range of biometric measures, such as fingerprints, retinal scans, and facial recognition, has to a large extent receded. The United States has changed its approach, followed by European nations and other countries around the world, all of which have decided that it is impossible to avoid conceding some personal rights for the sake of general safety.[6] This decision could lead to the establishment of biometric databases, which in the future could allow quick, reliable identification of terrorist suspects. A combination of technological developments based on understanding of human behavior in defensive systems could constitute a new component in the war on terrorism. An example of a system designed to identify malicious intent is the FAST project developed by the US Department of Homeland Security.[7] The system resembles a polygraph. A high intensity laser sensor reads people's rate of breathing and pulse, while another sensor identifies the shifting of body weight – the litmus test for behavior with malicious intent. Today, the warnings received by this system are not yet reliable and the errors are liable to result in false positives or the failure to pick up on real threats. Further means of development are needed for these systems before they can be declared operational.

c. *Cyber defense*: The development of countermeasures to cyber attacks must be founded on the assumption that this type of warfare knows no geographical boundaries. In such warfare, terrorist organizations exploit the freedoms of the democratic world and global communications. This war is characterized above all by the asymmetry in the ability of very

few to cause massive damage to central national systems. Preparing for defense against this threat requires ongoing tracking and unceasing efforts to develop countermeasures needed to defend against a threat that is constantly evolving.[8]

d. *Intelligence gathering*: Improving intelligence about the organizations, teams, and isolated individuals engaged in terrorism is a huge challenge. This challenge has many aspects, and in order to make progress, far reaching technological efforts are needed. A wide array of intelligence means are required, as are technological developments (eavesdropping, surveillance, decryption in real time) that will allow a leap in terms of future intelligence capabilities. It is necessary to increase the synergy between the intelligence and security institutions operating within and between nations. The Israeli attempt to combine the efforts of the General Security Service, the IDF, the Israel Police, and the Border Police in the war against terrorism is a good example of such synergy.

e. *Defense against high trajectory weapons*: The response to the high trajectory threat requires the construction of defensive systems with high rates of success of interception. Defensive systems in Israel – those already existing and those under development – clearly demonstrate the levels approach. The response to short range threats is now embodied by the Iron Dome system. For mid-range threats, there are the Arrow 1 missile, which has been operational for several years, and the Arrow 2 system, whose development is almost complete. In addition, the David's Sling system (also known as Magic Wand) is now under development. The Arrow 3 is being developed to confront long range missile threats, and will become operational once the necessary budgets are allocated and it demonstrates effectiveness in testing. In a limited area in Iraq, the American army used Vulcan Phalanx cannons to defend against high trajectory weapons.[9] Israel investigated the possibly and decided against the system. Simple calculations concluded that the Phalanx provides a response that requires the use of a very large number of cannons. In addition, the budgets for cannon purchases and, even more so, the allocation of manpower needed to operate them indicated their negative cost-benefit ratio. Nonetheless, it may have been worthwhile, especially in terms of the public and political aspects of defending the home front, to purchase several such systems and place them in certain locations, such as Sderot. This would also have afforded an opportunity

to test in practice both the solution itself and the justification for rejecting it from a public perspective.

f. *Laser interceptors*: A second field in defending against high trajectory weapons is the use of the powerful laser system, Nautilus, whose development encountered several crises. The development of the chemical laser based system was interrupted when the American army decided to withdraw from the project. A fierce and bitter argument erupted because there was no response to the short range high trajectory weapons threat and the growing public pressure exerted by the residents of Sderot and the settlement adjacent to the Gaza Strip. A sober analysis of the situation demonstrates that at present there is no archetype of a chemical laser system operating on the Nautilus principle in the United States. Because of the system's limitations, its effective range is at most 10 kilometers. Furthermore, its inability to function in rain and fog makes it an unreliable defense. The system's rate of fire is not at the speed of light, because the laser beam has to rest for several seconds on the rocket head before exploding it. The budgets required for these systems are much larger than the data published in the press.[10] Nonetheless, it would be right to accelerate the development of anti-missile laser systems, solid-state laser technology, that would be safer, more reliable, and perhaps even significantly cheaper.

The important challenges facing defensive weapon systems are their cost and improved interception rates for each of the levels. Laser weapons must find their proper place within the short range defensive systems while using safe laser technologies and finding a solution for a compact, inexpensive system. The response to the high trajectory weapons threat by means of ground attack also requires tactical solutions, in part new ones, and technological solutions. These must give the operational forces the ability to destroy missiles effectively in the launching areas while providing survivability and defense to forces moving towards the target.

Defense in Layers

The principle of levels of defense can be adopted and implemented in many areas of the war on terrorism. Layers of defense against the rocket and missile threat provide a response to different threats and supply backup for the defensive levels next to them. Defending against suicide bombers will improve as the result of adding measures and actions preventing the

first stages of preparing an attack. These are the distant levels in terms of time and distance from the attack itself.

One can generate levels of defense against arenas of explosive devices and booby-trapped buildings. The technological goal of sensing explosives from a distance could serve as a basis for adding an important layer in confronting the threat. The layers would consist of a combination of tactical preparation with technological support and sensors and the use of existing and still to be developed robotic tools.

Defending against weapons used at border crossings and air routes is a classic example of layers. Even now, a range of sensors, comprehensive defensive systems, and innovative technological means that have reached operational status are used at border crossings. Layers in systems of biometric scans allow backup for instances in which there are no values in databases using methods of identification currently in use (fingerprints, retinal scans, and facial recognition). Additional layers are supposed to identify changes in breathing, pulse rate and voice, body motions, eye movements and changes in body heat, the rate of speech and intonation. The higher the number of layers available to the defending side, the better the chances of picking out those suspected of terrorist activity. Developing layers of systems and backup and redundant measures would also benefit defense against cyber terrorism. Defense would start with internet providers and continue through the computers themselves and the internal networks of the defending organizations.

The principle of layers does not in and of itself represent a magic solution to the war on terrorism. Examining every threat listed above together with searching for an additional layer of defense or attack will eventually lead to the construction of a system that provides a better – if not hermetic – response to the threats of terrorism.

Conclusion

Today, homeland security is a vastly different battlefield than the theater of the World Wars, Korea, Vietnam, and the Yom Kippur War in Israel. The lessons of the war against terrorism bespeak the need to adopt an approach of constructing layers of defense in every realm. One cannot of course remain only with smart defense systems, no matter how effective. In order not to leave the initiative in the hands of the terrorists, it is necessary to improve the offensive capabilities.

Will the repeated stings of targeted assassinations of senior terrorists decide this war? Apparently not. On the other hand, a nation's capabilities to hold onto the territory of another nation and continue fighting manpower and resource-intensive wars on terrorist cells are also limited. It is not necessary to stay in enemy territory for long. The lesson learned from the IDF's 18-year stay in Lebanon after 1982 and the lessons learned by the American army after its wars in Iraq and Afghanistan show that the use of surprising tactics and innovative technologies help in a war everyone understands is an ongoing one. The secret of containing threats lies in the ability to continue acting in the war while maintaining a bearable ratio of losses.

Thus, what is needed is an approach that allows significant foiling of terrorist activity at a cost that will not entail an unbearable budgetary burden. Such an approach would rely on old and new technologies that allow missions to be accomplished at a tolerable casualty cost. This approach, in which every action is of short duration, would prevent most of the risks of going about one's routine while staying for an extended time in occupied areas. At the same time, multi-layered defenses would be given to civilians against the range of threats inherent in the war on terrorism. This defense must allow life in the civilian sector to carry on without too much disruption. This will allow the active operating forces sufficient time – within the limits of the always-ticking political clock – to undertake their missions properly.

Notes

1 It is difficult to come up with a universally accepted definition of terrorism. Among the dozens of alternatives is the Security Council's 2004 definition: "criminal acts, including against civilians, committed with the intent to cause death or serious bodily injury, or taking of hostages, with the purpose to provoke a state of terror in the general public or in a group of persons or particular persons, intimidate a population or compel a government or an international organization to do or to abstain from doing any act," United Nations Security Council Resolution 1566, October 2004.

2 K. B. Olsen, "Aum Shinrikyo: Once and Future Threat?" *Emerging Infectious Disease Journal* 5, no. 4 (1999).

3 Zvi Magen, Yiftah Shapir, and Olena Bagano-Moldavski, "Russian Arms Exports to the Middle East," *Strategic Assessment* 13, no 2 (2010): 83-95.

4 Jean Baudrillard, "The Spirit of Terrorism," *Le Monde*, November 2, 2001.

5 J. Sarah Caygill, Frank Davis, and Seamus P. J. Higson, "Current Trends in Explosive Detection Techniques," *Talanta* 88, January 15, 2012, pp. 14-29.

6 Jeffery A. Larsen and Tacha L. Pravecek, *Comparative U.S.-Israeli Homeland Security*, The Counter Proliferation Papers, Future Warfare Series, No. 34, USAF Counter Proliferation Center 46-47, pp. 25-35, and http://cpc.au.af.mil/PDF/monograph/comparativeusisraeli.pdf, and also *Inquiry into the EU-US Passenger Name Record Agreement*, CEPS Policy Brief, No. 125, March 2007.

7 Samantha Michaels, "Department of Homeland Security Develops New Technology to Detect Terrorist Intent," March 11, 2010, http://nationalsecurityzone.org/site/department-of-homeland-security-develops-new-technology-to-detect-terrorist-intent.

8 "DoD Cyberstrategy Unveiled; Critical Attack Revealed," *National Defense Magazine*, July 14, 2011 , http://www.nationaldefensemagazine.org/blog/Lists/Posts/Post.aspx?ID=467.

9 "Air Defense: Phalanx Marches through Afghanistan," *Strategy Page*, March 2012, www.strategypage.com/htmw/htada/20120313.aspx.

10 Shmuel Mittelman, "Petition to the High Court of Justice: Iron Dome Selected with Whitewashing and Debacles," *Maariv*, July 14, 2010; and Oded Amichai, "Opinion," July 21, 2010.

What Lies behind Chinese Cyber Warfare

Gabi Siboni and Y. R.

兵之形，避實而擊虛
"Avoid strength, attack weakness."
Sun Tzu, *The Art of Warfare*

Introduction

Over the past several years China has been developing operational capabilities in the field of cyberspace warfare. A cyber attack may be defined as the unauthorized penetration of computer and communications systems belonging to individuals or organizations for the purpose of espionage and information theft, in order thereby to damage or disrupt the functioning of these systems or to damage other systems dependent on them, even to a point of causing actual physical damage. Despite denials by the Chinese government, researchers posit that China is behind a string of cyber attacks[1] against the United States,[2] Japan,[3] France,[4] Australia,[5] and other Western nations.[6]

Chinese activity in the field of cyberspace warfare is intensive and aggressive. It appears that China, focusing on extensive collection of intelligence and commercial information in various fields, is targeting a range of companies – from those with specific technological expertise to organizations with financial and economic knowledge, such as in the cyber attack on the International Monetary Fund in late 2011.[7] However, the fact that companies and organizations providing essential services and communications infrastructures have also been attacked suggests that

Dr. Gabi Siboni is a senior research associate and head of the Military and Strategic Affairs Program and Cyber Warfare Program at INSS. Y. R. is a senior figure at the Prime Minister's Office.

there many be other motives in play. If so, what underlies these attacks, and is it possible to identify the strategic principle with which China operates in the West in general and the United States in particular? To this end, one must examine China's cyber warfare strategy, the Chinese organizations involved in recent years, and the resources invested to realize China's goals through this type of warfare.

It is commonly assumed that before 2009, most of the attacks attributed to China were directed against the American military and the administration, such as Operation Titan Rain against American government agencies[8] and Operation Ghost Net against diplomatic targets in the UN. By contrast, in recent years the attacks attributed to China have been directed against civilian targets, including national infrastructures of critical importance, companies forming a part of the chain of access to those targets, and companies that if attacked, generate an outcome that serves an economic or commercial need.

In recent years there has also been a quantitative leap in attacks against infrastructures. The first was the Shady RAT series of attacks from mid-2006 until February 2011.[9] The second series was Operation Aurora, an especially sophisticated series targeting Google, a critical infrastructure at the global level. These started in mid-2009 and lasted until the end of that year. The third, which received a great deal of media attention, was against RSA, a company specializing in information security and internet servers providing secure ID and one-time password services.

