Military and Strategic Affairs

Volume 6 | No. 1 | March 2014

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

ISSN 2307-193X (print) • E-ISSN 2307-8634 (online)

Military and Strategic Affairs

Volume 6 | No. 1 | **March 2014**

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 a refereed journal 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.

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

The Institute for National Security Studies (INSS)
40 Haim Levanon • POB 39950 • Tel Aviv 6997556 • 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

ISSN 2307-193X (print) • E-ISSN 2307-8634 (online)

In Retrospect: The Second Lebanon War

Ehud Olmert

The processes that led to the Second Lebanon War and the events that took place during the war are analyzed six years after the war. The starting point for the analysis is the withdrawal from Lebanon in 2000, which, according to the analysis, was justified. However, from a broad perspective, it is evident that the overall processes since the withdrawal led to strategic choices that resulted in the IDF's reduced operational preparedness. The article examines the decision making processes near the start of and during the course of the war through a review of the IDF's main operational activity during the war. In addition, it describes the political moves during the fighting and at its conclusion. Finally, there is an analysis of the campaign's achievements and the main lessons derived from it.

Keywords: Second Lebanon War, Lebanon, IDF, strategy, Hizbollah

It is an overstatement to call the military effort undertaken by Israel in Lebanon during the summer of 2006 a "war." The events known today as the Second Lebanon War did not actually begin on July 12, 2006; they began on the day the State of Israel decided to adopt a policy of containment in response to the kidnapping and killing of its three soldiers in 2000 – when it threatened to make the ground shake in Lebanon but then did nothing. In fact, the Second Lebanon War began when Israel lost its deterrent capability; when it failed to act, explicitly contradicting its commitment to do so; when it decided to accept a situation in which the other side chose the timing, the scope, and the manner in which to drag Israel into a situation where it was forced to react rather than dictate. This was the state of affairs for six years after October 2000.

Ehud Olmert was the Prime Minister of Israel during the Second Lebanon War. This essay is based on his lecture "The Second Lebanon War: The Test of Time," delivered at the INSS conference "The Lebanon Wars and Israel's Security Concept," July 12, 2012.

This article will address only the military aspect of the campaign in Lebanon in 2006, from a six-year perspective. Firstly, it should be emphasized that the withdrawal from Lebanon in May 2000 was justified. I differ on this matter with my friend Effi Eitam – a great soldier, but one who is happy with our presence in territories that are not part of the State of Israel and do not contribute to its international legitimacy, although this legitimacy is necessary and essential in order to realize Israel's strategic interests. This happiness is not part of my worldview and was not part of it when I was Prime Minister. Thus, the decision to withdraw from Lebanon was correct and justified, and although the manner in which we departed may be questioned, it is beyond the scope of this discussion. After withdrawing from Lebanon, for six years Israel closed its eyes to the situation forced upon it on the northern border. Not only did it refrain from responding to events and act, or fail to act, in direct contradiction to threats issued by officials who set Israel's policy goals; it also diverted the vast majority of security operations and military preparations to combat in another arena, with other tools and other methods, regardless of the clearly predictable security and military needs that would ultimately be imposed on us on the northern border.

The lack of operational preparedness as reflected in certain events during the Second Lebanon War resulted from a deliberate strategic preference – and it no longer matters who made this decision, nor will I engage in accusations or assign responsibility. This strategic preference was manifested by the IDF's failure to prepare as necessary, in terms of training and capabilities, to provide effective responses at the right time and in the right context during the Second Lebanon War.

Even before January 2006, I was a member of the security cabinet and, in that capacity, of the small team of ministers addressing the issue and arena of Lebanon. Beginning in January 2006, the question of Lebanon became an integral part of my agenda. To the best of my understanding and knowledge, having also examined the archives, no measure taken during the six years prior to 2006 compares to the measures taken during the six months after January 8, 2006 – in terms of focused assessment of the situation in Lebanon, the feasibility of operating there, and the need to address the emerging situation. On that date, I held my first meeting with a team of senior advisors, including then-Chief of Staff Lieut. Gen. Dan Haloutz, in order to discuss what we could and should do, given the

assessment that there was very little time before we would be challenged in the north. According to the situation assessment, we were progressing toward a conflict on the northern border, and the question was whether, under the circumstances, we should continue the policy of containment that had been in place for six years, or whether we should change this policy, taking into account that doing so would drag us into a violent conflict and state of friction with the opposing forces. Without exception, the position of all those in the military leadership – from the Chief of Staff, to the head of Military Intelligence, to the head of Military Intelligence's Research Division, and all other officials – was that we could not maintain the policy of containment. This was also the view of the General Security Services (GSS), the Mossad, and all the other advisors. The salient position, including of the Chief of Staff, was that if we were attacked in the north in accordance with Hizbollah's regular pattern – that is, kidnapping of soldiers and firing of rockets against towns on the northern border – and we failed to respond, then Israel would suffer strategically very much, worse even than if the regime in Syria changed unexpectedly. Then-head of Military Intelligence (today the Director of the Institute for National Security Studies) has said similar things, and when the Second Lebanon War broke out, he stated that the kidnapping incident on the northern border, which led to the war, was the result of a failure to address the abduction of the soldiers on the same border in October 2000. In other words, the position of the officials to whom we can listen and from whom we can learn – those who have the information and who deal with the issue of Lebanon on all levels and from all directions – was uniform: we would have to operate according to an entirely different model from the one applied during the six years after October 2000 and, in effect, since we left Lebanon in May of that year.

I too took the position that there was no option but to change the rules of the game, and not only was there was no alternative but that it was nearly certain this would happen. Accordingly, I instructed military officials to take all precautions and prepare as best as possible to prevent a situation in which we would have no choice but to respond more forcefully than before under comparable circumstances, but of course to be ready to act if such a situation in fact developed. I remember my warning – one of many – in one of the preliminary discussions, when I said, "In the end, from one person's blunder, Israel is entering a strategic tailspin."

On the day in June 2006 of Gilad Shalit's abduction on the southern border and in the days that the followed, we held a series of discussions in which the salient question was not what happened at that border, rather, what is expected to happen on the northern border. The army was requested and explicitly instructed by the political leadership (by me and by the Defense Minister, whose actions were responsible, restrained, level-headed, measured, and impressive) to be on the highest level of alert along the northern border to prevent the possibility that the blunder I mentioned would occur: a kidnapping that would lead to events such as those that ultimately did transpire. I remember that we were curious about whether the model of a tunnel, as it existed in Gaza, was possible on the northern border, and the answer from defense officials was that the possibility always existed, but the likelihood was very low. In the end, the event that took place in July 2006 on the northern border was not the result of an operation using the tunnel model, but the classic model that Hizbollah has used throughout the years. Unfortunately, we fell into this trap, in spite of the orders to be on high alert to prevent precisely such an incident. To a certain extent, the events that led to the outbreak of the war may be attributed to a failure to carry out the order conveyed through the military high command, in accordance with a directive from the political leadership, to make every effort to avoid a particular situation that would lead to an inevitable development. This order stemmed from our rational and agreed assessment that if such a situation emerged, we must change our manner of response, meaning that we had no intention of continuing the policy of containment.

One of the arguments I have heard in retrospect from various individuals – in contrast to what they said at the time – is that when the kidnapping on the northern border took place, we should have taken time out in order to consider our response. In fact, during the six months preceding the kidnapping, we had been thinking about what to do if such an incident took place. There is no need to elaborate on what we all well know – that if one does not respond when the provocation occurs, one loses legitimacy. Legitimacy for the type of operation that can be launched close to the time of the provocation is lost within two to three days.

Some of those officials from the period of the Second Lebanon War subsequently changed jobs but remained within decision making bodies. At that time we had to prepare a possible response to the missile fire from

the Gaza Strip. It was clear even then that a response – which ultimately emerged as "Operation Cast Lead" – was only a matter of time, and we would have no choice but to act because we could not continue to live with constant, daily containment of missile fire against Ashkelon and the communities, kibbutzim, and development towns in the south, especially when this fire could reach Ashdod and Beersheba as well. The question, therefore, was when to respond. The answer was as soon as the first missile strikes Ashdod we must start to act. I recall that during this discussion, I pounded hard on the table and responded to these comments by pointing out that we had waited several years to hear this, and from the very same people who had said on the eve of the Second Lebanon War that we should take a time out, as if the other side were giving us such a time out for thinking! Indeed, sometimes the way one views a course of action changes, especially when one sees things from a different place and a different angle. In any case, during countless deliberations we discussed the possible model of response in the event that what did actually happen were to happen on the northern border, so that we would not need to take the time out in order to consider how to proceed.

One of the first pieces of advice, or more accurately, the first positions presented to me by the military leadership about responding to an incident on the Lebanese border – and in this regard, it is clear that the military leadership is ultimately included in the positions expressed by the Chief of Staff – was not to draw a distinction between Hizbollah and the Lebanese state, but to regard the Lebanese state as a target for response and, therefore, to strike its national infrastructures by means of a quick, destructive, and very short operation. My main disagreement with the Chief of Staff was on this issue, and it remains so to this day. I believe that then-Chief of Staff Dan Haloutz maintains the same position on this issue even today. In his book, he explained and elaborated on his stance, but even after following his explanation I did not agree with him, nor do I agree with him today. This is a good example of the gap between the positions of the operational military leadership and those of the political leadership. Naturally, under the circumstances, the latter has a broader picture of the world. Although I do believe that Lieut. Gen. Haloutz's world view is very broad and comprehensive, by virtue of his position as Chief of Staff, and under the circumstances at the time, his perspective has been

limited to what appears to him to be critical at that moment, while the political leadership must see the bigger picture.

One of the most important elements that must be understood – and I say this not only in retrospect about the Second Lebanon War, but also to invite thinking about what some people want to see happen in the future – is that Israel is a strong country with tremendous power. We have tools that few states have. We have capabilities that few countries in the world have. However, we cannot take action unless we also establish a broad foundation of international legitimacy. Anyone who thinks that we can act without international legitimacy has a faulty perception of reality and understanding of Israel's status, position, and relationships. One source of satisfaction in relation to the Second Lebanon War is that although our military action included heavy shelling and bombardment – which inflicted pain and loss and affected the way of life of civilian populations on a huge scale, causing some one million people in Lebanon to leave their homes and go north – the international community stood behind us. This support did not emerge by chance. It was created because we knew how to secure international legitimacy, which gave us the backing to carry out our action.

What would have happened had we attacked Lebanon's infrastructures at a time when the Western world, first and foremost the United States and Europe, believed that there was a chance of cooperating with the Siniora-Hariri government in a way that would change the situation, and demonstrated true concern for it and for its future? It is very possible that the war would have ended within forty-eight hours and Hizbollah would have continued to fire missiles, harass the northern border, and disrupt the way of life of the entire population in Israel's north. In my opinion, the decision we made not to attack Lebanon's infrastructures was correct and responsible. It reduced – although it did not eliminate – the possibility that the entire population of Lebanon, including its Christians, would become Israel's mortal enemies forever because we had equated all of them with Hizbollah. Bombing Lebanon's infrastructures would have been a mistake, and I am happy we were not dragged into such action.

Another issue that should be addressed is the question of a ground operation deep into Lebanese territory. On this matter, my position and that of the Chief of Staff were identical from the outset, and Defense Minister Amir Peretz, whose actions during this war justified my confidence in him, agreed with us. Our position was that we were not interested in a

ground penetration deep into Lebanon because we realized that the days of entering and occupying territory with ground forces for the sake of deterrence or prevention of harm to the population are past. I say this as a person who over the years, even before I served as Prime Minister and certainly during my term in office, developed a more balanced perspective toward the possibilities, the needs, and the preferences of a country on Israel's scale. If you do not understand this point, you do not understand a very fundamental component of our ability to conduct Israel's military and defense affairs in a way that is balanced, responsible, cautious, and smart. Nevertheless, I should note – and I am in full agreement with Lieut. Gen. Haloutz's angry remarks in defending himself when he was attacked for allegedly telling the cabinet that we should rely solely on airpower – that during a July 12 cabinet meeting, when the Chief of Staff was asked what would be considered a victory in the process recommended by the army, which in turn I recommended that the cabinet adopt, he answered: "There will be no knockout here . . . If anyone expects that they will raise white flags and we'll end the war that way, that isn't going to happen." What the Chief of Staff said, which I also thought was correct, is that we must create such military pressure that ultimately, in as short a process as possible, it leads to international intervention, thereby altering the situation existing on the Lebanese border since 2000 and achieving the goals adopted by the cabinet and issued in a public announcement following the meeting on July 12.

There was one objective that we did not achieve, which we knew in advance we would not achieve, having discussed it as well in the cabinet meeting. We announced, inter alia, that we were working to bring about the release of the two kidnapped soldiers. We did not say they were murdered, although even then we had almost no doubt that they had been. In case there was even a 1 percent chance they were alive, we did not want to raise the possibility of Hizbollah murdering them lest it then turn this possibility into fact. Furthermore, we concluded at the cabinet meeting that there was no chance of rescuing the soldiers in a military operation. Nevertheless, the government could not announce its objectives in launching such an operation without mentioning the two kidnapped soldiers. It cannot bring about an international operation placing pressure on all actors in Lebanon, without itself declaring that the liberation of the soldiers is an objective. The fact that this declared goal was not achieved is sometimes brandished against the government. I am amazed when I see people

writing, responding, and arguing about matters that were published and are publicly known, but because they do not conveniently fit into a thesis or a conception, they are ignored. Accordingly, I would like to reiterate the following point: sometimes objectives are announced because they are part of the relevant context of a struggle that combines military action, diplomatic moves, and explanations, even though it is known in advance that they are not likely to be achieved.

The main undertaking during the first phase of the campaign was the aerial effort, which resulted in remarkable achievements. It infuriates me to hear certain people say that the Israel Air Force and the Chief of Staff think that "everything is the air force." To this I reply that in the future battlefield those in charge of all the military systems will fall under the air command of the State of Israel, and their role, their weight, and their scope will exceed all the other elements. The entrenched, conventional, and dogmatic approach regards war as entailing a thousand tanks bursting forth across enemy lines – because once it was customarily believed that war must be shifted to the enemy's territory – then conquering it and seizing control over it, and therefore, according to this view, only an infantryman knows how to wage war. This approach is valid only for a ground battle. The best man will know how best to synchronize the various components of a modern war in the future battlefield. Such a person can be in either the ground forces or the air force, and on this matter, neither one is better than the other.

As noted, the first operation of the Lebanon campaign in 2006 achieved great success – striking targets selected by the army, using mainly aerial capabilities and other precision weapons in our possession, which were operated wisely, diligently, resolutely, precisely, and unhesitatingly. This opening operation deeply shocked and unnerved Hizbollah officials.

The second effort we sought to undertake was on the ground. It was on the first Saturday night of the war. We flew to the Northern Command, and I personally instructed the OC Northern Command to "clear" the territory up to a depth of three kilometers from the border. This meant that we would not enter Lebanon – not reach the Litani River, not reach the Awali River, and certainly not north of that. One of the IDF generals on whose abilities, talents, and achievements there is general agreement, told me two years later that he thought, as did the Chief of Staff and I, that had we decided then to enter deep into Lebanese territory we would have still been fighting there. The desire to enter territories where there is no need to

be is a drive that should be restrained, and in fact, we did enter the battle in Lebanon with restraint in this regard. The decision to clear an area of three kilometers stemmed from the desire to prevent a daily threat from light weapons, which could have made the life of those living along the border impossible. Once they cannot be threatened with such weapons, the security situation improves, and soldiers patrolling the border cannot be abducted. This was the optimal ground objective, and no more.

It turned out that a considerable number of the failures in the use of forces in Lebanon were within limited range and were not a result of an extensive, large scale, dramatic military ground operation. These were tactical failures that require us to learn lessons and draw conclusions. In fact, an enormous effort was made in this regard after the war. However, these failures do not overshadow the significant achievements of the overall effort in the Lebanon campaign, which resulted from the correct combination of the military effort and the political effort.

As mentioned, we sought international legitimacy for the operation in Lebanon. Not only did we receive it, but we were not pressured, even by the Americans. I cannot recall when or whether any defensive military operation along these lines in Israel's history resulted in less pressure from any international player, especially the most important player in our view, the US government. Moreover, despite the rumors and published reports, I did not speak with President Bush during the war even once. The only conversation we had was on the Friday on which the Security Council passed a ceasefire resolution. Prior to that, we had reached a final agreement on the draft resolution through phone calls with the president's National Security Advisor and his Secretary of Defense, and we went over every word and every comma. Only later, long after midnight, did President Bush call me, saying he had not wanted to call earlier because he realized that I needed the time to do as I saw fit. It is no trivial matter to hear such things in the context of a relationship with the country most important for our security and our existence.

We did not intend and we did not wish to extend the ground operation in Lebanon beyond the narrow sector that we considered important for achieving our goals – very significant goals from the perspective of the civilian population in the north of the country. In addition, we conducted military maneuvers that created the pressure that ultimately led to activity by the international community. This activity enabled us to achieve the

goal of placing an international military force in southern Lebanon, which significantly changed the security situation that had existed there for six years. All the conditions for achieving this objective emerged after two and a half weeks of fighting, a very reasonable amount of time according to all those involved.

On July 29, 2006, in a conversation in my home with the US Secretary of State, we agreed on the details and drafted a resolution to be put to a vote in the UN Security Council three days later, after she had presented it to Lebanese Prime Minister Siniora and the draft was finalized. Then, as sometimes happens, an incident occurred: the IDF shelled a multi-story building in Kafr Qana in southern Lebanon. As a result of this incident, Lebanon presented a dramatic picture of a terrible disaster in which one hundred civilians were killed, mostly women and children. The Lebanese reaction created a strong impression in world public opinion, to the point that for the first time since the start of the campaign we thought we had to defend ourselves against it. Given the situation, the President of Lebanon also asked the US Secretary of State not to come to Lebanon. Thus, the timetable that would have allowed us to end the fighting two and a half weeks earlier than it actually ended was disrupted. This was a turning point that in turn disrupted the overall course of events. Eventually we realized, as did the Americans, that we had to find a way to enable the resolution to be passed in the Security Council and, to this end, to secure the consent of the Lebanese sovereign, i.e., the government of Lebanon, to the stationing of international military forces in southern Lebanon. We found a way to do this, and the United States resumed negotiations with all those concerned.

Thus we advanced toward Wednesday, August 9, the day on which the political- security cabinet met. The issues on the agenda were, on the one hand, the possibility of implementing the proposal that was intended to provide a long term solution to the security situation in southern Lebanon, and on the other, the possibility that passage of the resolution would be delayed and that further debates and discussions would be needed before it was finalized. During that cabinet meeting, I was surprised by a telephone call from the US Secretary of State, who asked to speak with me directly. I assumed that she wanted to influence the cabinet discussion, especially in light of the rumors that had begun circulating among the public and in the international media to the effect that Israel was planning a large scale ground campaign in southern Lebanon. Instead, Condoleeza Rice told me

explicitly that the United States accepted Israel's position and would do what was necessary to bring about the stationing of a NATO intervention force with 12,000 soldiers in southern Lebanon, and that it would present a draft resolution on the matter to the Security Council that evening or the next day. After this conversation, the cabinet decided to authorize me and the Defense Minister to decide whether or not to engage in a more extensive operation in Lebanon, of course taking into account developments related to the Security Council resolution.

On that occasion and on others as well, the Americans asked us how much time we would need to bring hostilities to an end once the Security Council resolution was passed. Israel's answer then was ninety-six hours. This answer was based on experience and on the understanding that we could not know in advance whether passage of the Security Council resolution would coincide with an optimal situation with respect to the troops on the ground or whether we would need more time to improve it. It was also unclear whether the other side would accept the resolution and cease fighting.

While at that stage the IDF wanted to enter into a ground operation in Lebanon, we in the government saw this operation only as a means of applying pressure, not as a strategic shift toward territorial occupation. By increasing the pressure, we intended to lead the international community to adopt a resolution that we expected would yield the results necessary for achievement of the objectives we had set for the war. At that point, the Chief of Staff told me that soldiers had been deployed on the ground and that there were division commanders pressing to enter Lebanon. I spoke with the commanders, I explained my position to them, and I added that I was proud of the soldiers and commanders who wanted to enter Lebanon, but that the political leadership has a broader view, which includes additional considerations that it must weigh, and it is the leadership that will decide if and when to act.

It is important to understand that entering Lebanon requires several hours of mobilization. Thus, to do so when darkness falls on Thursday requires making a decision at noon or in the early afternoon on that day. But it was not possible to make such a decision because passage of the Security Council resolution was on the agenda for that same night, and we had reached understandings with representatives of the Secretary of State, almost to the last detail. Late in the hours between Thursday and

Friday, a message arrived from a very senior US government official, conveyed to us by our UN ambassador, Dan Gillerman. The message said that a completely different resolution, initiated and drafted by France, was going to be presented to the Security Council, and that the United States was unable to withstand the pressure applied by France. When we examined the sequence of events, we reached the conclusion that the only way we could alter their course was to have the more extensive IDF action in Lebanon appear to be factually underway, thereby exerting the necessary pressure on the actors in the international arena. The attempts we made on Friday morning to contact someone from the American team were in vain; they were all asleep at that hour (10 A.M. in Israel and 3 A.M. on the East Coast in the United States), and of course, we could not wake the Secretary of State or the President. Therefore, everything ultimately came down to a point in time in which, if we had postponed the decision on expanding the operation, there might very well have been insufficient pressure to pass the resolution in the form that we had been discussing all along with the United States. This could have resulted in a different resolution being passed that was contrary to our interests, which we would not have been able to accept and would have had to oppose. These are the circumstances that led to the operation that comprised the final forty-eight hours of the war.

The Chief of Staff of that time would testify that the IDF received approval to begin the ground effort only, and that the first question he was asked was how many hours he needed in order to terminate the operation once he received the order to do so. The Chief of Staff replied that he would need from eight to nine hours. These facts indicate that here too, from the outset, there was no intention to change strategy, but only to create the conditions that would lead the international community to finalize a Security Council resolution along the lines we considered appropriate.

When morning arrived, we managed to reach the US Secretary of State, the National Security Advisor, and President Bush at his ranch in Texas. In a conversation with the National Security Advisor, it became apparent that there had been a misunderstanding and that the French draft resolution was not the correct draft. We began once again to review the wording of the original resolution, and we reached agreement on a new version that was slightly less precise than the agreement we had had before the incident in Kafr Qana on July 29, but that still accorded with the basic parameters we

sought. As a result, it was decided, in coordination between me and the Secretary of State and the UN Secretary General, that the resolution would enter into force within sixty hours – the length of time the IDF had told us it would need between passage of the resolution and implementation of a ceasefire.