This essay argues that an analysis of the publicly available information about the more recent attacks makes it possible to establish that China does in fact stand behind these attacks and also makes it possible to identify the link between China's cyberspace warfare strategy and its choice of targets. The analysis includes an examination of the companies attacked to identify possible motives for the attacks. For example, attacking companies and organizations supplying technology allows access to general cutting-edge technology, military technology, and so on. The motives for these attacks are presumably to steal capabilities and conduct industrial espionage against nations and commercial competitors. Attacking companies and organizations in the financial and even political sectors allows access to valuable intelligence in these fields. By contrast, the intelligence value for immediate use in attacking companies providing critical infrastructures and communications services is usually relatively low. Rather, gaining

access, if only to some providers of communications and internet services in the West and the United States, is liable to give attackers the ability to damage these services.

China's Cyberspace Warfare Strategy

China's strategy of cyberspace warfare was formulated in the previous decade as part of a profound modernization process undertaken by the Chinese military. Based on the awareness that when it comes to kinetic warfare the Chinese armed forces are structurally inferior to the armed forces of the West, such as the United States military, the strategy reflects the understanding that in order to confront an enemy with technological superiority in the area of information flow, it is necessary to disrupt the enemy's access to this information. The approach involves dealing an opening blow comprising a cyber attack, an electronic attack, and a kinetic attack on the enemy's information web and military technology centers. Such a blow will lead to the creation of blind spots on the enemy's part, allowing Chinese forces to operate with greater efficiency.[10] The Chinese assumption is that by disrupting the flow of information it is possible to cause significant damage to the capabilities of a sophisticated enemy and gain an advantage in the early stages of a confrontation.

The strategy developed by China in the last decade sees integrated network operations[11] as a key platform for the field. The strategy is based on a combination of four types of operations:[12] attacks on computer networks; electronic warfare, including anti-electronic and anti-radar measures; computer network protection; and computer network exploitation.[13] One of the key components in the Chinese strategy is controlling the enemy's flow of information, on the operating assumption that China's enemies (especially Western nations, with an emphasis on the United States) are highly dependent on information flow-based technology. The assumption is that during a confrontation, the ability to damage the flow of information would allow China to attain an advantage in the physical battlefield. This integrated approach gives China interdisciplinary operational capabilities, allowing it to use force effectively to attack an enemy.

Selected publications have undertaken detailed analyses of the most important institutions in the Chinese military in terms of network operations.[14] This essay describes two of these central military bodies: the Third Bureau (in the General Staff of the People's Liberation Army),

responsible for SIGINT, and the Fourth Bureau, responsible for ELINT and electronic warfare. The Third Bureau employs experts in many fields: technicians, computer experts, language experts, intelligence experts, and more. Indeed, several Western researchers have surmised that the manpower operating in the Third Bureau numbers over 130,000 personnel.[15] The vast scope of the bureau's activity and the range of missions with which it is charged make it eminently fit to carry out cyber operations on the web. This bureau has many "collection stations" throughout China; it is responsible for gathering intelligence from voice and related data, and fully processing and assessing it. The department is also apparently responsible for internal intelligence gathering in the Chinese military for the purpose of internal information security and protection. The Fourth Bureau, responsible for ELINT, i.e., electronic intelligence operations and electronic warfare, seems to operate also in the field of integrated network operations.[16] It appears that the Third Bureau is the body coordinating overall activity in this field.

In addition to the military organization, China also has a very large hacker community,[17] including hackers who have claimed responsibility for a number of cyber attacks and are apparently involved in operations driven by national goals. Although the Chinese government presumably takes steps to enforce Chinese law, which prohibits this type of activity, it often turns a blind eye to the phenomenon and even provides material support for some of it, in a type of outsourcing of government cyber activity.[18] In addition, the Chinese army recruits civilians – from the hacker community and hi-tech industry – to its web militia units.[19] The web militia is integrated with the regular military, though its members are unpaid volunteers.

In contrast to the common perception of Chinese cyber activities, some researchers claim that these activities are designed first and foremost for internal needs, and that Western nations need not be overly concerned about the threat to their cyberspace. In this view, the Chinese have developed capabilities primarily to monitor opponents to the regime and control information available to Chinese citizens, essentially for political needs largely directed at preserving the regime.[20] However, while totalitarian regimes, including China, indeed use cyberspace capabilities for internal political ends,[21] this is only part of the picture, as evidenced by the series of cyberspace incidents emanating from China in recent years.

One of the main components of China's cyberspace strategy is the critical need for access to enemy communications infrastructures; without this access it is difficult to plant powerful blind spots. Attaining effective access to communications networks requires extensive and long term work on infrastructures. An attack on enemy communications networks is possible only if there is regular access to them over time, providing attackers with high quality intelligence that allows them secretly to install malware for use when the time comes. Such access requires long term maintenance and preservation because of the constant changes enemies make in their communications and information set-ups, and because they continually install new defensive systems designed to uncover malicious activity.

China's Cyber Attacks

The last six years have seen more than a few cyberspace attacks attributed to China, which apparently were intelligence gathering operations. An analysis of these attacks affords a means to identify China's basic attack techniques and infer its policy and methods. The attacks portray a world power intent not on focusing on a specific target, rather on gaining wide infrastructure access. In the case of Operation Aurora, the goal was to gain access to Google's password mechanism and the versions control software. In the RSA attack, the goal was to gain access to the internal network in which all information relating to secure ID was managed; such access could in the future be used to mount a more effective attack on other companies using the system, including security companies and companies engaged in sensitive activity.

The techniques identified in the well organized attacks were highly similar, using social engineering,[22] exploiting software weaknesses, and inserting delay mechanisms to expand intra-organizational access and extract information. The fact that China has taken these measures in a consistent, systematic manner over the past several years strengthens the assertion that the attacks were designed deliberately and that the same organizations were responsible, and weakens the claim that the attacks were the work of random hackers. Further substantiation may be found in the analysis made by the Northrop Grumman Corporation,[23] which noted several criteria:

a. *Similarity in keyboard behavior*. Similar behavioral characteristics or patterns in the attackers' methods in the various attacks were identified, e.g., attacking similar information parts and using similar tools.
b. *Scope of preliminary preparations*. The attacks comprised actions requiring preparation and prior knowledge, stemming apparently from preliminary action taken over several months before the actual attack. For example, familiarity with the architecture of the attacked networks was clearly evident.
c. *Attacker discipline*. The attackers were highly disciplined, e.g., they did not open files to scan the contents initially before copying them, indicative of the probability that they were operating on the basis of prior information.

Operation Nitro

Operation Nitro involved a series of attacks that occurred primarily from late July 2009 until mid-September 2009, when Symantec published information about it.[24] Its main purpose, likely technological espionage, was carried out in several consecutive waves, distinguishable by their targets. At first, human rights organizations in China were attacked, followed by motor industries; in the final stage, 29 chemical companies were targeted. The targeted companies were Fortune 100 companies working in chemical R&D and special materials for application in military vehicles and companies involved in the construction of infrastructures for chemical industries and the manufacturing of advanced materials. The attack method was similar to the method used in other attacks launched by the Chinese and included the following components:

a. Malicious code usually disguised as a security update. A great deal of non-personalized email was sent to organizations, unlike other operations in which great efforts were made to direct the email to individual email addresses.
b. Insertion of a back door (Trojan horse) into the targeted computers.
c. Increased access to the networks attacked while using remnants of passwords found on the attacked computers in order to gain control of central network computers.
d. Collection of material on interim servers and dispatch of this material outside the network.

In all, some 100 computers were attacked, 29 in the chemicals field and 19 belonging to the security sector. Most of the companies attacked were in the United States (about 30 percent), Bangladesh (about 20 percent), and the United Kingdom (15 percent), with the remaining located in some 20 different states around the world.

Operation Aurora

Operation Aurora included a series of attacks beginning in mid 2009 and continuing until December of that year. In January 2010, Google was the first to report it. The company announced that the attackers had hacked into Gmail accounts belonging to Chinese dissidents active in the United States, Europe, and China.[25] Adobe also reported attacks in the same operation, which targeted at least 34 organizations and companies.[26] McAfee, the information security company, analyzed the attacks. The findings indicated that the purpose of the attacks was to gain access to source codes of the attacked companies, especially the version management software Periscope used by hundreds of large software companies. McAfee discerned several stages in the attack:[27]

a. The operators of the attacked computer would receive a harmless-looking email or notification from what appeared to be a safe source.
b. The operator would take the bait and click on the link attached to the notification leading to a server containing malware.
c. The web browser in the attacked computer would download a binary code camouflaged inside a picture file and operate a back door that would connect to a control server located in Taiwan.
d. As a result, the attackers would gain full control of the computer and thus also to sensitive information communicated through the network.

This method was widely used in many of the attacks known as APTs (advanced persistent threats). At first, the term indicated sophisticated attacks on military and government networks, but currently the term is used to mean attacks of high intensity (i.e., state-level intensity) on a civilian target.

The Night Dragon and Shady RAT Attacks

These waves of attacks started in mid 2006 and continued until February 2011. McAfee, which gained access to one control server used by the attackers, identified the server after a log file analysis[28] and determined

that some 70 targets had been attacked.[29] Given that McAfee gained access to only one control server, the attack presumably targeted many others as well. The analysis mapped the companies attacked and the time frames that the computers were controlled by a server through which the attackers extracted sensitive information. The targets included: 21 government organizations, 6 industrial and energy companies, 13 communication, computer, and electronics companies, 13 security companies, and 6 financial companies. In this context, the attacks on the Norwegian oil and gas companies are particularly noteworthy.[30] Attacks on companies considered national infrastructures, such as energy companies, could be evidence of the desire to create access for the purpose of damaging them at some point in the future.

RSA Attack

The RSA attack provides the basis for an in-depth analysis because one of the servers involved was a botnet[31] of some 2,000 computers. Penetrating the botnet's central server made it possible to analyze the list of infected computers; the analysis generated a list of 763 companies.[32] The attack was first reported by RSA in March 2011.[33] The stages of the attack, typical of other attacks as well, can be charted as follows:

Extensive infrastructure intelligence gathering ➜	Constructing the profile of the attacked computer's owner ➜	Sending email to attacked computer's owner ➜
Installing a back door in the computer ➜	Gathering initial information and expanding the attack ➜	Extensive information gathering

The first stage involves extensive gathering of infrastructure intelligence about the organization targeted. This intelligence is usually gathered from social networks and other open sources. The purpose of the information is to identify potential individual targets, as they will serve as the optimal channels to work within the attacked organization. For example, in the RSA attack, two small groups of employees were selected. They were not necessarily the final targets of the attack but were apparently selected because the attackers felt it would be convenient to start the attack with them.

The next stage involves constructing the profile of the attacked computers' owners: after identifying the penetration points, a profile of those to be attacked is constructed. This requires constructing a full enough picture that allows for the creation of an ostensibly harmless email that would not arouse any suspicion on the target's part. Such information gathering and the construction of a suitable profile require widespread, focused information gathering based on good organizational skills and resources (and especially English language skills).

This is followed by sending malicious email especially adapted to the attacked computer's owner (ZeroDate spear phishing email), which requires two steps. The first entails constructing a formula, structure, and look of a harmless message that would not immediately be erased by the user and would in fact prompt the user to open its links. Email is sent to specific groups of selected employees. At times the message is adapted to every individual user according to the profile constructed. The second action is including an attachment to the email with a security weakness and back door. Weaknesses are software security breaches through which attackers can insert their malicious code. At times the weakness is original, identified in the attacker's weakness identification process (apparently the case with Aurora); at other times, the weakness is well known (ZeroDate) and the attacker relies on the possibility that the targeted computer has not yet installed the patches to fix the weakness.[34] For example, in the RSA attack, the subject line of the email was "Recruitment Plan 2011" and had an Excel document attached, "Recruitment Plan 2011.xls." The ZeroDate weakness was CVE-0609-2011 in Adobe Flash. The moment one of the employees opened the file, the computer was infected via a back door. During the attack the weakness was considered unknown and there was no security update. The update was distributed about a week after the attack.

Installing a back door in the computer: Malicious code is inserted into the infected computer, which allows attackers to control it via a control server.[35] Usually back doors link the attacked computer to the attacker's server, and from there the computer is operated according to instructions from that server based on the commands of the human operators, usually working in shifts. This direction of communication – from within to outside the organization – makes it very difficult to identify the communication.

At this point the attackers gather initial information. Every attacked computer is matched with an attacker group analyzing the computer's

contents and trying to assess how to gather information from the attacked computer and what information to gather. At this stage there is usually an assessment of the attacked computer's access to servers and other sources of information within the organization in order to identify the network map and learn how to expand the attack.