Looking back after six years at the results of the Second Lebanon War, we see first grade children in Kiryat Shmona who have never sat in bomb shelters. Before 2006, northern Israel had not known such quiet, even among the parents of that generation's soldiers. During the preceding decades, residents of the north had spent much time in shelters. There is no doubt that the effort we invested in Lebanon in the summer of 2006, which was restrained relative to the demands or expectations some people had of placing IDF troops in all sectors on a large scale, created a state of deterrence that had never before existed along the Lebanese border, with the possible exception of the years preceding the Six Day War. I do not accept the argument that the Second Lebanon War generated a state of mutual deterrence. Since then, we have undertaken whatever action we wanted in the northern arena without being even momentarily deterred by the possibility that matters would escalate to a point where Hizbollah was firing on us. Hizbollah's supposedly highly resourceful leader, who is still living in his bunker, testified to this when he stated that had he known we would respond in such a way to our soldiers' abduction on the northern border, he would not have acted as he did.

The media lost its sense of proportion and, alongside political figures with vested interests, sought to prove that Israel had failed in the Second Lebanon War. These claims encouraged Hizbollah's leaders to ask why, if the Israelis themselves admit defeat, they should believe otherwise. Nevertheless, they have not ceased to fear the long arm of the State of Israel, and in the six years that have elapsed since the war, they have not taken action against us. When rockets were fired from Lebanese territory on three occasions – and we know with certainty that whoever fired them has no connection to Hizbollah – the instinctive response from the organization's leadership was to make sure we were informed that they were not responsible, in the hope Israel would not strike back at them. Accordingly, it is safe to conclude we succeeded in creating a strong state of deterrence as a result of the Second Lebanon War.

Anyone who thinks Hizbollah will never use its stockpiles of weapons, including missiles, and will not fire from the north, or will not fire on Israel from the south or from Syrian territory, who claims Israel can do whatever it wishes, including occupying territories, and that all of those around us will sit quietly without responding, is mistaken and is misleading others. The arena around us will not be quiet forever, especially if we attempt to change the equation through operations that are outside the usual range of expectations. In this context, it should be emphasized that our enemies' ability to influence our way of life in Israel will be judged not in the number of missiles they have but in their desire to make use of them. This is where our deterrent capability serves us.

As for Syria, even if the Syrian President's days in office are numbered, we must remember that since 1974, as a rule there has been quiet along our border with Syria, and neither the government of Hafez al-Assad nor that of Bashar al-Assad changed this situation, even when events unfurled touching upon us and the Syrians: during the Second Lebanon War, when Syria did not respond, and afterwards as well, when Imad Mughniyeh, Hizbollah's special operations chief, was killed in Damascus. The Syrians believed they knew who was responsible, yet they have not responded. Furthermore, they know of other operations that have not been revealed in the media, and they have not responded to those either. The reason for this is the deterrence we created!

It would be wrong to claim the Second Lebanon War did not include any errors or failures. I would be the last to make such a ridiculous assertion. Even the Chief of Staff said there were failures in carrying out military operations and we were not fully prepared, although I was never told the IDF was not capable of carrying out all the tasks required of it. In fact, the opposite was the case. Indeed, there were failures in various operations during the Second Lebanon War, such as in Bint Jbeil and Maroun al-Ras. It is impossible to overlook these failures, and we have not ignored them. We learned from the failures and drew the necessary conclusions. In this context, we examined the origins of the disparagement that caused the problems we encountered in Lebanon, and of the exclusive focus on the war on terror, which disrupted the internal balance in the military.

In spite of the failures, during the Second Lebanon War, for the first time, we conducted an integrated campaign, exceptional in its scope, intensity, and success. We did this by means of what we can call a strategic staff,

which combined all the responsible bodies – the IDF, the other security agencies, the foreign policy bodies, and ultimately, the Prime Minister, who is responsible for all these bodies together. This staff met every day, together with the National Security Staff and all other relevant bodies, and was headed by the Prime Minister's Chief of Staff and his political advisor. Military personnel received all the relevant information and prepared working papers that suggested options and formulated proposals for decision makers. This is one of the only points on which the Winograd Commission understood things properly, as reflected in its praise for the work of the strategic staff in its second report. In other words, despite the claims there was no integration or coordination between military operations and diplomatic activity, in fact, the commission's second report greatly praised this coordination, the scope and intensity of which were unprecedented.

Many lessons were learned from the Second Lebanon War, including about home front preparedness. The government that I headed adopted the necessary changes indicated by those lessons, made the appropriate decisions, and allocated the necessary resources in order to allow these changes to take place. In addition, we drew the correct conclusions about priorities in procuring weapons, which in our opinion are relevant to the type of threat that will confront us in the future.

The future battlefield will be within cities, not along a line hundreds of kilometers from our homes. Anyone who thinks that in order to better protect Israel's security we must conquer another thirty kilometers eastward or northward is making an ignorant assumption that our enemies will not be able to develop or acquire a rocket reaching Israeli population centers, irrespective of the depth of our presence within enemy territory. We must build our capabilities not in order to conquer territories, but to create deterrence by using special offensive tools that are relevant to the current types of threat while working within the boundaries of international legitimacy, which as noted, is a crucial element of Israel's security structure. If we know how to create deterrence correctly, to allocate resources appropriately, and not to waste billions for purposes that are ostensibly strategic but in fact constitute a complete waste of funds that could have been spent on Israel's critical needs, we will achieve our objectives.

The government that I had the privilege of heading made no less of an effort than other governments to reach peace settlements with the

Palestinians and with Syria, two endeavors that were both correct and justified, in their time and their scope. At the same time, the government I headed struck at those who threatened our security, with greater force and determination than Israeli governments in the past thirty years. On the basis of this experience, it may be asserted that what is required of us is action that is more intelligent, more cautious, and more proportionate regarding investment of the necessary resources in order to be generally prepared for the threats we anticipate. These resources exist, but some are wasted and some must be allocated to the address of other problems related to strengthening Israeli society – education, welfare, and additional issues not traditionally defined as security issues. We must continue to do so, and in particular we must bear in mind – and this is my most important point, one I often reiterate – we are a very strong state and we know how to mobilize the international community for objectives we consider critical for survival, especially those in the international community who support us, who are committed to ensuring our needs, and who provide us with tools crucial for our existence. We must continue on this path so as not to separate ourselves from the international community, which is important to the success of our struggle and to achievement of the goals we set for ourselves.

Nuclear Weapons in Asia: Perils and Prospects

Stephen J. Cimbala

The spread of nuclear weapons in Asia threatens nuclear deterrence and crisis stability in the region and offers unique challenges to United States and allied security. The article contrasts two possible futures for nuclear Asia: a relatively more constrained proliferation regime with tiered levels of agreed deployment ceilings among states; and an unconstrained nuclear arms race in Asia. Not only regional tensions, but also the overlap between regional and global antagonisms and ambitions might upset nuclear deterrence stability in Asia.

Keywords: Deterrence, nonproliferation, missile defense, coercion, China, Russia, Japan, Iran, Pakistan, India, North Korea, South Korea, United States

The Obama administration has refocused its military-strategic priorities towards Asia, as well as portions of the Middle East within geostrategic reach of Asia. This refocus in US strategic planning and deployment is not only driven by China's rise in economic and political influence, but also by the growing risk of regional nuclear arms races that could lead to increased political tensions, and in the worst scenario, the outbreak of a nuclear war. The spread of nuclear weapons in Asia not only raises the likelihood of wars between states with weapons of mass destruction, but also increases the likelihood of nuclear handoffs to terrorists or other non-state actors dissatisfied with the existing international order.[1] In addition, a nuclear conflict between two large states in Asia, such as India and Pakistan, has the potential to escalate into a wider regional war with potential global consequences.[2]

Dr. Stephen J. Cimbala is a professor of political science at Pennsylvania State University.

As military planners project toward the third decade of the twenty-first century, the political context for current and future Asian nuclear arms competition is clearly different from the political context that surrounded US-Soviet Cold War rivalry. Therefore, disciplined conjecture about the likelihood of deterrence, crisis, and arms race stability in a future nuclear Asia is both timely and prudent.[3] The present study considers pertinent policy challenges to nuclear strategic stability in Asia and analyzes some options for more or less stable configurations of Asian nuclear weapons states.

Nuclear Proliferation: Yes or No?

United States policy has supported the Nuclear Non-Proliferation Treaty (NPT), requiring non-nuclear state signatories to the treaty to abjure the option of nuclear weapons. Under the NPT regime, non-nuclear states have the right to develop a complete nuclear fuel cycle for peaceful purposes, for example, generating electricity. States adhering to the NPT are required to make their facilities and infrastructure available for scheduled or challenge inspections by the International Atomic Energy Agency (IAEA). The IAEA has a mixed track record: depending on the cooperation or resistance of the regime in question, inspectors have obtained accurate roadmaps of countries' nuclear programs or they have been misled. In Iraq, for example, regular IAEA inspections prior to 1991 failed to detect the complete size and character of Saddam Hussein's efforts to develop nuclear weapons.

US intelligence has also performed erratically in ascertaining the extent of WMD-related activity, including nuclear activity, in potential proliferators. The CIA assured President Bush and his advisors that the presence of large quantities of WMD in Iraq in 2003 was a foregone conclusion, but no WMD were found by inspectors after the completion of Operation Iraqi Freedom and the ousting of Hussein from power. The CIA was apparently taken by surprise in 1998 by India and Pakistan's nearly simultaneous detonations of nuclear weapons, followed by announcements in New Delhi and Islamabad that each was now an acknowledged nuclear power. In yet another instance, the US government signed an agreement with North Korea in 1994, freezing North Korea's nuclear development programs, but in 2002 North Korea unexpectedly denounced the agreement, admitted it had been cheating, and marched progressively into the ranks of nuclear weapon states.

The possibility of nuclear material or technology finding its way into the hands of terrorists is a concern that provides further incentive for containing the spread of nuclear weapons and delivery systems. Reportedly, al-Qaeda has tried to obtain weapons-grade material (enriched uranium and plutonium) and assistance in assembling both true nuclear weapons and radiological bombs (conventional explosives that scatter radioactive debris). Nuclear weapons are in a class of their own in terms of mass destruction – a miniature nuclear weapon exploded in an urban area has the potential to cause much more death and destruction than either biological or chemical weapons similarly located.

Joining the concern over terrorists obtaining nuclear weapons is disconcerting evidence of nuclear entrepreneurship resulting in proliferation. The A. Q. Khan network, which comprised Pakistani and other government officials, middlemen, and scientists, conducted international commerce for several decades in nuclear technology and know-how. Described as a "Walmart of nuclear proliferation," the Khan network apparently transferred nuclear material to North Korea, Libya, and Iran, among other states.[4] States seeking a nuclear start-up can save enormous amounts of time and money by turning to experts in and out of government for help. Additionally, the knowledge of how to fabricate nuclear weapons is no longer as esoteric as it was in the early days of the atomic age.