The central information gathering stage takes place after access to the company's servers has been gained and the desired information identified. The transfer of large amounts of information in a way that does not arouse suspicion and does not allow identification by monitoring software usually installed by large organizations is highly complex. It is generally done by means of another computer in the network whose access and permissions levels are high enough so that it upgrades the permissions of the servers to export information while using information-compressing encryption and algorithms. For example, in the case of RSA, the attackers finally arrived at a computer that stored sensitive information about the secure ID system, which later allowed the attackers access to information at other companies,[36] all of this bypassing the monitoring systems' warnings about illegal actions.[37]

The approach described herein requires the allocation of many professional resources. It seems that two groups working in tandem with different tools participated in this attack. The first identified the targeted information in the company's network, while the second worked separately to manufacture the channel for extracting the information. A third group, designated to preserve access for later use in the future, may also have been involved. Such an approach reflects the thinking of a world power working with a very high degree of professionalism while investing heavily in resources, such as highly skilled manpower and intelligence capabilities. Indeed, in this attack it is possible to discern some elements suggesting that a world power – presumably China – was behind it. These elements include:

a. *Infrastructure access*: Breaking into a company's one-time password mechanism (OTP) in order to gain access to other companies indicates a desire for extensive action requiring major resources.
b. *Scope of attack*: Open publications reported 763 infected computers found on one of the servers involved in the RSA attack. At least some of the targets required preliminary manual action, i.e., it was necessary to gather preliminary data about the target, construct emails in English

that served as bait, and conduct a preliminary analysis of accessibility. An attack of such intensity would have required the organization of infrastructures at the level of a world power, indicating that this was not the work of individual hackers.

c. *The Sykipot back door program*:[38] This program, a variant of PoisonIvy, served Chinese attacks since 2006 (in similar versions) and through early 2012.[39] The use of similar software (with relatively few changes) indicates organizational coordination among the various attackers over the last several years.
d. *Identifying marks*: The back door programs had strong links to China. According to an analysis of the software text, there were clear markers for the Chinese language, including remnants of information in Chinese in binary code (debug information). In addition, error messages in Chinese were identified. Finally, the only user's guide for the back door is in Chinese.
e. *The control servers*: An analysis of the sites where the control servers were placed and from where the attacked computers were controlled showed that most of them were located in China (299 of the 329 control servers).[40]

These findings strengthen the hypothesis that China is behind attacks requiring an extensive, systematic organizational and infrastructure system. Given this, one should not be surprised by the announcement made by General Keith Alexander, the Director of the NSA, which confirmed that China was behind the RSA attack.[41]

The list of 763 companied appearing on one of the servers involved in the RSA attack was analyzed. The analysis included identifying the companies through the internet and characterizing their activities according to three categories: technology companies apparently attacked for the purpose of technological espionage; financial and economic companies that would yield commercial information; and communications providers. These findings usually mean that the infected computer was linked to a public internet service provider (ISP). The analysis showed that close to 80 percent of the companies and organizations attacked were communications providers, while the other 20 percent were split between technological, financial, and other companies. The data indicates a typical botnet breakdown, which includes a very large number of infected computers belonging to private individuals who connected to the internet using an

ISP. The rest of the attacked computers were distributed among some 90 countries, including five in Israel.

Concluding Insights

The series of attacks since 2006 indicate a transition to attacking critical infrastructures, both in the communications and energy fields. Regarding the RSA attack, it is possible that the list of companies on the server included a random botnet list compiled by the Chinese in a lengthy process before the attack was discovered in order to serve as an infrastructure for future attacks. It is possible to send attack email from every infected computer, transfer files, and hide the attacker's identity. However, it is also possible that some of the list is not random and includes companies that are explicitly targeted for attack.

The findings about the attacks in recent years strengthen the research hypothesis that the attacks described are part of a systematic, orderly campaign underway by China. China's cyberspace warfare strategy suits the choice of some of the attack targets, most of all those connected to critical infrastructures. The attack against Google in Aurora, the Shady RAT attacks, and especially the RSA attacks all signal a transition to a systemic approach that targets communications and critical infrastructures. China's strategy, designed to damage the enemy's weaker and lesser-protected realms in a move prior to using kinetic force, requires extensive activity to create long term access to critical infrastructures, including communications. Unlike normally noisy information gathering operations discovered from time to time, it is more difficult to discover operations aimed at infrastructures and gaining access to them for use at some time in the future. It is quite possible that they will never be discovered.

In addition to the attacks discussed above, in April 2011 China was accused of intercepting no less than 15 percent of all internet traffic.[42] Therefore, this activity is likely part of attacks designed to create intelligence access to internet traffic and intercept transmissions before they are encrypted. Moreover, the conclusions of this essay are based on knowledge accrued as the result of analysis of information about attacks that were discovered and publicized. Because some attacks are not discovered and others are discovered but not publicized, one may assume that China is running other cyberspace operations. It is hard to know what exactly is taking place at the companies under attack. One

possibility is that they have been fitted with back doors different from the ones used to preserve access and that this back door will be put into action at the attackers' discretion in order to damage the relevant communications infrastructure. Moreover, a sleeper back door is virtually undetectable by existing defensive technologies such as various anti-virus programs.[43]

This is particularly serious with regard to the United States, where there tends not to be a physical separation of communications networks. In other words, the so-called civilian internet[44] is also frequently used in the computer systems of sensitive installations and organizations, and even critical national infrastructures such as electricity producing nuclear reactors and transportation infrastructure control systems. Furthermore, in some cases the United States security systems make extensive use of civilian internet infrastructures, and the separation of networks of sensitive operational systems is not sufficiently developed. This is an essential security weakness allowing attackers a great deal of access to these infrastructures by means of attacking less protected civilian systems. This means the creation of the ability to severely disrupt information transmission at some unspecified future date. Because of this weakness, preliminary damage to communications and telephony infrastructures during a confrontation is liable to disrupt operational and security systems based on these infrastructures.

The response to this weakness requires adopting a comprehensive systemic approach. Attempts to improve the defenses of communications infrastructure providers are insufficient to prevent future attacks. The use of the internet for communications of sensitive systems cannot be based solely on access permissions. No matter how protected, these permissions represent a severe security breach. One of the important components of a response to the weakness described herein lies in differentiated communications networks. It seems advisable to isolate operational networks of the whole gamut of critical systems, such as security systems, operational communications systems, and command and control systems of installations identified as critical national infrastructures. The ability to operate control systems of critical installations through the internet is liable to prove to be a serious problem the moment a sophisticated attacker decides to use back doors at some future point.

Notes

1 Steve DeWeese, *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation*, Northrop Grumman, October 9, 2009, p. 67.

2 Kenneth Lieberthal and Peter W. Singer, *Cybersecurity and U.S.-China Relations*, The Brookings Institution, February 2012.

3 On the attack on Mitsubishi Ltd. in Japan in August 2011, see Hiroko Tabuchi, "U.S. Expresses Concern about New Cyberattacks in Japan," *New York Times*, September 21, 2011, http://www.nytimes.com/2011/09/22/world/asia/us-expresses-concern-over-cyberattacks-in-japan.html?_r.

4 "Chinese Hacked French Ministry for G20 Data," *The Week*, March 8, 2011, http://www.theweek.co.uk/technology/7229/chinese-%E2%80%98hacked-french-ministry-g20-data%E2%80%99.

5 Erik Helin, "Fingers Point to China in Australian Prime Minister Hack," *Brick House Security,* March 30, 2011, http://blog.brickhousesecurity.com/2011/03/30/australia-pm-hack.

6 On the attack on Canadian government sites, see Greg Weston, "Hackers Attack Canadian Government," *CBS News,* February 16, 2011, http://www.cbc.ca/news/politics/story/2011/02/16/pol-weston-hacking.html.

7 John Markoff and David Sanger, "IMF Reports Cyberattack Led to 'Very Major Breach,'" *New York Times,* June 11, 2011, http://www.nytimes.com/2011/06/12/world/12imf.html.

8 Nathan Thornburgh, "Inside the Chinese Hack Attack," *Time US*, August 25, 2005, http://www.time.com/time/nation/article/0,8599,1098371,00.html.

9 Dimitri Alperovitch, "Revealed: Operation Shady RAT," Version 1.1, McAfee, 2011, http://blogs.mcafee.com/mcafee-labs/revealed-operation-shady-rat.

10 DeWeese, *Copability of the People's Republic of China to Conduct Cyber Warfare*, p. 69.

11 Integrated network electronic warfare.

12 Tim Stevens, "Breaching Protocol: The Threat of Cyberespionage," *Jane's Intelligence Review*, March 2010, pp. 8-13.

13 Timothy L. Thomas, "Chinese and American Network Centric Warfare," *Joint Forces Quarterly* 38, p. 77, http://www.dtic.mil/doctrine/jel/jfq_pubs/1538.pdf.

14 DeWeese, *Copability of the People's Republic of China to Conduct Cyber Warfare*, p.31; Mark A. Stoke, Janny Lin, and L. C. Russell Hsiao, *The Chinese PLA Signal Intelligence and Cyber Reconnaissance Infrastructure,* Project 2049 Institute, 11, 2011, pp. 6-14.

15 It is difficult to verify this assessment.

16 James Mulvenon, "PLA Computer Network Operations: Scenarios, Doctrine, Organizations, and Capability," in Roy Kamphausen, David Lai, and Andrew Scobell, eds., *Beyond the Strait: PLA Missions Other than Taiwan* (Washington, DC: National Bureau of Research, 2009), p. 273.

17 In Mandarin: Hikè 黑客, literally "black guest."
18 Stevens, "Breaching Protocol," pp. 8-13.
19 Timothy L. Thomas, "Comparing US, Russian and Chinese Information Operations Concepts," *Foreign Military Studies Office*, Fort Leavenworth, KS 66048, February 2004, pp. 12-13.
20 Thomas Rid, "Think Again: Cyberwar," *Foreign Policy*, March/April 2012, http://www.foreignpolicy.com/articles/2012/02/27/cyberwar?page0,6.
21 See publications on China's cyberspace espionage against the Tibetan government in exile and the break-in of the Dalai Lama's computer infrastructure; Stevens, "Breaching Protocol," pp. 8-13.
22 In the context of this essay, this term denotes the ability to deceive the owner of the computer under attack by creating a posture that fits the user's profile so that the computer will take action that interests the attacker, e.g., respond to email addressed to the owner in a way that is contrary to the security policy of the organization in which s/he works.
23 DeWeese, *Copability of the People's Republic of China to Conduct Cyber Warfare,* p. 60.
24 Eric Chien and Gavin O'Gorman, *The Nitro Attacks, Stealing Secrets from the Chemical Industry,* Symantec Security Respond, 2011, www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the_nitro_attacks.pdf.
25 It is possible that there was no connection between the hacking of the Gmail accounts of individuals and the attack designed to access the Google and Adobe source codes.
26 Ariana Eunjung Cha and Ellen Nakashima, "Google China Cyberattack Part of Vast Espionage Campaign, Experts Say," *Washington Post*, January 14, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/01/13/AR2010011300359.html.
27 McAfee Labs and McAfee Foundstone Professional Services, *Protecting Your Critical Assets, Lessons Learned from "Operation Aurora,"* http://www.mcafee.com/us/resources/white-papers/wp-protecting-critical-assets.pdf.
28 Log files are files that continuously and automatically document defined computer activity.
29 Alperovitch, "Revealed," p. 3.
30 "Hackers Attack Norway's Oil, Gas and Defence Businesses," *BBC News*, November 18, 2011, http://www.bbc.co.uk/news/technology15790082-.
31 A botnet is a collection of software agents installed on host computers. In many cases these are infected computers that contracted the software agent without the computer owner's knowledge. The software agents can be operated under previously defined conditions or by commands coming from a control server.
32 Brian Kerbs, "Who Else Was Hit by the RSA Attackers," October 2011, http://krebsonsecurity.com/2011/10/who-else-was-hit-by-the-rsa-attackers.

33 Uri Rivner, "Anatomy of an Attack," April 1, 2011, http://blogs.rsa.com/rivner/anatomy-of-an-attack.

34 ZeroDate weaknesses are software security breaches publicly identified and noted. Usually, as soon as the breach becomes known, the software developer provides a response in the form of a security patch distributed to the public. There is generally a gap between the time the patch is distributed and the time it is actually installed on users' computers. The window of opportunity for attackers starts when the weakness is announced and lasts until the patch is installed on the targeted computer. During this timeframe, attackers can insert malicious code through the breach.

35 Around November 2010, some of the computers of the companies under attack were already in communication with the attackers' control networks.

36 One of the companies attacked using information gathered in the RSA attack was Lockheed Martin. See Mathew J. Schwartz, "Lockheed Martin Suffers Massive Cyberattack," *Information Week*, May 31, 2011, http://www.informationweek.com/news/government/security229700151.

37 Large organizations usually have systems that monitor computer network traffic in order to identify behavior that is illegal according to predetermined rules. Such systems have different commonly used names, including SEIM (security event and information management) and NBA (network behavior analysis). These programs have a set of rules designed to alert administrators to non-permitted or unusual network behavior and also to prevent it from occurring.

38 Stephen Doherty et al., "The Sykipot Attacks," December 14, 2011, http://www.symantec.com/connect/blogs/sykipot-attacks.

39 Mathew J. Schwartz, "More Sykipot Malware Clues Point to China," *Information Week*, December 21, 2011, http://www.informationweek.com/news/security/attacks232300940/.

40 Kerbs, "Who Else Was Hit by the RSA Attackers."

41 Nicholas Hoover, "NSA Chief: China behind RSA Attacks," *Information Week*, March 27, 2012, http://www.informationweek.com/news/government/security232700341/.

42 Stew Magnuson, "Cyber Experts Have Proof that China hs Hijacked U.S.-Based Internet Traffic," *National Defense,* December 11, 2010, http://www.nationaldefensemagazine.org/blog/Lists/Posts/Post.aspx?ID249=.

43 Gunter Ollmann, *Serial Variant Evasion Tactics Techniques Used to Automatically Bypass Antivirus Technologies*, Damballa, 2009,http://www.damballa.com/downloads/r_pubs/WP_SerialVariantEvasionTactics.pdf.

44 The concept of "civilian internet" denotes internet communications networks used by the public at large and having no particular protection.

Applied Strategy: The Challenges of Applying Force in a Changing Middle East

Ron Tira

Israel's strategic environment of mid 2012 differs significantly from that of a few years ago.[1] In the current environment, the military force application that Israel is liable to need differs in purpose, constraints, and the accompanying military-political interface from the force application of the past. The purpose of this article is to discuss some of the particular characteristics of force application in this contemporary environment.

One of the main parameters requiring a change in thinking is that in the emerging multi-sided strategic system, using military force against a particular enemy can have important political and strategic consequences for relations with third parties – some enemies, some allies, and some with vacillating positions. Clearly this constraint existed in the past as well, but it has now become weightier. The number of relevant third parties is increasing; the ties between the actors are more complex and often less predictable; and the political and strategic effects on third parties can sometimes be more significant than the direct result of force application against the enemy.

For Israel, this is true of two current challenges. The first part of the article deals with the challenges of using force in the context of the most critical security issue today – the Iranian nuclear program. A possible attack against Iran is intended to have a significant effect on the policy of the relevant actors, not only on Iran's nuclear and physical capabilities. Thus the debate focusing exclusively on the length of time Iran will need to repair

Ron Tira, author of *The Nature of War: Conflicting Paradigms and Israeli Military Effectiveness*, is a businessman and a reservist in the Israeli Air Force's Campaign Planning Department.

the damage caused by an attack indicates a lack of understanding of the objective and strategic meaning of an attack.

To an extent, the purpose of an attack is, inter alia, to influence the policy of the US, an ally, and not merely the enemy's policy. This fact should be a consideration underlying the design of an operational plan. Thus, it is possible that the covert campaign by intelligence agencies against the nuclear program does more harm than good. Even if the covert campaign yields immediate benefit with regard to Iran's nuclear and physical capabilities, its effect in the political and strategic sphere is negative. The reasons for this will be discussed at length below.

The second part of the article deals with the challenges involving the application of force in Israel's other potential main theaters of confrontation, led by Gaza and Lebanon.

Internal instability in Egypt and Jordan and internal developments in Turkey cause these countries to vacillate in two ways. First, the emerging policies in Egypt and Turkey are equivocal: theses states may be either allies or potential challengers. Second, Israel's use of military force in theaters like Gaza and Lebanon is liable to have a negative impact on internal developments in Egypt and Jordan.

Indeed, a large scale military campaign in Gaza, Lebanon, or any other bordering theater area is liable to prove politically and strategically costly in Israel's relations with the vacillating countries. Stronger interdependencies and linkages between theaters mean that the price that Israel might pay in its relations with Egypt, Jordan, and Turkey is liable to outweigh any direct military gains against the enemy. And even if the decision makers in these Sunni states assess that they could benefit from an engagement between Israel and a Shiite entity such as Hizbollah, challenges might surface by the increasingly important factor of popular Sunni Arab sentiment following an attack against Lebanon and its government.

In recent decades, Israel's enemies have tried to restrict its freedom of action and military effectiveness in a variety of ways, including the use of sub-state organizations and intentional blurred distinctions between the civilian and military worlds as well as between war and lull. The next stage in restricting Israel's freedom of military action could result from exploitation by Israel's enemies of the vacillating states, whether in the diplomatic arena or through hostile operations from their territory or in the vicinity of their military assets.

Part I: The Iranian Nuclear Challenge

The Rationale for an Attack against Iran

The argument that an attack against Iran will be ineffective because it would cause only limited and reparable damage to Iran's nuclear program has surfaced again in recent months. This focus on the physical result of an attack omits its essential goal and its political nature. As Clausewitz said, the main importance of force application lies in its influence on policy, not just the specific physical damage that it inflicts.

The goal of Iran's policy is to obtain nuclear weapons. The goal of Israel's policy is to change Iran's policy. Iran is determined to obtain a nuclear capability, and any damage to its nuclear capability, whether limited or extensive, military or covert, will only delay the implementation of Iran's policy by the time required for reconstruction. It therefore follows that in order to carry out its policy, Israel must influence not only Iran's nuclear capabilities (which can be rebuilt), but mainly its policy. Damaging nuclear capabilities may buy limited time, but it is doubtful whether by itself it can change policy. Israel may find it more challenging to directly affect Iran's policy, but the US is capable of it.

Iran portrays itself as a regional and even a global power, but this portrayal masks profound structural, economic, and military weaknesses. One out of every seven Iranians is illiterate, its gross national product is roughly equal to that of Argentina, and at least some of its key weaponry dates back to the 1960s and 1970s. Iran suffered critical damage and sacrificed almost an entire generation in the eight-year war against Iraq and its army, an army that the US defeated within a few days. It can be assumed that in any direct confrontation between the Iranian military and an advanced Western military, the latter will prevail.

Why then is the US unsuccessful in forcing its political will on Iran? What works in Iran's favor is the asymmetry in the seriousness and determination in the respective Iranian and US attitudes toward the Iranian nuclear program. From Iran's perspective, the nuclear program is a supreme goal, and it is willing to incur major risks and pay high prices to achieve it – or at least it is posturing in such a way.[2] Indeed, Iran is succeeding in deterring its enemies and positioning itself as ready for any confrontation – even though its profound weakness presumably means

that it does not seek a direct military confrontation with the West, and would probably not withstand one.

The US does not appear as determined as Iran. It balances a large number of considerations, among them a rise in the price of oil and potential damage to its economy, the November 2012 elections, and the need for an international coalition. In addition, it is still traumatized by its wounds in Iraq and Afghanistan, and hesitates to take risks and pay the accompanying prices. Another factor working against the US is that in recent years, due to the way it dealt with a number of regional challenges (including Iraq, Bahrain, and Lebanon), it has been perceived as indecisive and inclined to recoil from strategic commitments.[3] If, however, circumstances prompt the US to attribute the same importance and urgency to the nuclear question as Iran does, it can be assumed that the world's only superpower would have the upper hand.

Iran wishes to gain time in order to advance its nuclear program. The US seeks to avoid or at least postpone high risk and potentially costly decisions, and it therefore continues to delay the moment of truth of its declared policy. At this stage, Israel is also deterred by the price that will be exacted from it by Iran's proxies and the international community if it acts alone against Iran's nuclear program. Consequently, for now, it too is not expediting the moment of truth. Furthermore, it is possible that some of the measures being employed by the US – a series of visits to Israel by senior officials, the meetings with Iran, sanctions, and movement of forces in the Persian Gulf – are designed not to influence Iran, but to persuade Israel to bide its time. A fundamental equilibrium point of the political-strategic system is thereby emerging, whereby all three parties allow time to pass.

The risk exists, however, that Iran and the US administration share additional strategic equilibrium points. The first point is a possible common interest of Iran and the US in creating a perception that the nuclearization threat is not immediate and the diplomatic dialogue has not yet been thoroughly explored, which lends them justification for allowing time to pass. The second potential common interest between Iran and the US is creating an impression that military action would be useless, allegedly due to both the redundancy of the nuclear program and Iran's expected response. The third and most important risk is that Iran and the US may develop a common interest in a quantum leap from the stage of "there is more time for diplomacy" to a stage of "it's too late for military action,"

without passing through a stage in which only military action may still change Iran's policy.

These points of equilibrium are unacceptable to Israel, which must expedite the emergence of a strategic moment of truth in which all parties put their ultimate cards on the table. A variable that might upset these equilibrium points would be Israel's immediate willingness to pay the prices and take the necessary risks for carrying out its policy. Such a new situation is designed to force a change in the risk-benefit analyses of the other two vertices of the triangle. In other words, the goal of a military strike by Israel will not be to cause any particular damage to Iran's nuclear assets, but to resist the existing strategic and political equilibrium points and generate a different political-strategic reality, in which Iran's desire to obtain nuclear weapons is tested at a moment of truth, when the three parties are equally committed to the test.

In order to influence the political considerations of the parties, it may not be necessary for an Israeli military strike to target the entire nuclear program, and instead it can also target other high quality strategic targets in Iran. The required achievement is not damage to a given number of centrifuges, rather, it is the persistence of the military action against Iran until the goal is achieved. The IDF must preserve its force during the attacks, so that Israel can deliver a credible political message that it will simply not accept the old equilibrium points, and can pursue a viable military strategy for as long as necessary. Therefore, in this specific case, the principles of force protection and security are more important than the selection of targets for attack. Attacking specific targets that lead to major losses for the attacking force will impact negatively on the ability to persist in the required military strategy, and are therefore liable to impede the military force from executing the chosen policy. The force buildup and the operational concept must be aimed mainly at developing operational endurance.

The Covert Campaign: More Harm than Good

According to various press reports, Western intelligence agencies are conducting a covert campaign to disrupt Iran's nuclear program, via attacks against individuals, equipment sabotage, and cyber attacks. According to the strategic rationale outlined above, however, the covert campaign may well yield more harm than good. If we accept the rationale that we seek to

move the political-strategic equilibrium points in the Iran-US-Israel triangle and change the respective attitudes towards time, risks, and costs, this is the criterion by which the covert campaign's effectiveness must be judged.

The covert campaign involves relatively few risks. It is ambiguous with respect to the responsibility for operations and the question of whether specific events are the result of a deliberate action, malfunction, or accident. Operations in this campaign can be disavowed, and the price that the actor instigating the campaign must pay is lower than that of the overt military alternative[4] (this obviously refers to the costs and risks incurred by the dispatching state, not the operational unit, whose risks are liable to be high). The covert campaign is therefore to a great extent the recourse of a party seeking to avoid risks.

When a covert campaign is the principal line of action selected, the underlying message communicated is that the actor fears an overt and direct military confrontation because of the attending costs and risks. A negative strategic dynamic is thereby created, owing to the difference between the rival parties in their attitude towards risks. Iran is posturing as a tough, risk-accepting actor. Israel and the US choose risk-hedging means, such as the covert campaign, cyber attacks, sanctions, and diplomatic negotiations, and are therefore perceived as risk-averse actors who seek to limit their exposure to the price they will have to pay in the moment of truth.

So while Iran is seen as determined and willing to take risks, Israel and the US are seen as receding, without either of them having to show their cards. The winner in each round is determined by the fact that the US and Israel are unwilling to call the bet, not by how strong their cards are. The underlying truth is that Iran does not want a direct military confrontation, and would probably be badly defeated in a situation in which all three parties put their cards on the table. The dynamic that has emerged, however, enables Iran to adopt a strategy based on a projection of power, even though this is not backed up by real capabilities, and on the assumption that the US and Israel will be the first to fold.

The exceptions that prove the rule are the rare cases in which Iran's rivals showed determination, laid their cards on the table, and demonstrated credibility in their willingness to take risks; Iran retreated in these cases. An example of this is Iran's capitulation in January 2012, after threatening to blockade the Strait of Hormuz in the event of the US returning its ships to the Persian Gulf.[5]

As the covert campaign progresses, however, and more and more dubious events occur, it is gradually emerging that the behavior of the US and Israel is consistently limited in risk. This consistent behavior pattern makes it easy for Iran to formulate its strategy: a poker player who knows how high his opponent will bet can always push him into folding by raising his bet above his opponent's risk threshold. Under this dynamic, almost all the red lines presented by Israel and the West in recent years have been crossed.[6] Nuclear installations have been operated and uranium enriched in large quantities, while the real power of the parties has never been put to the test.