In response to 9/11 and to the possible failure of nuclear containment in Asia and the Middle East, the George W. Bush administration sought to reinforce traditional nonproliferation with an interest in preemptive attack strategies and missile defenses. US superiority in long range precision weapons made preemption technically feasible, provided the appropriate targets had been identified. Bush policy guidance apparently also permitted the possible use of nuclear weapons in preemptive attack against hostile states close to acquiring their own nuclear arsenals.[5] While missile defenses are further behind the technology power curve compared to deep-strike attack capability, the first US national missile defense (NMD) deployments took place in 2004, and the Obama administration has embarked on an ambitious program for European-deployed land and sea-based missile defenses called the European Phased Adaptive Approach (EPAA).[6] Preemption strategies and defenses are controversial in their own right.[7] For present purposes, however, they appear to be simply talismans

of US government awareness and acknowledgment, as containment and deterrence can no longer complete the anti-proliferation tool kit.

A Multipolar Nuclear World

Uncertainty about the rate of nuclear weapons proliferation in Asia in the future is in contrast to the comparative stability of nuclear proliferation during the Cold War,[8] when nuclear weapons spread from state to state at a slower rate than even pessimists projected. In part this was due to the bipolar character of the international system and the nuclear preeminence of the Soviet Union and the United States over other contenders. Both superpowers discouraged horizontal proliferation among other state actors, even as they engaged in vertical proliferation by creating larger and more technically advanced arsenals. In addition, the NPT and the regime it established contributed to limit the rate of the spread of nuclear weapons among states that might otherwise have gone nuclear.[9]

The end of the Cold War and the demise of the Soviet Union have moved the zone of political uncertainty − and the interest in WMD and missiles − eastward, across the Middle East, South Asia, and the Pacific basin.[10] North America and Western Europe, pacified or at least debellicized by an expanded NATO and a downsized Russia, regard nuclear weapons as dated remnants of the age of mass destruction. The recent Revolution in Military Affairs has created a new hierarchy of powers, based on the application of knowledge and information to military art.[11] Nuclear and other WMD are, from the standpoint of the postmodern West, the military equivalent of museum pieces, although still dangerous in the wrong hands.

In contrast, major states in Asia and in the Middle East within the range of long range missiles based in Asia regard nuclear weapons and ballistic missiles as potential trump cards. The appeal of nuclear weapons and delivery systems for these states is at least threefold. First, they enable "denial of access" strategies for foreign powers who might want to interfere in regional issues. US military success in Afghanistan in 2001 and in Iraq in 2003 only reinforced this rationale of access denial via WMD for aspiring regional hegemons or nervous dictators. Second, nuclear weapons might permit states to coerce others that lack countermeasures in the form of deterrence. For instance, Israel's nuclear weapons, not officially acknowledged but widely known, suit Israel as a deterrent against offensive

behavior by its surrounding Arab neighbors and as a possible "Samson" option on the cusp of military defeat leading to regime change.[12]

Third, nuclear weapons permit states lacking the resources for advanced technology conventional military systems to compete with declared major powers. Russia is the most obvious example of this syndrome. Without its nuclear arsenal, Russia would be vulnerable to nuclear blackmail, or even to conventional military aggression, from a variety of strategic directions. Russia's holdover deterrent from the Cold War, assuming eventual modernization, guarantees Moscow military respect in Europe and makes its neighbors in Asia more circumspect.[13] North Korea is another example of a state whose reputation and regard are enhanced by its possible deployment of nuclear weapons and potential deployment of long range ballistic missiles.[14] Without nuclear capability, North Korea is a politically isolated rogue state with a bankrupt economy that would receive almost no international respect. But as an apparent nuclear power, North Korea has played "nuclear poker" with a five-nation coalition attempting to disarm its program by peaceful means: the US, Russia, Japan, China, and South Korea.[15]

The power transition from the second to the third generation of the Kim family regime in North Korea has given further rise to concern over nuclear proliferation in Asia. In an agreement signed with five powers in February 2007, North Korea promised to shut down its nuclear reactor at Yongbyon and to admit international inspectors into the DPRK to verify compliance within 60 days. For taking this step, North Korea was to receive an emergency shipment of fuel oil from the United States, Russia, China, and South Korea. The first phase of this pact thus froze the North Korean plutonium-based weapons program but left its suspended uranium-enrichment program for future discussions. In September 2007 North Korea agreed to declare and disable all of its nuclear programs by the end of the calendar year 2007.[16]

However, in keeping with a North Korean trend, backsliding relations with its nuclear interlocutors and shifting sands in North Korean domestic politics have since stranded the six party talks into diplomatic stasis and arms control uncertainty. The death of Kim Jong-il and his succession by son Kim Jong-un in December 2011 focused world attention on the implications of a power transition within a regime of uncertain stability and military and strategic provenance.[17] In response to UN sanctions after its

third nuclear test in February 2013 and to joint military exercises between the United States and South Korea, North Korea launched a bombastic diplomatic offensive in which it declared the 1953 Korean armistice null and void and threatened nuclear strikes against South Korea, US Pacific bases, and American state territory (although experts said North Korea lacked the technology for nuclear strikes against the continental United States).[18]

Failure to contain proliferation in Pyongyang could spread nuclear fever throughout Asia. Japan and South Korea might seek nuclear weapons and missile defenses. A pentagonal configuration of nuclear powers in the Pacific basin (Russia, China, Japan, South Korea, and North Korea – not including the United States, with its own Pacific interests) could put deterrence at risk and create enormous temptation toward nuclear preemption. Apart from actual use or threat of use, North Korea could exploit the mere existence of an assumed nuclear capability in order to support its coercive diplomacy.[19] In Paul Bracken's terms, North Korea can use its nuclear weapons to support either a "strategy of extreme provocation" or one intended to "keep the nuclear pot boiling" without having crossed the threshold of nuclear first use.[20] In October 2013 there were reports of the DPRK renewing nuclear activities, and perhaps preparing for new nuclear tests.

A five-sided nuclear competition in the Pacific would be linked, in geopolitical deterrence and proliferation space, to the existing nuclear deterrents of India and Pakistan, and to the emerging nuclear weapons status of Iran. An arc of nuclear instability from Tehran to Tokyo could place US proliferation strategies into the ash heap of history and call for more drastic military options, not excluding preemptive war, defenses, and counter-deterrent special operations. In addition, an unrestricted nuclear arms race in Asia would most likely increase the chance of accidental or inadvertent nuclear war. It would do so because: (a) some states in the region already have histories of protracted conflict; (b) states may have politically unreliable or immature command and control systems, especially during a crisis involving a decision for nuclear first strike or retaliation; (c) unreliable or immature systems might permit a technical malfunction resulting in an unintended launch, or a deliberate but unauthorized launch, by rogue commanders; (d) faulty intelligence and warning systems might cause

one side to misinterpret the other's defensive moves to forestall attack as offensive preparations for attack, thus triggering a mistaken preemption.

China Looms Large

The rising economic and military power of China relative to that of the United States and other nuclear weapons states must also be considered when assessing the changing geopolitical arena. China's growing economy and its strengthened military forces will almost certainly lead to greater Chinese assertiveness and influence in the Asia-Pacific region over the course of the next several decades. Viewed from the standpoint of some classical international relations theory, China is a rising power posing a potential threat to an existing hegemon, at least regionally and perhaps globally. One expert analysis of US-China relations from the perspective of power transition identifies three sets of outcomes or scenarios that might occur between now and mid-century: (1) a deadly contest for change, (2) a peaceful changing of the guard, or (3) a reluctant accommodation.[21] This geostrategic competition need not end in war. In the short term, Chinese economic modernization requires a period of sustained development uninterrupted by major interstate war. In addition, in the long term, a power transition between the United States and China will most likely require China to apply the principle "at odds, but not at war" to its relationship with the US. As David Lai explains, "Indeed, in a power transition process, if the upstart sees that its comprehensive national power will surpass that of the extant hegemonic power by virtue of its expected development, it will be foolish for the rising power to initiate a premature fight with the latter."[22]

There are other possible axes of competition and conflict in the region in which China could become embroiled. Russia and Japan are two competitors for regional influence against China, and the possibility of an outbreak of local or large scale war between China and Russia or between China and Japan is not precluded. Russia's large combined arms military exercise in the Siberian Far East, Vostok-2010, was designed in part to test the readiness of its reformed armed forces, especially its brigade-based ground forces aspiring to advanced conventional operations and a Russian version of network-centric warfare. Although Russian officials designated the opponent in these exercises as hypothetical, it was difficult to escape the conclusion that the Chinese People's Liberation Army (PLA) was on the minds of Russian military planners. Jacob W. Kipp noted:

> The air and ground exercises near Chita and Khabarovsk make no sense except as responses to some force threatening the territorial integrity of Eastern Siberia and the Far East. The only forces with the military potential to carry out air and ground attacks that deep into Russian territory are the PLA in support of the so-called separatists identified in the scenario.[23]

Thus far, we have discussed the problem of an Asian nuclear arms race as an abstract, albeit alarming, problem. The following sections of the paper will analyze the issue further by exploring two contrasting scenarios: a proliferation-constrained model, in which a multilateral agreement among nuclear weapon states and others essentially freezes the status quo in long range nuclear weapons deployments; and an unconstrained Asian nuclear arms competition leading to the addition of new nuclear weapon states and potentially more instability in Asia.

Asian Nuclear Arms Race Scenarios

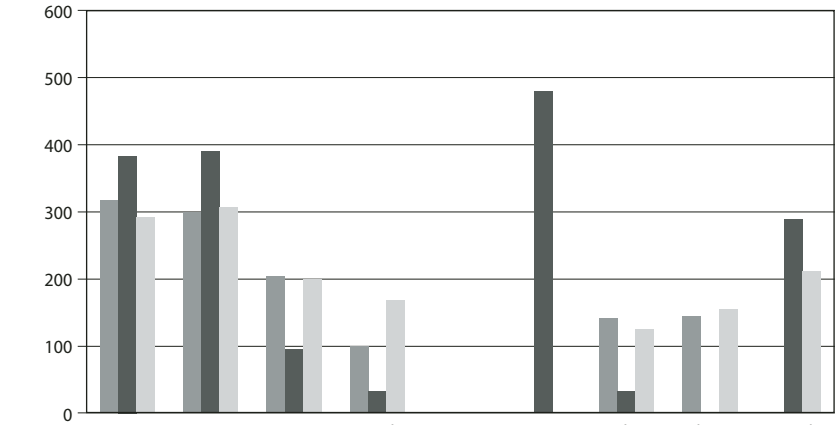
Scenario 1: Constrained Nuclear Proliferation

A multilateral agreement on nuclear arms limitations and/or reductions would have to establish some rank order among existing nuclear weapons states and close the door to admission of others. Preferably, it would also negotiate the successful dismantlement of North Korea's nuclear weapons and infrastructure. A rank order among the remaining nuclear weapons states might be established as follows: for the United States and Russia, an upper limit of 1,000 operationally deployed long range nuclear weapons each; for China, France, and the UK, a ceiling of 500 weapons; and for India, Pakistan, and Israel, a limit of 300. States would have to count all weapons deployed on either intercontinental or intermediate range launchers, but not on missiles or bombers of shorter range. Obviously some agreed mechanism of monitoring and verification would have to be established, perhaps through the IAEA (International Atomic Energy Agency) and its program of inspections.

This scenario calls for a considerable amount of cooperation among the P5 (the permanent members of the UN Security Council, which also happen to be the first five members of the nuclear club), and may well encounter difficulty among the various military chiefs of staff. However, the sacrifices being asked of states under this regime are small if it means

preventing an unregulated market for nuclear weapons in Asia and the Middle East. With an enforceable agreement of this sort in place, the UN and the IAEA would have additional credibility and clout in bringing pressure to bear against aspiring or nascent nuclear proliferators.