Judging by the results, therefore, the covert campaign is not succeeding in upsetting the equilibrium points in the Iran-US-Israel triangle. Despite the physical damage, Iran is not altering its policy. Any covert damage to the nuclear program (if it occurs at all) only requires Iran to repair the damage, or to adjust and execute a tactical maneuver. Eventually, it returns to its strategic path and its nuclear ambitions. Furthermore, the covert campaign gives the political leaderships of Israel and the US a soothing feeling that "they are doing something," thereby seemingly justifying postponement of the moment of truth and the fact that critical time is allowed to pass. For this reason as well, the covert campaign maintains – rather than challenges – the basic equilibrium point.

The covert campaign is therefore not the way of bringing the game to its moment of truth; it is a behavior pattern from which the enemy learns that it need not fear high risk measures that exceed the price range it has already taken into account, and that despite the physical-tactical damage to its assets, the enemy can continue marching toward its political-strategic goals. Thus in order to achieve its goals, Israel cannot continue to maintain a policy of low and measured risks. Israel must bring the game to a point at which bets are almost unlimited, in which no player folds, and all of them must show their cards. Israel can achieve this if it initiates and maintains a higher level of risk in the game. The cost and the risk are the entry ticket to the strategic game; willingness to pay the price and incur the risk is the strategy to resist the existing equilibrium points; and persistence under circumstances of risk and cost is the main theme of the campaign.

Attacking the Enemy's Strategy

Extending the spectrum of discussion and considering the need to attack Iran's strategy raises additional considerations in favor of a military attack and against a covert campaign. A successful strategy is one that presents the enemy with dilemmas – when every option selected by the enemy gives one an advantage. In this spirit, a military attack by Israel will present Iran with several strategic dilemmas:

a. Should Iran respond with wide scale action against American interests, or should it confine its response to Israel and try to avoid involving the US?
b. Should Iran continue its current effective approach of expanding its capabilities and remaining at the nuclear threshold, or should it stage a breakout to developing nuclear weapons?

With respect to the first dilemma, if Iran responds against vital interests of the US (action in the Strait of Hormuz, for example), it will by itself bring the moment of truth in the strategic game closer. On the other hand, if Iran confines its response mainly to Israel through its proxy Hizbollah, at least the next confrontation with Hizbollah will be for a worthy strategic cause. Israel should assume that it will face Hizbollah sooner or later, for one reason or another, and it is preferable for the next round to result from the Iranian nuclear program rather than circumstances with no benefit for Israel, such as an internal Lebanese crisis, a miscalculation, or an event like the local border incident at Milestone 105 (the cause of the Second Lebanon War).

Incidentally, an Israeli attack against Iran will also present Hizbollah with difficult dilemmas, because the organization will have to decide whether or not to behave as an Iranian proxy, which would entangle Lebanon in a war from which it will suffer large scale damage for the sake of an issue that does not concern Lebanon's national interests. In any case, Iran's response will expose the limitations of its power, and Iran currently has greater deterrent capability than it would have after trying to carry out its threats. Subsequent to actual Iranian application of force, as opposed to its current successful posturing, the strategic dynamics and calculations may considerably differ from the current ones.

With respect to the second dilemma, if Iran stages a breakout by developing nuclear weapons, it will again promote the arrival of the moment of truth. If Iran continues its current approach of expanding its

infrastructure and remaining at the nuclear threshold, but with reduced capabilities as a result of the attack, it will reinforce Israel's contention that the nuclear program can still be rolled back by violent means.

For these reasons, only an open military attack, not a covert campaign, also constitutes an attack against Iran's strategy.

Part II: The Use of Force in the Main Theaters of Confrontation

The Vacillating States

Three key states – Turkey, Egypt, and Jordan – were partners of Israel and made a substantive contribution to its strategic freedom of action. Significant changes are underway in all three of these states, and their great importance to Israel makes it necessary to discuss them prior to a discussion of Israel's enemies.

The Turkish military (which is, or at least was, secular) was a key player in Turkish politics. For many years, Israel regarded it as a partner in containing pan Arabism, the Soviet Union/Russia's Middle Eastern tentacles, Syria, Iraq, and Iran, and in the war against sub-state organizations. This approach was expressed in close military and intelligence coordination, reinvigorated in the mid-1990s. Political backing from a regional Muslim power also provided Israel with useful freedom of action.

The 2002 elections, however, initiated a dramatic change in Turkish politics, with the gradual exclusion of the Turkish military from the political power centers and the military's becoming less secular. Turkish Prime Minister Recep Tayyip Erdoğan shifted Turkish policies to a confrontational stance towards the US, Europe, and Israel. The first signs of friction between Israel and Turkey appeared during the Second Lebanon War; Operation Cast Lead provided Erdoğan with an opportunity to ignite a crisis, and the flotilla to Gaza orchestrated by the Turkish organization IHH led to a profound rift. Another point of friction that has drawn insufficient attention is the Eastern Mediterranean gas fields, which were divided in an agreement between Israel and Greek Cyprus. Turkey does not recognize Greek Cyprus, and Turkey and Lebanon do not recognize the agreement on division of the gas fields.

Turkey is not Israel's enemy, and should not be treated as such, but Turkey's emerging policy has several consequences. First of all, at this stage Turkey is no longer Israel's partner in the regional balance of power.

On the contrary: it seeks to hamper Israel and capitalize on crises with it. Second, Turkey is expanding its political and diplomatic penetration of the Arab world, and wishes to position itself as a regional patron. Third, Turkey is bolstering its physical presence in the theater, including the presence of military assets. These developments increase the potential friction between the countries, and are becoming part of Israel's tapestry of political, strategic, and operational considerations.

Certainly Israel should try to avoid deterioration in relations with this NATO-member state, yet it is difficult to assess under what circumstances friction between Turkey and Israel might increase, and how far such deterioration would go. Circumstances exist, however, that are liable to heighten the danger of worsening relations. If the IDF embarks on a large scale campaign in Gaza, Lebanon, or another bordering arena, Turkey may well attempt to fulfill its aspirations to regional leadership by backing its Arab allies. Israel's freedom of action can be restricted through political means, but the possibility of some Turkish physical presence in the theater cannot be ruled out. For example, Turkey might expedite humanitarian aid to the theater and use military forces to secure its delivery. An Israeli aerial or naval blockade on the theater, if imposed, could well become a point of friction between Israel and Turkey, and it should be carefully considered whether the complications of a blockade outweigh its advantages. Turkey's physical presence in a theater is itself liable to pose difficult operational dilemmas.

Egypt is the most important Arab state, and until the peace agreement with Israel, the Egyptian military constituted the principal challenge in each of Israel's wars. In the first two decades following the peace agreement between the two countries, a dual political reality existed. On the one hand, Israel benefited from greater freedom of action, secure in the knowledge that the border with Egypt was peaceful. Even during crises like the First Lebanon War and the first intifada, Israel was free of concern about the opening of another front in the south. On the other hand, Egypt remained politically hostile and acted against Israel on various issues, including the Nuclear Non-Proliferation Treaty and the attempts to channel Jewish immigration from the Soviet Union to the US, as well as in regional political questions and at international diplomatic forums. In Egyptian jargon, it tried to "cut Israel down to its natural size."

In the first decade of the new millennium, however, Egypt gradually became a strategic partner of Israel against Iran and its proxies in the Arab world. The Israeli-Arab fault line was replaced by a fault line between Israel and the Sunnis on the one hand and the Shiites on the other (and their satellites, some of whom were Sunnis). This reversal in Egyptian policy expanded Israel's freedom of action, and strengthened it strategically, as significantly reflected in the bilateral, regional, and international backing Egypt gave Israel in the Second Lebanon War and Operation Cast Lead.

A new political reversal occurred in February 2011 – this time for the worse – when Egyptian President Husni Mubarak was ousted from power and Egypt embarked on a path that strengthened the Islamic movements at the expense of the seasoned military establishment. The question of where Egypt is headed is still open, and Egypt should certainly not be treated as an enemy. At the same time, the internal developments in Egypt have several consequences. First, the strengthening of the Islamic movements weakens Egypt's status as a stable ally of Israel against their common enemies, and it cannot be assumed that Egypt will back Israel's future military campaigns the way it did in recent years. Second, Israel's embarking on a large scale military campaign (in Gaza, for example) in and of itself is liable both to prove a factor in shaping internal Egyptian politics and to strengthen the factions that oppose peace with Israel.

Hamas has deep-rooted historic and personal ties with the Egyptian Muslim Brotherhood Egypt, and the two are to a large extent sister movements. Indeed, given the removal of Mubarak and the crisis in Hamas-Iran relations concerning Iran's support for Syrian President Bashar Assad, a trend is emerging in which Hamas is weakening its ties with Iran and replacing them with ties to the Egyptian Muslim Brotherhood. The system in which Israel and Mubarak squared off against Iran and Hamas is liable to be replaced by a Hamas and Egyptian Muslim Brotherhood axis opposed to Israel. Moreover, Egyptian public opinion is more assertive than in the past, and even if policymakers in Egypt are willing to accept certain Israeli military measures, newly-empowered Egyptian public opinion is liable to reject them. These processes are generating a direct link between Israel's use of military force – primarily against Hamas – and the internal Egyptian dynamic and Israeli-Egyptian relations, one that clearly restricts Israel's freedom of action.

A symbiotic relationship between Israel and the Jordanian royal house has existed for years. The Hashemite family suffers from profound weaknesses, particularly as it rules over a Palestinian majority. Furthermore, Jordan is situated at a crossroads between more powerful forces: Syria, Egypt, and Iraq. In face of these weaknesses, Israel has provided the Hashemite family with a protective umbrella by stating that a threat to the Jordanian royal house constitutes a casus belli for Israel. This situation has successfully withstood several tests, particularly in 1970. For its part, Israel has found the Hashemite family to be a partner in two important spheres. The Hashemite kingdom has become a de facto demilitarized zone with no enemy forces, and has usually prevented hostile use of its territory and long borders with Israel. In certain senses, Israel's strategic depth extends to eastern Jordan. In addition, an Israeli-Hashemite partnership, albeit limited, has emerged concerning the containment of Palestinian national aspirations and their direction to channels that relieve the threat to Israel and the Hashemite monarchy.

Jordan was too weak to seal its territory hermetically against terrorist action and expeditionary forces directed against Israel. Its weakness even infrequently obliged it to participate in Arab coalitions against Israel. Yet most of the time and on most issues it kept its part of the symbiotic bargain. Worthy of note is the warning provided by King Hussein to Israel about the Arab plans to launch the Yom Kippur War. The peace agreement signed by Israel and Jordan in 1994 was little more than a symbolic declaration of a strategic reality that in any case had already existed for decades.

Today, however, the Hashemite dynasty faces complex threats from a number of directions, and its future is unclear. The first threat – the internal agitation in Jordan – has reached a stage in which the legitimacy of the king is challenged openly. The second threat is that even the Bedouin tribes, who have been the mainstay of the monarchy, are beginning to take part in the agitation against the king.[7] The third threat is a result of the American withdrawal from Iraq, which has left room for Iranian influence in Mesopotamia, thereby bringing Iran to Jordan's back door. It may only be a question of time before Iran begins to intervene in Jordan. The fourth threat is the Hashemite dynasty's loss of the support provided by Mubarak; it is doubtful whether the Egyptian Muslim Brotherhood would back the Hashemites against Islamic agitation. The fifth threat is the unpredictable

spillover effect on Jordan of a potential breakup or change of regime in Syria.

The challenges and increasing weakness of the Jordanian royal dynasty have two main consequences for the use of military force by Israel. The first is that a situation in which Israel conducts a large scale military campaign in some theater while the Israeli ambassador sits in Amman and the king sits idle is liable to pose a difficult internal challenge to the royal family. The challenge will be even more difficult than that posed by Operation Defensive Shield and Operation Cast Lead. The second is that if the Hashemite monarchy falls for any reason, Israel will lose an important asset that contributed greatly to its security and strategic power. Israel's longest border is liable to change its character. It therefore follows that where the Hashemite monarchy is concerned, Israel's freedom of action is narrowing.

A Major Military Campaign and the Vacillating States

The potential political and strategic benefit of a large scale campaign by Israel in one of the prime confrontation theaters is limited. Both southern Lebanon and Gaza are examples of this.