Would the preceding arrangement among existing nuclear weapons be deterrence stable and/or crisis stable? Figure 1 illustrates the constrained proliferation model at work and presents the numbers of weapons assigned to the various states in the model.[24]

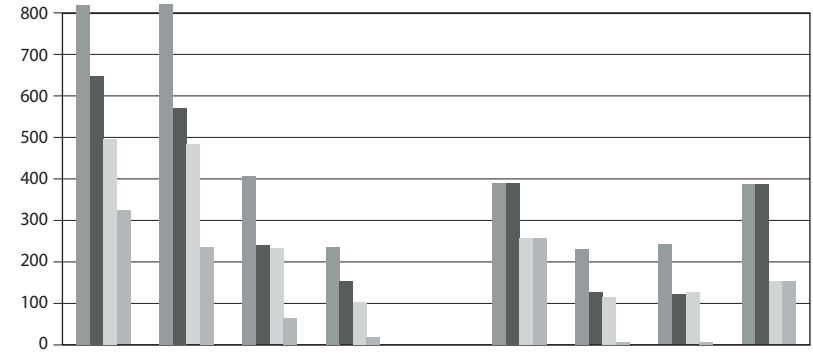


	Russian Forces	US Forces	PRC Forces	Israeli Forces	UK Forces	Indian Forces	Pakistan Forces	French Forces
ICBM	318	300	204	100	0	142	144	0
SLBM	384	392	96	32	480	32	0	288
AIR	294	308	200	168	0	126	156	212

ICBM – intercontinental ballistic missile
SLBM – submarine-launched ballistic missile
AIR – air-delivered weapons

Figure 1. Constrained Proliferation Model: Total Strategic Weapons

Figure 2 displays the numbers of second strike surviving and retaliating weapons available to each state, given reasonable assumptions about the capabilities of attackers and defenders with notional forces and the recognition that nuclear forces are deployed primarily for the purpose of deterrence. No one can predict with full certainty how they would perform under the stress of a two- or many-sided nuclear war.



	Russian Forces	US Forces	PRC Forces	Israeli Forces	UK Forces	Indian Forces	Pakistan Forces	French Forces
GEN, LOW	812	812	407	238	389	233	243	388
GEN, ROA	641	569	242	157	389	129	127	388
DAY, LOW	495	483	236	107	260	120	130	156
DAY, ROA	324	240	70	26	260	14	13	156

GEN – generated alert
DAY – day-to-day alert
LOW – launch on warning
ROA – ride out the attack

Figure 2. Constrained Proliferation Model: Surviving and Retaliating Weapons

Figures 1 and 2 show that although all states retain sufficient numbers of surviving and retaliating warheads with the potential for stable deterrence, larger arsenals have more survivable redundancy. Whether this range among states, post-attack, would matter in a world having witnessed the first nuclear weapons fired in anger since Nagasaki, is a question with both scientific and ethical components. In the best of all worlds, the constrained proliferation model would provide for a degree of deterrence and crisis stability sufficient to retain the nuclear taboo or de facto abstention from nuclear first use well into the third decade of the twenty-first century.

Figure 2 shows that it is at least possible for this constrained proliferation regime to provide for deterrence stability based upon assured retaliation; crisis stability, however, is a little harder to assess. Figures 1 and 2 indicate that in the constrained proliferation model states can provide for sufficient degrees of crisis stability − if their nuclear-capable forces are duly responsive to authorized commands and are beyond political usurpation or malfunction. At the very least, it can be said that the model does not exclude this optimistic scenario.

On the other hand, political leaders and their military advisors, and not some magic system or process, will determine whether any particular multipolar nuclear regime will succeed or fail in preserving crisis stability. Therefore, on top of their disinclination toward a nuclear preemptive attack, states should provide for a margin of error in the performances of their nuclear alerts, response system, and command and control networks. In this regard, states might prefer to emphasize force structures that are less dependent upon prompt launch for survivability – sea-based ballistic missiles compared to land-based ones, for example, or mobile land-based missiles compared to silo-based missiles. States contiguous to prospective enemies will be especially prone to first strike fears unless they have well protected forces and command systems buffered against "decapitation" attacks,[25] attacks intended to paralyze or destroy the opponent's political and/or military command and control system, apart from, or in addition to, any attacks on nuclear or conventional forces, populations, or other targets.

Scenario 2: Asian Nuclear Arms Race

What would a nuclear arms race in Asia look like in 2020 or thereafter? If proliferation in Asia is successfully contained or rolled back, by political or by military means, the threat of an arms race declines and there is no need for speculation. However, if we assume a more pessimistic future in which proliferation is not contained, the third decade of the twenty-first century might witness an eight-sided nuclear club of states in Asia and/or the Middle East, including Russia, China, Japan, North Korea, South Korea, India, Pakistan, and Iran, with the ability to contribute to nuclear destabilization in Asia (other possibilities for nuclear weapons proliferation exist, especially in the aftermath of Iran becoming a declared and de facto nuclear weapons state, led by Saudi Arabia, Turkey, and Egypt). Although this scenario does not contain proliferation, it does not automatically result in war. The assumption that nuclear weapons can spread among these states without war necessarily ensuing will be questioned by some, and with some justification. For example, the US has declared that an Iranian or a North Korean nuclear capability is presently unacceptable: the former must be prevented, and the latter must be rolled back. In addition, some experts would surely argue that China would never accept a Japan armed with nuclear weapons.

On the other hand, the rollback of North Korea's nuclear program is far from a certainty: a complicated international bargaining process may leave the DPRK as a standing nuclear power, with a trade-off including more glasnost on the part of the regime, a willingness on the part of Pyongyang to adhere to some international arms control agreements, and economic assistance from the US and other powers to help rebuild North Korea's collapsed economy. As for the Iranian nuclear case, both Israel and the United States have obliquely threatened preemption (presumably with conventional weapons) against Iran's nuclear infrastructure and against any nuclear capable military forces, but the costs of carrying out the threat of preemption against Iran must be factored into the equation.[26] Unlike Iraq, Iran is a large state and cannot be conquered and occupied by outside powers. Iran could also reconstruct any destroyed nuclear power plants or other infrastructure. An additional consideration is political: any Israeli preemption against Iran becomes a recruitment poster for another holy war by jihadists against Israel. Iran is one of the major sponsors of Hizbollah and other groups that have carried out past terror attacks in Israel. An Israeli preemption against Tehran might therefore spark a new conflagration or otherwise destabilize the peace process.

The point is that many uncertainties loom, and the exclusion of any specific candidate from the future nuclear club is not automatic. Therefore, the analysis below includes eight current and prospective nuclear weapons states located in Asia (or in the Middle East but potentially contributory to nuclear instability in Asia) and assigns to them notional forces.

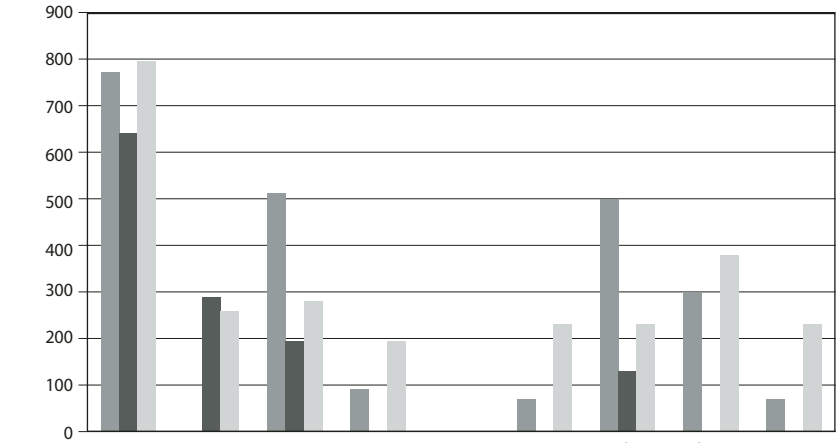
Assume that the older and newer nuclear forces are deployed without treaty constraints. Russia, for example, would feel free to exceed its New START-limited ceiling of 1,550 operationally deployed warheads on launchers of intercontinental range. At the same time, Russia's capacity for nuclear force building and modernization is not unlimited and may fall short of the most ambitious goals set by President Putin and military industry head Dmitri Rogozin.[27] Russia would seek to maintain its perceived status as a nuclear weapon state of the same rank as the United States, and therefore would want to appear as the strongest nuclear military power in Asia, relative to potential regional rivals. In this scenario, Russia and other nuclear powers are assumed to have freedom to mix various types of launch platforms among land-based, sea-based, and air-launched weapons. Cruise missiles are omitted from the present analysis for purposes of

simplification, but it is important to note that as cruise missiles become smarter, stealthier, and more widely available, they could be a preferred weapon for some states if capped with nuclear charges, compared to ballistic missiles.

States with nuclear capabilities in this scenario include Russia, China, Japan, India, Pakistan, North Korea, South Korea, and Iran. Although some might object to the inclusion of Japan, others will likely accept Japan as a nuclear weapon state for at least three reasons. First, Japan has a post-World War II history of military pacifism, and memories of its World War II and earlier aggressions against regional rivals have faded somewhat. Second, in terms of its political objectives within the international system, Japan is more of a status quo than a revisionist actor, and therefore, it can be assumed that a Japanese nuclear weapons capability would be no more threatening than that of Britain or France. Third, a nuclear armed Japan could assist in the containment of China (along with India and Russia).[28]

Other arguments, however, suggest that Japan is not likely to obtain nuclear weapons in the first place. First, Japan has the extended deterrence protection of the US nuclear umbrella and is sharing technology development for missile defenses with the United States. Second, public opinion in Japan remains skeptical about the need for a nuclear weapons capability and the risk that it would entail. Even political elites in Tokyo who favor a more assertive Japanese defense policy in general are burdened by the recent national tragedy of the Fukushima nuclear disaster in March 2011.[29] Third, for historical and political reasons China would regard a nuclear Japan supported by the United States as a major threat to its own national security, perhaps increasing China's military buildup and adversely impacting upon US Chinese relations.

Figure 3 charts the forces deployed and available to the various state parties in the Asian arms race model presented. It is obviously impossible to project their future forces in detail. We have taken the heuristic shortcut of assigning generic kinds of forces by category of launch system: land-based missile, submarine- launched missile, and bomber. In addition, deployed nuclear-capable missiles and bombers are not necessarily assumed to have intercontinental ranges. Some states in the model will be more concerned with contiguous and regional rivals capable of being attacked by short, medium, and/or intermediate range missiles and aircraft, than they will be about intercontinental or transoceanic attack capabilities.