Hizbollah's rocket array, with its high redundancy, is now deployed with unprecedented depth. According to media reports, it is dispersed among the population in 160 civilian urban areas. Reaching a military decision against Hizbollah, in the sense of depriving it of the ability to operate high trajectory weapons against Israel, is impractical in a reasonable amount of time and at a reasonable price. Furthermore, any military campaign will have difficulty in addressing the fundamental problem of Lebanon: the country comprises ethnic minorities lacking state-like coherence, and its weak central government will have trouble enforcing its sovereignty in its own territory. It is possible to degrade Hizbollah, damage it, and affect its behavior for a while, but it is difficult to imagine a military campaign that could create a different fundamental political reality in Lebanon that would be better for Israel. In attempting to design a campaign in Lebanon, Israel can choose between a large scale campaign in which both sides will pay high prices and a smaller campaign that will exact limited prices from both sides. The optimal political result, however, will probably be similar in both alternatives, and will in any case be limited.

In contrast to Hizbollah, it is possible to deprive Hamas of the ability to launch rockets against Israel, but this involves a takeover and comprehensive combing of the entire Gaza Strip. If the IDF occupies the Gaza Strip, the problem arises what to do with it afterwards. More important, it is difficult for a military campaign to address the fundamental problems of Gaza: a dense Palestinian population, which suffers from human, civilian, and economic underdevelopment and embodies a radical culture, and is situated in geographic proximity to Israel's heartland. The possible military achievement in Gaza may be better than what can be expected in Lebanon, but here too it is difficult to imagine a political end state that represents a stable and sustainable reality that is better for Israel.

The modest political and strategic achievements that can be obtained in a large scale military campaign in Gaza or Lebanon should be weighed against the potential complications in political and strategic relations with the vacillating states mentioned above. Were the expected gains against the enemy remarkable, it might be worthwhile to pay the price of worsening relations with the vacillating states. However, it is questionable whether there is any point in risking the upsetting of relations with the vacillating states and perhaps causing them internal shocks, merely for the sake of obtaining a limited and transient achievement against the enemy.

The change in the Arab world also provides a new context for the challenge of collateral damage to civilians. This is not only a question of media, the laws of war, or Israel's relations with international organizations. The increased weight of public opinion in the considerations of Arab decision makers means potential effective pressure on them when collateral damage is caused. In the emerging reality, some degree of legitimacy from Arab public opinion for an Israeli campaign is more than just valuable – and that creates a much higher hurdle for the use of force.

The obvious problem lies in the fact that Israel is not the only party deciding whether to conduct or refrain from a violent confrontation. The enemy also gets a vote. As Israel's freedom of action narrows, that of its enemies is expanding, or at least is seemingly expanding. Assessing Hizbollah's freedom of action in a changing environment is a complex question, since it derives from Iran's position and political considerations, internal shockwaves in Syria, inter-ethnic relations in Lebanon, the actions of the international court investigating the Harari murder, and so on. At the same time, in certain circumstances, Hizbollah's complex array of interests

is liable to generate motivation on its part for deliberate escalation with Israel.

An analysis of Hamas' freedom of action is also far from simple, and the movement must contend with various limitations.[8] In estimating possible courses of action by Hamas, however, the changing reality must be taken into account, including the increased weight of the Islamic movements in Egypt, the loosening of the Jerusalem-Cairo axis, the crisis in Iran-Hamas relations, and the undermining of Egyptian governability in Sinai. Hamas, or at least some elements in it, now has affiliations (to some extent conflicting) with Tehran, Cairo, and Ankara. The growing closeness between the Egyptian Muslim Brotherhood and Hamas entails two aspects: on the one hand, the constraints on the Egyptian leadership can be a restraining factor on Hamas (and this has been the case in recent months). The strengthening of Hamas' state-like characteristics as the ruler in Gaza also constitutes a restraining factor. On the other hand, the close relations between Hamas and Egypt are liable to imbue Hamas with the sense that it enjoys greater freedom of action against Israel. At some point, Hamas may seek to challenge what remains of Israeli-Egyptian relations by drawing Israel into a major military campaign in Gaza. In contrast to its behavior in recent months, it is liable to use its rocket arsenal in a way that will leave the Israeli government with little choice other than to embark upon a large scale military campaign in Gaza. In this case, the political trap set by Hamas should be understood and avoided wherever possible.

The realization that the possible political and strategic benefits of a campaign in Gaza or Lebanon are liable to be meager, and that the costs and potential entanglements in relations with the vacillating states are significant, can lead the Israeli military planners to several conclusions. First, under the currently prevailing circumstances, major campaigns liable to cause large scale collateral damage should be avoided whenever possible. When a violent event or miscalculation occurs, force should be applied in a way that facilitates a rapid exit from the cycle of violence and avoids undesirable escalation. Second, if the enemy deliberately chooses escalation and makes a large scale campaign unavoidable, the perspective should be widened and the military plan's political and strategic effect on the entire region should be considered, including public opinion in the vacillating states.

These are seemingly the exact parameters for the IDF's consideration of essentially defensive strategic plans. The problem is that given the current war model of Hizbollah and Hamas, the question of what a defensive strategy means in this context needs to be clarified. When the enemy attacks deep within Israel's territory with high trajectory fire from deep within its own territory while remaining in a defensive disposition on the frontlines (a concept in IDF jargon known as "offensive-defense"), it is unclear what unique operational content can be given to an IDF defensive strategy. On the face of it, it is necessary to reach the enemy launchers with either firepower or by maneuver in order to affect them, but these launchers are deployed deep within enemy territory and are embedded in urban civilian areas. It is therefore necessary to consider whether this is indeed the only possible way of applying force in situations of both strategic defense and strategic offense (if it is at all possible to distinguish between them under these circumstances), or whether there are more effective ways of using force.

The military planner should search for ways to restrict the enemy's strategic freedom of action to continue fighting, and convince it to terminate the current cycle of violence, even without reaching a military decision against the enemy. It should be considered whether it is possible to operate in places and ways that can reduce friction with the enemy population, avoid a permanent seizure of territory, and maintain the legitimacy of using force. Because of the emergence of interdependence between theaters, it should also be considered whether it is correct to commit a campaign to a given theater of conflict, or whether it is more important to preserve the ability to switch rapidly between theaters. The military must add the legitimacy of the use of firepower and maneuvering as viewed by public opinion in Egypt, Jordan, and Turkey to its list of considerations (though not as the sole consideration). Achieving legitimacy is not restricted to the duration of the fighting, and intensive action in this direction should be taken both before and after force is used.

In the Six Day War, the opposing sides conducted a symmetrical battle on a smooth playing field, and Israel achieved a clear decision. Since 1967, the violent confrontations with Israel have featured efforts by its enemies to restrict its ability to realize its full military potential. This has been done in a number of ways: using non-state armed organizations, planting combatants among civilians and blurring the division between civilian

and military, blurring the distinction between war and lull, and creating intermediate low intensity confrontations in which Israel suffers attrition but does not embark on a major campaign. The next stage in restricting Israel's military freedom of action may consist of the use by Israel's enemies of the vacillating states on two levels. On the political and strategic level, Israel's considerations will include its relations with the vacillating states, and it will therefore restrain itself more than in the past. On the tactical and physical level, Israel's enemies can attempt to attain new degrees of freedom for themselves by operating from the territory of the vacillating states in close proximity to their assets, including military assets.

Conclusion: From an Isolated Campaign Theater to a Multi-sided War Theater

In recent decades, strong gravitational forces have pushed the various players into close strategic blocs, and have blurred the differences between them. Such gravitational forces were active in the conflict between blocs during the Cold War, for example, and starting in 1991, they have been manifested in the pro-American and anti-American Middle Eastern camps. Following the decline of American hegemony and other changes, however, these gravitational forces have weakened. Consequently, differences in interests among the various players have been highlighted, and the tapestry of affiliations among the players has become more complex.

In the emerging reality, the clear dichotomy between rival and ally has been replaced by a range of intermediate behavioral patterns. This phenomenon complicates Israel's use of force and the analysis of its influence on players who are not enemies, but who do not coordinate their actions with Israel – yet are active in the war theater and are relevant to the strategic dynamic. This phenomenon requires a stronger military-political interface than in the past.

This situation is relevant to the Iranian nuclear challenge, in which some of the most important effects of using force are not on the enemy, but on an ally – the US. This is also relevant to the bordering confrontation theaters. Since the 1980s, Israel has become accustomed to conducting wars with a single isolated campaign theater, and most of the crises it has faced have been bilateral. It appears that this reality no longer exists, and it is faced with a complex system of affiliations, some of which will emerge and be shaped only as a result of the fighting.

Notes

1 Ron Tira, "The Breakup of Israel's Strategic Puzzle," *Strategic Assessment* 14, no. 3 (2011): 43-56.

2 Ron Tira, "Yes They Can: The US Can Prevent Iran from Acquiring the A-Bomb," *Infinity Journal*, IJ Exclusive, May 2012.

3 Ron Tira, "The United States in the Middle East: An Exercise in Self-Defeat," *Strategic Assessment* 14, no. 1 (2011): 41-54.

4 Martin C. Libicki, "The Strategic Uses of Ambiguity in Cyberspace," *Military and Strategic Affairs* 3, no. 3 (2011): 3-10.

5 "Foreign Warships Will Need Iran's Permission to Pass through Strait of Hormuz," *Fars News Agency*, January 4, 2012.

6 Reza Kahlili, "Iran Nuclear Compromise No Longer Needed," *Washington Post*, April 9, 2012.

7 H. Varulkar, "The Arab Spring in Jordan: King Compelled to Make Concessions to Protest Movement," MEMRI, December 12, 2011, http://www.memri.org/report/en/0/0/0/0/247/0/5906.htm.

8 Shlomo Brom, "The Storm within Hamas," *INSS Insight* No. 316, February 28, 2012.

Iran: Maritime Measures below the Threshold of War

Yoel Guzansky

The option of operating in the naval theater allows improved deterrence and attack capability vis-à-vis Iran and makes it possible to impose crippling sanctions. And indeed, one of the options examined in recent years for dealing with Iran – ostensibly under the threshold of war – is a naval blockade that, inter alia, would prevent goods, including petroleum and petroleum products, from entering and leaving Iranian ports. The goal would be to persuade Iran to change its policy, with an emphasis on stopping its nuclear development. Supporters of these measures argue that such steps would be sufficient to cause critical damage to Iran and force it to change its policy, without the use of military force. This article will examine various aspects of maritime enforcement and prevention methods in the context of Iran, first and foremost a naval blockade, for the purpose of stepping up pressure to thwart proliferation of non-conventional weapons. In addition, it will discuss the ramifications of these enforcement and prevention measures and the relevant alternatives available to the international community.

A Naval Blockade

In principle, maritime law is seen under the rubric of the laws of peace of international law, that is, the laws that govern relations between countries that are not in a state of armed conflict. There are three fundamental principles in this system of law: the principle of flag-state sovereignty (which is beyond the scope of this article); the principle of freedom of navigation on the high seas, which stipulates that ships enjoy complete freedom of movement in international waters; and the principle of

Yoel Guzansky is a research fellow at INSS.

territorial waters, which stipulates that in contrast to what is applicable to international waters, in territorial waters there is no freedom of movement, and barring unusual situations, movement is contingent on the approval of the coastal state.

These fundamental rules have several exceptions; the most notable concerns a state of armed conflict, under which the laws of naval warfare allow the parties to the conflict to impose restrictions, both on vessels of the other party to the conflict and on neutral vessels. In other words, in a state of armed conflict at sea, some of the basic rights conferred by peacetime maritime laws are eclipsed by the rights conferred on the parties to an armed conflict (belligerent rights).

The laws of naval warfare have not been regulated through a binding international treaty (in contrast to the laws of land warfare). However, the customary rules that are binding on states in armed conflicts at sea are anchored in several basic documents; especially noteworthy are the "London Declaration concerning the Laws of Naval Warfare" (1909) and the "San Remo Manual on International Law Applicable to Armed Conflict at Sea" (1995). Under these rules, there are several measures that can be taken, such as visit, search, and seizure of ships; restriction of naval activity in the area of the military operation; and declaration of a combat zone.

The meaning of freedom of navigation on the high seas is that ships of all nations have an equal right to make use of the high seas in every way possible. As a result, in peacetime, ships flying the flag of one country may not interfere with the passage of ships flying the flag of another country. The prohibition on interference with freedom of navigation on the high seas also applies to warships that in peacetime seek to interfere with the ships flying state flags different from the warship's flag. There are several exceptions: piracy, the slave trade, hot pursuit, a ship that hits underwater cables, and if sanctions are imposed by the UN Security Council on navigation on the high seas by a particular state.