	Russian Forces	Japanese Forces	PRC Forces	DPRK Forces	ROK Forces	Indian Forces	Pakistan Forces	Iranian Forces
ICBM	772	0	510	90	70	500	300	70
SLBM	640	288	192	0	0	128	0	0
AIR	796	260	280	192	232	230	380	230

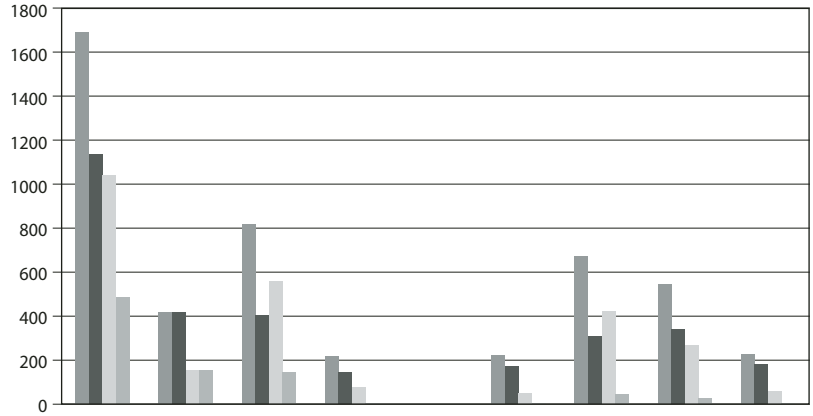
ICBM – intercontinental ballistic missile
SLBM – submarine-launched ballistic missile
AIR – air-delivered-weapons

Figure 3. Asian Arms Race Model: Total Strategic Weapons

Each nation would have to plan for the likelihood that only a portion of its forces would survive a nuclear first strike, retaliate, and arrive at their assigned targets. The numbers of each state's second strike surviving and retaliating forces following notional first strikes are summarized in figure 4.

Several findings are significant. From the standpoint of deterrence stability, there is no clear measure by which one can say that a specific number of additional nuclear powers will equate to a certain degree of decline in deterrence. In theory, it is not impossible for a many-sided nuclear rivalry, even one as regionally robust as the one presented in this case, to be stable. Provided it has the resources and the technical know-how to do so, each state could deploy sufficient numbers of "second strike survivable" forces to guarantee the "minimum deterrent" mission, and perhaps the "assured destruction" mission as well.

Both "minimum deterrence" and "assured destruction" are terms that overlap in practice. Assured destruction (or assured retaliation) forces are second strike forces sufficient under all conditions of attack to inflict "unacceptable" societal damage. Unacceptable varies with the recipient of



	Russian Forces	Japanese Forces	PRC Forces	DPRK Forces	ROK Forces	Indian Forces	Pakistan Forces	Iranian Forces
GEN, LOW	1689	423	819	221	226	676	547	231
GEN, ROA	1134	423	406	148	175	312	345	186
DAY, LOW	1042	156	563	81	57	426	270	63
DAY, ROA	487	156	150	8	6	51	27	6

GEN – generated alert
DAY – day-to-day alert
LOW – launch on warning
ROA – ride out the attack

Figure 4. Asian Arms Race Model: Surviving and Retaliating Weapons

the damage and depends on cultural values and political priorities. But it would be safe to assume that the decapitation of the regime and the loss of at least 25 percent of its population and/or one half of its industrial base would satisfy the requirements of assured destruction for "rational" or at least sensible attackers.

Minimum deterrence is a standard presumably less ambitious than assured destruction: it requires only that the defender inflict costs on the attacker that would create enough pain to make the gamble of an attack insufficiently appealing.[30] For example, during the Cold War, the French nuclear retaliatory forces were unable to deter a Soviet attack on NATO independently, but they might have deterred nuclear blackmail against France separately by threatening Moscow with the prospect of "tearing an arm off," or destroying several Soviet cities. Some expert analysts have suggested that a minimum deterrent strategic nuclear force for the United States might be maintained with as few as several hundred operationally deployable weapons.[31] Former US National Security Advisor McGeorge

Bundy put forward the most assertive definition of minimum deterrence in his argument that ten nuclear weapons on ten cities would be a "disaster beyond history."[32]

Although the projection of past events into future scenarios is always perilous, something like the July crisis in Europe in 1914 could erupt in Asia once nuclear weapons have been distributed among eight major states with high military stakes in Asia and in numbers sufficient to tempt crisis-prone leaders. National or religious hatred, for example, could be combined with the memory of past wrongs and the fear of preemptive attack leading to first use. This could occur not only between dyads of states but between allies, as it did on the eve of the First World War.

Coalitions might form among a nuclear armed China, Pakistan, North Korea, and Iran, lined up against Russia, the US, South Korea, and India. This would be an alignment of mostly market democracies against dictatorships or authoritarian-type regimes. Another possibility would be conflicts between dyads within, or across, democratic and dictatorial coalitions: for example, rivalry between North Korea and South Korea, or between India and Pakistan. Russia might find itself in bilateral competition or conflict with China, or China with India. Iran might use its nuclear capability for coercion against US allies, such as Saudi Arabia or Israel, drawing American political commitments and military power directly into a regional crisis.

Putting this scenario aside, it remains the case that nuclear weapons are in a class of their own as instruments of prompt mass destruction. Therefore, what is important is not the numbers of nuclear weapons, but the possible effect of leaders' perceptions that higher alerts and faster launches are necessary in order to avoid catastrophic defeat, should war occur. There are no "winnable" nuclear wars depicted here, nor would there be, even if agreed levels among the powers were reduced to several hundreds of warheads.[33] The danger is that a war might begin not so much from deliberation, but from desperation in a situation in which states, feeling that their nuclear deterrents are threatened, make a hasty decision under pressure that permits neither reflection nor appropriate inspection of the information at hand.

Assessment

Stability in a region of states armed with nuclear weapons resides mainly in the policies of these states and in the intentions of their leaders. The number of nuclear armed states in a region does not by itself determine the probability of nuclear crisis or war. Nonetheless, nuclear complacency is ill advised. Regional rivalries, including ethno-nationalist and religiously inspired disagreements, combine dangerously with weapons of mass destruction, from the standpoint of international security and stability. A crowded nuclear Asia also threatens to expand regional rivalries into global confrontations because the Asian nuclear club includes nuclear weapons states with global ambitions. US military planners must also assume that the spread of nuclear weapons in Asia will increase the appeal of anti-access, area denial (A2AD) strategies, supported by enhanced conventional weapons and command and control capabilities for regional actors.

Nuclear forces may be deployed and operated with more or less sensitivity to the problem of provocative crisis behavior. According to Lawrence J. Korb and Alexander Rothman, the United States should adopt an unconditional "no first use" policy for its nuclear weapons and urge other nuclear weapons states to do likewise. An agreed multilateral "no first use" policy would help prevent an outbreak of nuclear war in Asia and contain such a war if it occurred.[34] On the other hand, a unilateral US declaration of this sort, without support from other nuclear weapon states, could weaken US extended deterrence now provided to non-nuclear allies, possibly compromising the NPT and encouraging formerly US-protected allies to develop their own nuclear weapons arsenals.

As a variant on this theme, Paul Bracken has proposed a US declaratory policy of "no first use, guaranteed second use." If any other country were to use the bomb first against the United States, or against any allied state, the United States would guarantee second use against the attacker.[35] This modified version of "no first use" might put some additional teeth into a declaratory policy that might otherwise inspire doubt or cynicism. On the other hand, the "no first use, guaranteed second use" stance could tie the hands of policymakers if a US ally were the first to use a nuclear weapon against another state that otherwise threatened to inflict upon it a decisive conventional military defeat or regime change.

No first use declarations also make no distinctions among the sizes of nuclear weapons used or their presumed purposes. Would, for example, a

demonstration shot above the territory of a state that causes no terrestrial damage or casualties count as first use (although it might damage electronics or space based assets)? Would a state that either insufficiently guards its nuclear weapons and materials, or demonstrates outright complicity with terrorists, thus leading to a terrorist nuclear attack, be guilty of nuclear first use requiring an obligatory second use? A safer version of declaratory policy is probably one that leaves options open and vaguely defined.

Declarations by themselves are useful but fall short of fulfilling the requirements for stable nuclear deterrence. Countries must see a prior pattern of credible diplomatic-strategic behavior on the part of those powers who favor system stability, as compared to those powers who seek to overthrow or amend the existing order. Credible diplomatic-strategic behavior related to nuclear deterrence is twofold. First, it lies in having a coherent national security strategy, detailing aspects relevant to the exercise of deterrence and the use, or threat, of force. Second, it rests on the availability of viable strategies and responsive forces for the use, or threat of use, of force under conditions of peacetime, crisis, and wartime exigency. Of special importance in containing nuclear proliferation and/or misbehavior on the part of proliferators is the need for understanding the military-strategic cultures of those whose nuclear first use must be deterred. Here the concern is that Western powers may not correctly read the mindsets of regional nuclear or nuclear-aspirational states until a regional crisis escalates into a war, and possibly, into a nuclear war. The mind of the enemy (or possible enemy) is the ultimate target of deterrence and other strategies for military persuasion or coercion. A multipolar nuclear system, like the hypothetical Asian arms race illustrated here, is dangerous not only because of the numbers of weapons or the numbers of nuclear armed states, but primarily given the potential for misperception that exists when leaders in crisis situations are tasked to make fast decisions with potentially lethal consequences. Additionally, cultural differences may come into play leading to false assessments of the case.

For the United States and its military planners, the conclusions emerging from this analysis suggest the following recommendations. First, the US will need to manage future challenges to deterrence and crisis stability in the Middle East and in South and East Asia by maintaining and improving a new strategic "triad" of: (1) long range nuclear and conventional offensive weapons and delivery systems, (2) anti-missile and air defenses, both

theater and strategic, and (3) offensive and defensive cyber weapons. Second, the US will also need to exercise deterrence and defense against regional Anti-Access/Area Denial strategies by maintaining escalation dominance in the aerospace and maritime continua, relative to probable regional opponents. Third, US diplomacy must support selective and multilateral military intervention that combines carrots (information operations or "the battle for the narrative") and sticks (the credible threat of use of effective and tailored military force, if necessary).

Notes

1 For contrasting perspectives on this issue, see Kenneth N. Waltz, "More May Be Better," in *The Spread of Nuclear Weapons: A Debate,* eds. Scott D. Sagan and Kenneth N. Waltz (New York: W. W. Norton, 1995), pp. 1-45, and Scott D. Sagan, "More Will Be Worse," in *The Spread of Nuclear Weapons*, pp. 47-91.

2 Lawrence J. Korb and Alexander Rothman, "No First Use: The Way to Contain Nuclear War in South Asia," *Bulletin of the Atomic Scientists* 68, no. 2 (2012): 34-42, see particularly p. 35.

3 For expert commentary on these three kinds of stability, see Elbridge A. Colby and Michael S. Gerson, eds., *Strategic Stability: Contending Interpretations* (Carlisle, PA: Strategic Studies Institute, US Army War College Press, February 2013).

4 Graham Allison, *Nuclear Terrorism: The Ultimate Preventable Catastrophe* (New York: Henry Holt, Times Books, 2004), pp. 61-63. On the topic of nuclear terrorism, see also Brian Michael Jenkins, *Will Terrorists Go Nuclear*? (New York: Prometheus Books, 2008).

5 Lawrence Korb with Peter Ogden, *The Road to Nuclear Security* (Washington, DC: Center for American Progress, December 2004), p. 5.

6 For US and NATO missile defense plans, see Lt. Gen. Patrick J. O'Reilly, *Ballistic Missile Defense Overview*, presented at the 10th Annual Missile Defense Conference (Washington, DC: US Department of Defense, March 26, 2012, 12-MDA-6631), http://www.mda.mil/news/downloadable_resources.html. In mid-March 2013, US Secretary of Defense Chuck Hagel announced revised plans to increase the numbers of ground-based missile defense (GMD) interceptors deployed in Alaska and California, partly in response to North Korean threats against the US and its allies. At the same time, Hagel also noted plans to revise the European Phased Adaptive Approach (EPAA) to eliminate its fourth stage interceptor scheduled for deployment in 2022. See "The Administration Yanks a Missile that Upset Russia," *Washington Post*, March 20, 2013, in *Johnson's Russia List* 2013, no. 51, March 20, 2013. See also the related study by technical experts, Committee on an Assessment of Concepts and Systems for US Boost-Phase Missile Defense in Comparison to Other Alternatives, *Making Sense of Ballistic*

Missile Defense: An Assessment of Concepts and Systems for U.S. Boost-Phase Missile Defense in Comparison to Other Alternatives (Washington, DC: National Research Council, National Academy of Sciences, National Academies Press, 2012), prepublication copy, www.nap.edu.

7 See Karl P. Mueller, et. al., *Striking First: Preemptive and Preventive Attack in U.S. National Security Policy* (Santa Monica, California: RAND, 2006) for an assessment of past and present US experience. Unnecessary confusion in the American policy debate about preemption and preventive war strategies is noted in Colin S. Gray, *The Implications of Preemptive and Preventive War Doctrines: A Reconsideration* (Carlisle, PA: Strategic Studies Institute, US Army War College, July 2007).

8 On the differences between the first and second nuclear ages, see Paul Bracken, *The Second Nuclear Age: Strategy, Danger, and the New Power Politics* (New York: Henry Holt/Times Books, 2012), pp. 106-26 and passim.

9 Joseph Cirincione, *Bomb Scare: The History and Future of Nuclear Weapons* (New York: Columbia University Press, 2007), p. 43 and passim. According to Cirincione, the following states have abandoned nuclear weapons programs, nuclear weapons, or both since the NPT entered into force: Argentina, Australia, Belarus, Brazil, Canada, Iraq, Kazakhstan, Libya, Rumania, South Africa, South Korea, Spain, Switzerland, Taiwan, Ukraine, and Yugoslavia; see p. 43.

10 Bracken, *The Second Nuclear Age*, particularly chapters 5-7. See also Bracken, *Fire in the East: The Rise of Asian Military Power and the Second Nuclear Age* (New York: Harper Collins, 1999), particularly pp. 95-124.

11 Michael O'Hanlon, *Technological Change and the Future of Warfare* (Washington, DC: Brookings Institution, 2000), pp. 7-31.

12 This point is noted in Keir A. Lieber and Daryl G. Press, "A New Era of Nuclear Weapons, Deterrence and Conflict," *Strategic Studies Quarterly* 7, no. 1 (2013): 3-12.

13 Nikolai Sokov, "Nuclear Weapons in Russian National Security Strategy," chapter 5, in Stephen J. Blank, ed., *Russian Nuclear Weapons: Past, Present, and Future* (Carlisle, PA: Strategic Studies Institute, November 2011), pp. 187-260. See also Nikolai Sokov, "The New 2010 Russian Military Doctrine: The Nuclear Angle," Center for Nonproliferation Studies, Monterey Institute of International Studies, February 5, 2010, http://cns.miis.edu/stories/100205_russian_nuclear_doctrine.htm.

14 North Korea's military capabilities are discussed in Andrew Scobell and John M. Sanford, *North Korea's Military Threat: Pyongyang's Conventional Forces, Weapons of Mass Destruction, and Ballistic Missiles* (Carlisle, PA: US Army War College, Strategic Studies Institute, April 2007). See also BBC, "North Korea's Missile Programme," *BBC Asia*, December 12, 2012, http://www.bbc.co.uk/news/world-asia-17399847?print=true.html, accessed April 4, 2013.

15 Writing in November 2011, Stephen J. Blank noted that "the Six-Party process is moribund, if not dead" and referred to a "growing intransigence" among the major negotiating parties. See *Arms Control and Proliferation Challenges to the Reset Policy (*Carlisle, PA: Strategic Studies Institute, November 2011), pp. 36-37.

16 Choe Sang-Hun, "North Korea says U.S. Will Lift Sanctions," *New York Times*, September 4, 2007, http://www.nytimes.com/2007/09/04/world/asia/04korea.html; Bill Powell, "North Korea has Agreed to Shut Down its Nuclear Program: Is He Really Ready to Disarm?" *Time*, February 26, 2007, pp. 32-33; and Glenn Kessler, "Conservatives Assail North Korean Accord," *Washington Post,* February 15, 2007.

17 Historical perspective on North Korea's interest in nuclear weapons and on US relations with the North Korea appears in Richard Rhodes, *The Twilight of the Bombs: Recent Challenges, New Dangers, and the Prospects for a World without Nuclear Weapons* (New York: Alfred A. Knopf, 2010), pp. 173-209. See also: David E. Sanger and Joseph Berger, "Arms Bid Seen in New N. Korea Plant," *New York Times*, November 21, 2010, http://www.nytimes.com/2010/11/22/us/22talk.html, and Siegfried S. Hecker, *A Return Trip to North Korea's Yongbyon Complex* (Stanford, California: Center for International Security and Cooperation, Stanford University, November 20, 2010).

18 See Matt Smith, "New North Korean Broadside Warns 'Moment of Explosion' Nears," *CNN*, April 3, 2013, http:/www.cnn.com/2013/04/03/world/asia/koreas-tensions/index.html; Martin Fackler, "Japan Shifts From Pacifism as Anxiety in Region Rises," *New York Times*, April 1, 2013, http://www.nytimes.com/2013/04/02/world/asia/japan-shifting-further-away-from-pacifism.html; and Jethro Mullen and Catherine E. Shoichet, "North Korea Puts Rockets on Standby to 'Mercilessly Strike' the U.S.,"*CNN,* March 29, 2013, http:/www.cnn.com/2013/03/29/world/asia/north-korea-us-threats/index.html.

19 George H. Quester, *Nuclear First Strike: Consequences of a Broken Taboo* (Baltimore, Maryland: Johns Hopkins University Press, 2006), p. 49. See also: Bracken, *The Second Nuclear Age*, pp. 189-95.

20 Bracken, *The Second Nuclear Age*, p. 149, discusses these possible strategies for Iran, but they also apply as possibilities for North Korea.

21 David Lai, *The United States and China in Power Transitions* (Carlisle, PA: Strategic Studies Institute, US Army War College, December 2011), p. 81 and passim.

22 Lai, *The United States and China in Power Transitions,* p. 173.

23 Jacob W. Kipp, "Russia's Nuclear Posture and the Threat that Dare Not Speak its Name," chapter 10 in Stephen J. Blank, ed., *Russia's Nuclear Weapons: Past, Present and Future* (Carlisle, PA: Strategic Studies Institute, US Army War College, November 2011), pp. 459-503, citation p. 489.

24 Grateful acknowledgment is made to Dr. James Scouras for use of his AWSM@ model for making calculations and drawing graphs in this study. Dr. Scouras is not responsible for any analysis or arguments herein.

25 Unfortunately the old Cold War-style recipes for nuclear decapitation are now complicated by the possibility of cyberwar and related information operations. US government and other definitions for cyberspace and related concepts are reviewed in Daniel T. Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," chapter 2 in *Cyberpower and National Security*, eds. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, DC: National Defense University Press, Potomac Books, Inc., 2009), pp. 24-42. See also Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, California: RAND Corporation, 2009); Timothy L. Thomas, *Cyber Silhouettes: Shadows Over Information Operations* (Fort Leavenworth, Kansas: Foreign Military Studies Office, 2005); and David S. Alberts, John J. Garstka, Richard E. Hayes, and David T. Signori, *Understanding Information Age Warfare* (Washington, DC: DOD Command and Control Research Program, US Department of Defense, 3rd edition, October, 2004). On influence operations, see John Arquilla, *Worst Enemy: The Reluctant Transformation of the American Military* (Chicago, Illinois: Ivan R. Dee, 2008), chapter 6. On the role of information operations in Russian military policy, see Timothy L. Thomas, *Recasting the Red Star: Russia Forges Tradition and Technology through Toughness* (Fort Leavenworth, Kansas: Foreign Military Studies Office, 2011), particularly chapter 6 and Appendix One.

26 On this topic, see Alexander Wilner and Anthony Cordesman, *U.S. and Iranian Strategic Competition: The Gulf Military Balance* (Washington, DC: Center for Strategic and International Studies, November 2, 2011), particularly pp. 102-28, and David Albright, Paul Brannan, and Jacqueline Shire, *Can Military Strikes Destroy Iran's Gas Centrifuge Program? Probably Not* (Washington, DC: Institute for Science and International Security, ISIS Report, August 7, 2008. For US intelligence community thinking on Iran, see Director of National Intelligence John Negroponte, *DNI Annual Threat Assessment 2006*, cited in Anthony H. Cordesman, *Iran's Nuclear and Missile Programs: A Strategic Assessment* (Washington, DC: Center for Strategic and International Studies, revised August 31, 2006), p. 23. For force projections and scenarios for the Middle East, see Cordesman, *Warfighting and Proliferation in the Middle East* (Washington, DC: Center for Strategic and International Studies, revised April 17, 2007).

27 For pertinent estimates, see Pavel Podvig, "New START Treaty in Numbers," from his blog, *Russian Strategic Nuclear Forces*, April 9, 2010, http://russianforces.org/blog/2010/03/new_start_treaty_in_numbers.shtml. The author also gratefully acknowledges a draft briefing by James R. Howe, *Current and Future Russian Strategic Nuclear Forces and Implications for US Policy, Strategy, and Force Structure* (Draft: Work in Progress, Vision Centric, Inc., June 3, 2013).

28 On the issue of Japan as a nuclear weapons state, see Bracken, *The Second Nuclear Age,* pp. 239-41.

29 See World Nuclear Association, *Fukushima Accident of 2011*, http://www.world-nuclear.org/info/Safety-and-Security/Safety-of-Plants/Fukushima-Accident.html, updated April 2, 2013.

30 On minimum deterrence, see Hans M. Kristensen, Robert S. Norris, and Ivan Oelrich, *From Counterforce to Minimal Deterrence: A New Nuclear Policy on the Path Toward Eliminating Nuclear Weapons* (Washington, DC: Federation of American Scientists and Natural Resources Defense Council, April, 2009).

31 James Wood Forsyth, Jr., B. Chance Saltzman, and Gary Schaub Jr., "Minimum Deterrence and its Critics," *Strategic Studies Quarterly* 4, no. 4 (2010): 3-12. Paul Bracken warns that it may be misleading to characterize South or East Asian nuclear forces as minimum deterrents, because that designation understates the range of scenarios for making political use of these forces, and in addition, insufficiently appreciates the effects of combining regional nuclear forces with advanced technology for information warfare, stealth, and precision strike. See Bracken, *The Second Nuclear Age,* chapters 6 and 7, particularly p. 188.

32 McGeorge Bundy, "To Cap the Volcano," *Foreign Affairs* 1 (October, 1969): 1-20, citation, p. 10.

33 This point is made in the larger context of an argument for further Russian and American nuclear arms reductions, and for strengthening the nuclear nonproliferation regime, by Wolfgang K. H. Panofsky, "Nuclear Insecurity," *Foreign Affairs*, September-October 2007, in *Johnson's Russia List* 2007, no. 180, August 23, 2007.