The most significant measure under the laws of naval warfare is a declaration of a naval blockade. This serves as a means for the parties to an armed conflict, under the laws of naval warfare, to prevent ships from entering ports or coasts under enemy control and from departing from them to the open sea. The purpose of this measure is to prevent passage of cargo and people by sea to and from a territory under enemy control. Naval blockades were imposed during the Korean War, the Cuban missile

crisis, the Vietnam War, and the war in the Falklands. Examples from recent years include naval sanctions against Iraq (1990-2003), the naval blockade imposed by Israel on Lebanon during the Second Lebanon War (2006), and the naval blockade imposed on the Gaza Strip at the start of the ground invasion in Operation Cast Lead (2009).[1]

Regarding Iran, several senior US[2] and Israeli[3] officials have declared their support for imposing a naval blockade in order to step up the pressure while avoiding a costly military confrontation. Israel has insisted that the sanctions imposed on Iran are too soft and insufficient to stop the Iranian nuclear program. Therefore, what might be needed is to back them up with a US naval blockade that would exert heavy pressure on the Iranian regime and prove that the United States and other Western countries are serious about preventing Iran's nuclearization.[4]

The binding customary rules for imposing a naval blockade so that it is considered legal and valid are:

a. *Declaration*: The party imposing a blockade must clearly bring it to the attention of all those likely to be affected, including of course neutral states; the declaration should include the date the blockade will begin, its boundaries, and perhaps how long it will last.
b. *Effectiveness*: The state that declared the blockade must enforce it actively and effectively.
c. *Non-discrimination*: The blockade must be enforced fully and in a non-discriminatory manner against all vessels (including those of the state imposing the blockade).
d. *Access to the coasts of neutral states*: Blockades should not block access to ports and coasts of neutral states.

In the San Remo Manual, there are two further conditions, although it is doubtful that they have customary status. The first is a prohibition on blockades intended to starve the local population or deprive it of measures essential to its survival. The second condition is proportionality; in other words, the imposition of the blockade will be illegal if the collateral damage it causes to the civilian population is excessive in comparison to the military advantage it produces.[5]

Once a naval blockade is declared, any attempt by ships to enter, exit, or pass through the area of the blockade is considered a violation and will give the party imposing the blockade the authority to seize the vessel (even in international waters, if it is clear that the purpose of the vessel is to violate

the blockade). If the vessel in question resists, force may be used against it (as long as advance warning is provided). This is clearly an action under the laws of armed conflict at sea.

UN Security Council Resolution 3314 (1974) defines the term "aggression" that was adopted by the state signatories to the Rome Declaration (and is expected to enter into force in 2015). In the resolution, the use of a naval blockade is explicitly defined as an act of aggression that can establish the right to self-defense by the party being attacked and can even lead to intervention by the UN Security Council. For example, there is no doubt that the declaration of a naval blockade on the coasts of Iran by the United States would be considered an act of war and would establish the right to self-defense by Iran against the "aggression" of the United States. A declaration of a naval blockade of this sort can be established in one of two ways:

a. A Security Council resolution imposing a naval blockade under chapter 7. This is the alternative preferred by the United States (if indeed it sees fit to impose a naval blockade on the coasts of Iran). In fact, several resolutions in this spirit have already been passed against Iran in light of its obstinacy and continued development of its nuclear project, but they have not reached the point of imposing a naval blockade. Such a resolution by the Security Council would be entirely legal and would not create any legal difficulty. However, there is significant political difficulty in passing it because of the expected opposition of key countries, including Russia and China, which might possibly even veto it.
b. A format that does not involve Security Council authorization (for example, due to the possibility of a veto by Russia, China, or both). In that case, the justification for the act of war by the United States – imposition of a naval blockade – so that it would not be considered a prohibited aggressive action could be based solely on the claim of anticipatory self-defense. This would be on the basis of the call by another state for American assistance (for example, Israel or the Arab Gulf states) given the "aggression" of Iran, its development of a capability to strike Israel, and its declared threat to destroy Israel.

These threats by Iran establish the possibility for Israel to claim anticipatory self-defense and seek military aid from the United States, which can include the act of war of imposition of a naval blockade on

the coasts of Iran. However, this claim is complex and raises some real legal questions, and there is no certainty that it would earn international legitimacy. First, there is still no smoking gun proving that Iran intends to develop nuclear weapons. (At the same time, some contend that the findings of the International Atomic Energy Commission report of November 2011 and the construction of the facility carved into the mountainside near the city of Qom indicate that Iran intends to develop military nuclear capability. Security Council resolutions on the Iranian issue also provide a basis for the assumption that illegal activity is taking place with their demand for Iran to suspend uranium enrichment.) Second, the claim of preventive self-defense is always complex, and it is doubtful that the international community would accept it, especially after the principal attempts through the Security Council were unsuccessful. Furthermore, Israel's attack on the Iraqi nuclear reactor on similar grounds did not get backing from the international community and was seen as an act of aggression by Israel against Iraq, prompting a resolution by the Security Council condemning Israel. Consequently, it is doubtful that the United States will wish to engage in a clear act of war such as a naval blockade without legal backup and without legitimacy from the international community (even though in some of the examples of a naval blockade cited above there was no such legitimacy).

Security Council Resolutions

In April 2004, the Security Council unanimously approved Resolution 1540 (under Chapter 7 of the UN Charter) calling upon states to prevent the proliferation of nonconventional weapons; to refrain from assisting any actor in the process of manufacturing and transporting nonconventional weapons; and to monitor the distribution of materials necessary for their manufacture. The resolution also established a Security Council committee to monitor its implementation. This was the first time that the Security Council issued a comprehensive resolution that included not only declarative clauses, but also operative requirements of the member states concerning clear and defined moves designed to fight proliferation of nonconventional weapons, while mentioning nonconventional terrorism and the connection between it and the non-state organizations as a "threat to international peace and security."[6]

UN Security Council Resolutions 1803 (March 2008) and 1929 (June 2010) provide a foundation for increasing oversight of cargoes entering and exiting Iran. Resolution 1803 calls upon states "to inspect the cargoes to and from Iran, of aircraft and vessels, at their airports and seaports," to ensure that they are not carrying prohibited goods. Resolution 1929 (the fourth in a round of sanctions on Iran) constitutes a further measure, setting out the framework for inspecting suspicious cargo on ships or aircraft for the purpose of preventing smuggling by Iran. However, there are several possible problems in the implementation of the guidelines of some of the clauses. For example, the state's ability to detain ships that have suspicious cargo is weakened if the flag state must give its agreement to the inspection, although there are countries like the United States that claim that the agreement of the captain is sufficient. The agreement of the flag state provides a more solid legal basis, but there is no way to ensure that it will be given, certainly not in the time required.[7] Naturally, there are liable to be difficulties in cases in which the flag belongs to a state that is not prepared to cooperate with the provisions of the sanctions. In any case, Iran considered these resolutions a violation of its fundamental rights and threatened to respond "appropriately" if cargoes of Iranian vessels were inspected.[8]

Preventing Proliferation of Nonconventional Weapons

The international community has additional tools that can serve as a basis for increasing pressure on Iran, especially in light of the difficulty of enlisting international forums, particularly the Security Council. One of the most notable tools is the Proliferation Security Initiative (PSI), an attempt to stop shipments of nonconventional weapons and related equipment to terrorists and to states of proliferation concern, through active cooperation at sea, on land, and in the air. The initiative, which reflects the preferred US active model (with emphasis on thwarting and preventing proliferation) was publicly announced by President George W. Bush in May 2003. The initiative provides a set of tools, to be used on a voluntary basis, with no formal umbrella organization, secretariat, or founding treaty. As of July 2012, 100 states have taken part in the initiative in one way or another, including states belonging to the original founding group (the United States, Britain, Australia, France, Italy, Spain, Portugal, Holland, Germany, Japan, and Poland). The initiative is based on an understanding that the

existing nonproliferation regime is not sufficient for preventing the spread of nonconventional weapons and that complementary measures must be taken.

The initiative's most notable success was the seizure of the *BBC China* (in October 2003), a German-owned ship carrying a cargo of centrifuges from Malaysia (as part of the distribution network of A. Q. Khan) through Dubai to Libya. The event was a major factor in Libya's subsequent announcement that it was giving up its nonconventional capabilities. In this case, following a request from the United States, the ship's owners directed the ship to the port of a member state, Italy, where it was searched and its banned cargo was confiscated.

Over the years, many naval and aerial exercises were held intended to consolidate joint working methods. Activity connected with the initiative has remained almost completely secret, but over two dozen interceptions are attributed to PSI activity, including the interception of shipments to Iran.[9] This is likely only the tip of the iceberg, given the large scope of maritime activity to and from Iran, but it is sufficient to deter potential rogue actors from transporting goods in this way. In its overall legal infrastructure, the initiative is in compliance with the UN Convention on the Law of the Sea and UN Security Council Resolution 1504. Indeed, Resolution 1504 was to a large extent passed in the spirit of the initiative (though because of pressure from China, the resolution does not mention the PSI), and it grants the initiative a retroactive legal imprimatur. In addition to claiming that the initiative actually harms the nonproliferation regime by its very existence, several states, particularly China and North Korea, have criticized it, believing it was directed mainly at them.

One of the problems faced by members of the initiative is establishing intelligence-operational cooperation with: a) coastal states that serve as a place to anchor for ships carrying cargoes; b) flag states under whose national flag the ships are registered (the registration provides the vessels the legal protection of that state); c) countries through which the forbidden cargoes pass. In addition, there is an apparent basic contradiction between the initiative and the principle of free trade. Thus far, the United States has signed agreements with Liberia, Panama, Malta, Belize, Cyprus, the Bahamas, Mongolia, Croatia, and the Marshall Islands, which allow an immediate search by most merchant marines in the world. These

agreements allow the United States to conduct inspections on a ship bearing the flag of these states at short notice.[10]

The US government has apparently seen that informal action allows flexibility and is much more effective than a formal institution, which is liable to be unwieldy and tainted by political interests. It appears that for now, it has stopped previous programs that were intended to institutionalize the initiative in one way or another. Moreover, although there is no institutionalized organizational infrastructure, a system of coordination has developed among states supporting the initiative; a group of experts in operations discusses suspicions about proliferation and plans training exercises to stop those transporting the equipment and materials related to weapons of mass destruction. This group includes experts from the military, law enforcement, intelligence, law, and diplomacy from twenty-one of the states that are partners to the initiative.[11]

The ability to use the PSI platform to impose a naval blockade is limited, both because of the labor pains of the initiative and because the initiative is intended to foil the proliferation of nonconventional weapons. However, in light of the precedent in which the *Monchegorsk*, an Iranian merchant ship, was forced to dock and unload its cargo in a third state, it appears that there is greater international willingness to make use of this tool in order to increase the pressure on Iran, and over time, the initiative is likely to receive greater legitimacy. Increased legitimacy is also likely to expand the initiative, from a focus on preventing shipments at sea to preventing shipments in the air and on the ground, and from preventing shipments of nonconventional weapons to preventing shipments of conventional weapons. It is important that key states in the Iranian context have joined the initiative in recent years, including the UAE, Turkey, and South Korea. However, it is also important to include prominent countries such as China, Indonesia, and Malaysia, which have thus far remained outside the initiative, and may embrace a problematic policy concerning unauthorized proliferation.

Discussion

The naval theater makes it possible to take advantage of Iran's vulnerability and pressure it to change its nuclear policy, and the West must do more than it has thus far in order to prevent Iranian access to maritime trade. Thus, for example, shipping companies that do business with Iran should

be barred from docking at ports in Europe and the United States (especially worth mentioning in this context is the Tidewater company, which handles 90 percent of Iranian maritime cargo). Most of Iran's revenues come from export of crude oil by sea. Iran's dependence on the import of raw materials that are not crude oil, such as refined petroleum products and consumer goods, is also extremely significant. It is possible to cause Iran tremendous damage by harming its ability to export oil or preventing the supply of refined oil, because some one-half of its fuel products are imported. The same holds true for food, industrial machinery, and electronic consumer goods – preventing them from being shipped to Iran would severely damage the Iranian economy. Disruption of traffic to and from Iran through the Strait of Hormuz could have significant economic and even political consequences for Iran, because of the regime's overwhelming dependence on export of crude oil (anticipated revenues of some $100 billion in 2012). The ports along the Persian Gulf coast have paramount strategic importance for Iran because they are the only channel for exporting Iranian oil and importing the goods required for the Iranian economy: some 90 percent of the imports to Iran and 99 percent of its exports go by sea, the large majority through the Strait of Hormuz.[12] Because of its dependence on export of oil through the Strait of Hormuz and its vulnerability to any interruption to free shipping in the Gulf, it has been reported that Iran intends to establish its first oil terminal outside the Strait of Hormuz.[13] When the new oil port is operational (which depends on laying the oil pipeline), Iran can export a significant portion of its oil without fear that the Strait of Hormuz will be blocked.

In the past, the US Congress discussed a bill that would prevent refined petroleum products from entering Iran by imposing a naval blockade. This bill has been put on hold, apparently because of the high cost associated with enforcing its provisions. However, it is reasonable to assume that in preparing the options for the "day after" the failure of the dialogue with Iran, the US Fifth Fleet is holding war games and discussing ways to increase the pressure on Iran, such as increased monitoring of banned goods entering and exiting the country. The PSI provides the initial tools for handling prohibited shipments to and from Iran in the naval arena. In the past, Iran received a significant number of shipments by sea from the Khan network (Pakistan-Dubai-Bandar Abbas). Interception of such shipments will require regular patrols in the Arabian Sea on the way to

the Strait of Hormuz by PSI members, and cooperation by the states in the ports close to Iran, especially the UAE, which is a critical transit station in Iranian maritime commerce. The operational foundation for the Iranian theater is stable. Thus, for example, in the heart of the Gulf, in Bahrain, there is a base of the US Fifth Fleet, and several international naval task forces have been operating very effectively for years in the Persian Gulf and the Gulf of Oman, such as CTF-150. All that is missing is the political will.

Security Council resolutions on the issue of Iran provide a legal infrastructure for increased monitoring of the country. In addition, the failure of the talks with Iran about its nuclear future could contribute to the willingness of the West to take further, more serious steps against it, particularly in light of the fact that the economic sanctions imposed thus far have not changed its nuclear policy. The PSI initiative is limited in its ability to intercept "soft proliferation" (capital, information, and so on), and its relevance is decreasing as Iran overcomes its dependence on the import of sensitive materials for its nuclear project. In addition, the initiative does not provide a full response to interception of sensitive shipments in the air and on land, but it is likely to be a platform for steps intended to restrict Iran's moves and increase pressure on the regime, a kind of partial naval blockade.

In contrast, a total naval blockade is a clear act under the laws of armed conflict at sea, which is considered an act of war and will establish an Iranian right to self-defense. In addition, blocking the entry of refined petroleum products to Iran and Iranian exports of crude oil would be serious from the Iranian point of view because the country is dependent on them, to the point that it would threaten the stability of the regime. In general, it is impossible to be certain that the pressure and the sanctions will cause the Iranian regime to change its policy on the nuclear issue, yet in order to avoid a military confrontation with Iran, an attempt should be made to prevent it from continuing its current policy by stepping up the pressure, under the threshold of war, in the naval arena as well.

Appendix: Thwarting Iranian Arms Shipments

For more than ten years, a war has been taking place far from Israel's coasts, against the smuggling of weapons from Iran, for example, the seizure of the Iranian ship *Karine A* near Sharm el-Sheikh in January 2002. Efforts to foil smuggling, stepped up after the Second Lebanon War, are ongoing

and involve cooperation with friendly states in the region. To a large extent the effort to stop prohibited arms shipments received legal and political legitimacy after Operation Cast Lead, and is also based on UN Security Council resolutions on Iran's nuclear program. At the end of Cast Lead, Israel and the United States signed a memorandum of understanding on the battle against smuggling of weapons from Iran to Hamas. As part of the agreement, a working group of several Western states was established to handle intelligence information toward prevention of weapons smuggling from Iran by sea to the Gaza Strip.[14]

In recent years the media has reported on many incidents of seizure of weapons shipments sent by sea from Iran to its proxies in the region. The attempt to vary the smuggling methods, the "high signature" of weapons shipments on land and in the air, and the ability to move especially large quantities of arms by sea have led the Iranians to increase their use of the naval medium.[15] Iran's arms shipments are in contravention of several UN Security Council resolutions, including Resolution 1747, which prohibits Iran from exporting weapons. Thus Iran's use of international shipping companies and European ports for moving arms is a systematic and gross violation of the laws of international shipping, and causes a substantial risk to civilian ships and ports involved in those shipments.

Following sanctions imposed (though not by the UN) on the large Iranian shipping companies, IRISL and HDS, Iran began to make use of European and international shipping companies as well, while concealing information from them regarding the contents of the cargoes.[16] To this end, Iran makes extensive use of front companies and false documents attesting to the innocence of the cargoes. Thus far, the Security Council has warned its members to be aware of possible violations of the sanctions by IRISL, but has not gone beyond this.[17] A published Security Council report charts the extent of Iranian arms smuggling and the use for this purpose of an IRISL subsidiary, which continues to operate ships whose chief destination is Syria. Thus, for example, in March 2008, an IRISL merchant ship left Iran for the port of Latakia in Syria, carrying a cargo with hundreds of tons of weapons for Syria. A NATO force that was in the area questioned the captain of the ship when it left the Suez Canal, and later even sought to carry out an inspection. After tactics of evasion, deception, and concealment, the ship succeeded in reaching its target without being inspected.[18]

In recent years, the Israeli Navy has managed to thwart several Iranian attempts at weapons smuggling. In March 2011, the navy seized the *Victoria*, a German-owned ship flying the flag of Liberia that was carrying weapons apparently intended for terrorist organizations in Gaza. Among the items found on the ship were six C-704 missiles ready for launching, two launchers, and two radar systems. In November 2009, the *Francop*, which carried a large shipment of weapons from Iran to Hizbollah, was seized. One month prior to that, the Maltese authorities, at the request of the United States, confiscated the cargo of the Hansa India, a German-owned merchant ship that was also transporting weapons from Iran to Syria. In August 2010, another shipment of arms from Iran to Syria, apparently intended for Hizbollah, was discovered. The shipment left a port in Iran disguised as a cargo of powdered milk. When the ship stopped in Italy, the container aroused suspicion, and in the course of an inspection carried out by the Italian police, a cargo of seven tons of explosives for missile and rocket warheads was discovered.

The foreign media have reported that since 2009, Israel intercepted convoys of weapons and ships transporting weapons to and from Sudan. The cargoes were transported on the Iran-Sudan axis through Oman and Saudi Arabia, and on the Syria-Sudan axis through Jordan and Egypt. In recent years, relations between Iran and states in the Horn of Africa have grown closer; Iran has sought in this way to establish a military presence along the shipping lanes in the area. Thus, for example, Iran established a naval port on the coast of Eritrea in the port city of Assab for the use of Revolutionary Guards personnel. In general, the Iranians have encountered difficulties in transferring shipments of weapons to Hamas through the Red Sea and Sudan, and from there, to the Gaza Strip through the Sinai. This is because of increased international monitoring of the movement of ships from Iran. It is little surprise, therefore, that in October 2010 the Nigerian security forces announced that during an inspection of the cargo of a ship from Iran that had docked in a Nigerian port, several tons of weapons were discovered, disguised as a shipment of building materials. In January 2009, authorities in Cyprus confiscated weapons and equipment for manufacturing weapons originating with the Iranian military industry, sent on the Russian ship *Monchegorsk*. Previously, ships from the US Fifth Fleet had stopped the *Monchegorsk* on the Red Sea,

but since it was registered in Cyprus, they did not conduct searches and asked the Cypriot authorities to do so.

In April 2012, the German-owned ship Atlantic Cruiser was stopped in the Mediterranean Sea. Large quantities of arms were found on the ship, which was apparently headed for the port of Tartus in Syria. The ship ultimately docked in Turkey.[19] Moreover, even the government of Yemen claims that Iran is making use of the naval medium in order to transfer ammunition to the Shiite rebels in northwest Yemen. The fighting in this region has expanded in recent years and includes direct military operations by Saudi Arabia – including at sea – through a partial naval blockade, whose purpose is to prevent weapons shipments from reaching the rebels.[20] These interceptions appear impressive, but the common assessment is that this is the tip of the iceberg of the Iranian activity. Yet even if these seizures cannot significantly change the next battle, they can embarrass Iran and reveal its intentions. However, the effort does not always produce results. Thus, for example, in April 2012, the Israeli Navy stopped the merchant ship *Beethoven*, which was flying the flag of Liberia. The forces boarded the ship at a distance of 300 kilometers from Israel's coasts, when it was on its way south in the direction of the Gaza Strip, but they discovered that there were no weapons on it.[21]

Notes

The author would like to thank Maj. Gen. (ret.) Avihai Mandelblit for his assistance with this article.

1 Yaakov Katz, "Navy in Gaza: Guardians of Israel's Border," *Maariv NRG*, January 9, 2009.
2 "U.S. Senator Calls for Naval Blockade of Iran," *Haaretz*, March 10, 2012.
3 Flavia Krause-Jackson and Tal Barak Harif, "Massive Blockade Needed to Stop Iran Threat, Israel's Steinitz says," *Bloomberg*, January 25, 2012.
4 Ben Caspit, "Israel to United States: Impose Naval Blockade on Iran," *Maariv NRG*, March 11, 2010.
5 See also "Making the Naval Blockade Accord with International Law: The Legal Framework," Turkel Commission Report, State of Israel, The Public Committee to Examine the Maritime Incident of May 31, 2010, pp. 36-42.
6 David Friedman, "Preventing the Proliferation of Biological Weapons: Situation Overview and Recommendations for Israel," *Strategic Assessment* 7, no. 3 (2004): 24-30.
7 Turkel Commission Report, pp. 52-53.
8 "Iran Vows Firm Response to 'Illegal' Resolution 1929," *Tehran Times*, June 19, 2010.

9 Emma Belcher, "The Proliferation Security Initiative: Lessons for Using Nonbinding Agreements," Council on Foreign Relations Working Paper, July 2011.
10 Amitai Etzioni, "Tomorrow's Institution Today," *Foreign Affairs* (May/June 2009).
11 Ephraim Asculai, "International Nuclear Nonproliferation Agreements: Current Status and Future Prospects," in Emily B. Landau and Tamar Malz-Ginzburg, eds., *The Obama Vision and Nuclear Disarmament*, Memorandum 107 (Tel Aviv: Institute for National Security Studies, March 2011), pp. 71-86.
12 Amos Yadlin and Yoel Guzansky, "The Strait of Hormuz: Assessing and Neutralizing the Threat," *Strategic Assessment* 14, no. 4 (2012): 7-22.
13 "Iran Plans Oil Export Terminal outside Gulf," *al-Arabiya*, May 22, 2012.
14 Barak Ravid, "Rockets from Iran Seized in Nigeria, Apparently on the Way to Gaza," *Haaretz*, October 28, 2010.
15 Yoel Guzansky, "The Naval Arena in the Struggle against Iran," INSS *Insight* No. 146, December 3, 2009.
16 Survey of the Meir Amit Intelligence and Terrorism Information Center (at the Israeli Intelligence and Heritage Commemoration Center), March 17, 2011.
17 "UN Report: Partial Blow to the Iranian Nuclear Program," *Ynet*, May 16, 2012.
18 Survey of the Meir Amit Intelligence and Terrorism Information Center (at the Israeli Intelligence and Heritage Commemoration Center), March 7, 2011.
19 "Report: German Arms Ship Stopped on Way to Syria," *Ynet*, April 14, 2012.
20 Eric Schmitt and Robert Worth, "With Arms for Yemen Rebels, Iran Seeks Wider Mideast Role," *New York Times*, March 15, 2012.
21 Amos Harel, "Navy Stops Ship in Mediterranean on Suspicion that it was Carrying Weapons," *Haaretz*, April 22, 2012.

Call for Papers

The Institute for National Security Studies (INSS) at Tel Aviv University invites submission of articles for publication in *Military and Strategic Affairs*, a refereed journal published three times a year in English and Hebrew and edited by Gabi Siboni, Director of the Military and Strategic Affairs Program and Cyber Warfare Program at INSS.

Articles may relate to the following issues:

- Military and strategic thinking
- Lessons learned from military organizations throughout the world
- Military force developments, including: human resources, weapon systems, doctrine, training, command, and organization
- Ethical and legal aspects of war and combat
- Military force deployment and operations
- Civil-military relations and decision making processes
- Security/military technology
- Cyber warfare and critical infrastructure protection
- Defense budgets
- Intelligence

Submitted articles should not exceed 5500 words (including citations and footnotes). Previous issues of the journal may be accessed on the INSS site at: http://www.inss.org.il/publications.php?cat=68&incat=&read=3579.

Daniel Cohen
Coordinator
Military & Strategic Affairs Program
Cyber Warfare Program
Tel: +972-3-6400400/ext 488
Cell: +972-50-5772338
danielc@inss.org.il