34 Korb and Rothman, "No First Use: The Way to Contain Nuclear War in South Asia," p. 37.

35 Bracken, *The Second Nuclear Age*, p. 263.

Commercial and Industrial Cyber Espionage in Israel

Shahar Argaman and Gabi Siboni

Cyberspace is especially suited to the theft of business information and to espionage. The accessibility of information, along with the ability to remain anonymous and cover one's tracks, allows various entities to engage in the theft of valuable information, an act that can cause major damage. Israel, rich in advanced technology and a leader in innovation-based industries that rely on unique intellectual property, is a prime target for cyber theft and commercial cyber attacks. This article examines the scope of cyber theft and cyber industrial espionage globally, and attempts to estimate how much financial damage they cause in countries around the world and in Israel. It seeks to raise awareness of the extent of the phenomena among the relevant authorities in Israel and provide recommendations on how to grapple with it.

Keywords: Cyber, espionage, industrial espionage, intellectual property, cyber crime, cyber theft, technology

> *"There are two types of companies: companies that have been breached and companies that don't know they've been breached.... The vast majority of companies have been breached."*[1]
> Shawn Henry

> *The director of the National Security Agency, Gen. Keith Alexander, called cybercrime "the greatest transfer of wealth in history." The price tag for intellectual property theft from U.S. companies is at least $250 billion a year.*[2]

Shahar Argaman is the director of the National Cyber Staff. Col. (ret.) Dr. Gabi Siboni is the head of the Military and Strategic Affairs Program and Cyber Security Program at INSS.

Background

Cyberspace is a product of the accelerated pace of technological developments in the last few decades. Initially, communications and computerized systems were linked together to function as local networks. These networks were later linked together to form a global medium of existence and activity. At present, cyberspace continues to develop on numerous levels: in the wealth of interconnected computerized tools, in the number and variety of networks, in the volume of information traffic, in the level of connectivity, in the variety of applications, and in the degree to which economic and social activity depends on cyber functions.

While cyberspace brings with it much positive potential and broadens horizons on every level of human activity, it also entails new threats and in effect presents a new arena for hostile activity, from the sabotage of information in cyberspace to damage to the physical world through cyberspace functions.[3] As the overall use of cyberspace increases, so too does the hostile activity within the arena,[4] which already includes a vast range of threats: denial of service, destruction of websites, exposure of personal information for the purpose of wielding influence or instilling fear, various types of crime, industrial and security espionage, and damage to national strategic infrastructures, databases, command and control systems, and even weapon systems.

By its very nature, cyberspace is a medium particularly well suited to espionage in general and commercial and industrial espionage in particular. Industrial espionage among commercial rivals is hardly a new phenomenon, but cyberspace allows simpler access than in the past to a great deal of information while allowing a high level of invisibility. The damage that can result from commercial espionage today is of unprecedented scope precisely because cyberspace is optimally suited to such activity. Another reason cyberspace has become a key means of espionage is that state-sponsored intelligence organizations use it in the pursuit of state-sponsored goals – political, security, technological, and economic – as do criminal outfits pursuing purely economic gain. Much information has emerged about cyberspace espionage between states, especially cyber skirmishes between the United States and China, indicating that commercial espionage has become a primary tool of states in general and the powerful ones in particular, serving as a weapon in their economic wars and pursuit of global dominance.

As a state rich in advanced technology, Israel is very much at risk. The vast amounts of information created by financial, scientific, and other institutions within the state are stored, moved, and managed in cyberspace, and are therefore accessible to a variety of attackers. In addition, the part played by innovation-based industries and unique intellectual property in the Israeli economy is highly significant. Israel is a global leader in startup industries, which by their very nature generate additional motivation for commercial espionage against Israel. Given that advanced persistent threats (APTs) are rarely discovered by standard security measures of commercial companies, Israeli companies, especially those developing unique knowledge, presumably constitute targets for commercial espionage and the theft of intellectual property, as is the case in other technologically advanced countries.

The purpose of this article is to examine the use of cyberspace for commercial espionage and theft of intellectual property. The article seeks to underscore the complexity in assessing the extent of these phenomena and the economic damage they cause. Finally, the essay seeks to analyze the scope of commercial espionage in Israel in order to raise awareness of the phenomenon in the public discourse and thereby promote action to curtail it and as a result contain the damage it incurs.

Cyberspace as a Medium for Commercial Espionage

While commercial espionage has existed since the dawn of history, the transition of much of the business world to the cyber realm has propelled commercial espionage to this arena as well. Indeed, cyberspace is ideally suited to espionage, particularly commercial espionage. It allows relatively anonymous activity, including convenient and safe transmission of vast amounts of information regardless of distance and national borders. At the same time, it is very difficult for the victims of espionage – be they commercial or government bodies – to detect its occurrence. Even if the victims are aware of the attack and identify the spyware used to effect it, it is hard for them to attribute the malicious action to a particular culprit and credibly establish the responsibility and identity of the attacker.

Commercial espionage in cyberspace costs very little compared to other means of intelligence gathering, and entails a low level of risk of exposure. Cyberspace espionage greatly reduces the need for agents to infiltrate the target, and thus intelligence entities throughout the world can amplify

their capabilities, in terms of intelligence gathering within cyberspace[5] and the integration of traditional forms of espionage with new capabilities in this sphere. As such, espionage becomes simpler for the attacker and more dangerous for the attacked. For example, espionage involving a mole working for the organization under attack becomes simpler in the cyberspace era: transmitting stolen information is easier and identifying its source is harder. Furthermore, law enforcement has a lenient approach to cybercrime, thus reducing the risk taken by those engaged in commercial espionage. A burglar caught breaking and entering a physical place of business to steal information will probably have to pay a much higher price than someone stealing the same information using a keyboard.

Commercial espionage may be defined as the unauthorized possession of confidential commercial information not revealed to the public at large, for the purpose of attaining a technological advantage or economic gain. Such information may include data on strategy, planning, technological innovation, product development processes, manufacturing and marketing processes, advertising campaigns, financial status, legal issues, key personnel, salary information, tenders and bids data, and more. Targets might include not only competing organizations but also academic research institutes and other entities possessing valuable information. Unlike information gathering from open sources, obtaining the information often entails criminal offenses. This activity is only one branch of a larger group of economic crimes, such as embezzlement, fraud, theft, disruption of business activity, and more. Commercial espionage by a state is usually intended to strengthen the state's own economy, to create an economic advantage for that state or a sector of its economy in relation to competing sectors around the world.

The rise in the scope of commercial espionage in cyberspace reflects the technological, economic, and social changes that have occurred in recent years and the corresponding manner in which information is created, moved, stored, and managed in economic and scientific organizations, including sensitive bodies. Throughout the world, almost all commercial and scientific records, even the most sensitive, are digitally stored and accessible to computer networks. Given this pattern and given the advantages currently available to hi-tech attackers such as state-sponsored intelligence organizations or sophisticated criminal syndicates, these groups can use cyberspace to carry out theft of commercial and business

information. Such thefts are on a scale that far outstrips any past commercial espionage, both in terms of the importance and sensitivity of the stolen information to its owners and in terms of sheer quantity.

Experience has shown that only a few companies can identify hi-tech attacks carried out by state-sponsored espionage organizations or sophisticated crime syndicates. Even fewer are capable of effective defense.[6] There are many examples indicating that even the most sensitive companies in the defense industry in the United States were relatively easy targets for commercial (or security) espionage through the internet by state-sponsored organizations, apparently out of commercial motives.[7]

A report by ONCIX (the Office of the National Counterintelligence Executive) to the US Senate[8] addressed the threat of theft of commercial information and key rivals carrying out such activity in the United States. China and Russia were described as having the highest capabilities in the field and being "the most aggressive collectors of US economic information and technology."[9] A July 2012 report to the Congress by the same agency[10] cites Congressional testimony by Director of National Intelligence (DNI) General James R. Clapper regarding the US intelligence community's national threat assessment. Clapper testified that intelligence agencies of enemy nations are systematically developing methodologies and technologies to challenge the capabilities of the administration and private sector in the United States that protect national and commercial secrets.[11] Indeed, the 2013 US threat assessment put cyber threats at the top of the list of threats facing the United States,[12] ahead of terrorism and the proliferation of weapons of mass destruction.

The Complexity in Assessing the Damage of Commercial Espionage

Given the very nature of commercial espionage, assessment of the damage it causes is difficult for various reasons, including first and foremost the methodological problem of quantifying the scope of damage resulting from the loss of intellectual property and the fact that only a tiny fraction of all advanced espionage activity ever comes to light. In testimony before a US government committee, Richard Bejtlich, Chief Security Officer at Mandiant,[13] a company specializing in incident response and computer forensics solutions and services for government, defense, and enterprise organizations, said that of the total number of sophisticated

espionage attacks originating in China investigated by his company, only 6 percent of the attacks were discovered by the targets. This indicates that a tremendous gap exists between the prevalence of the phenomenon and an accurate appreciation of the cost to the economy resulting from commercial espionage.[14] Furthermore, sophisticated organizations engaged in commercial espionage in cyberspace use specific spyware that are incapable of being identified, blocked, or neutralized by the standard defensive tools of most commercial enterprises. Today, cyberspace favors the attacker by a wide margin.

Many espionage agencies use cyberspace as a key information-gathering arena. The capabilities developed by security agencies for this purpose far outstrip current defensive responses to these threats. Furthermore, focused, dedicated attackers also enjoy the advantage of being able to learn about and even obtain the defenders' security tools,[15] enabling them to run simulations in order to identify the conditions under which they will not be exposed by the very security tools the defenders are using.[16] In addition, state-sponsored espionage is carried out by intelligence groups designed for this purpose, whereas effective defense requires comprehensive, state-sponsored activity that involves security outfits and non-security organizations from both the government and the private sectors – an effort that is, by nature, slow and cumbersome.

The FBI has estimated that for every incident of penetration into computer networks identified by a US company, one hundred similar incidents have occurred that the computer networks failed to identify.[17] A report by Mandiant published in February 2013[18] stated that the goal of the Chinese attack formation was commercial espionage and that in that year it had attacked 141 Western companies, primarily in the United States. This is an example of commercial espionage activity carried out by a state-sponsored body that had been operating for years and eluding public awareness until the publication of the report.[19] On the basis of this example, one may infer that other companies coming under attack by sophisticated formations almost always fail to identify the attack. Even on the rare occasion when they realize they have been attacked, the attack is not made known to the public and the economic and security implications are not studied in the overall national context.

In the few cases in which companies and other organizations realize they are targeted and even manage to identify the spyware installed on

their computers, they are hard pressed to assess the scope and type of information that has already leaked through their networks. Failure to protect the company's or organization's assets often means that those in charge of security in these outfits tend to downplay the damage caused by the espionage. When unknown software – that is, malware – is discovered on the company's computers, the natural inclination is to remove it and make sure that the system continues to work. Only rarely will a company carry out a comprehensive forensic investigation aimed at uncovering the true nature of the attack and identifying the tools used to carry it out, as such an investigation is very costly – both in financial terms and in terms of the time needed to carry out a forensic investigation, during which the company's computer communications are severely compromised. Even when a full, professional forensic investigation is successfully conducted and the company's management receives a full, reliable picture of the theft of commercial data, often the organization will prefer not to make the theft publicly known or will at least seek to minimize the damage assessment, in the hopes of reducing the damage to the company's reputation that would result from a complete description of the theft. Damage to the company's reputation would, of course, endanger the company's relationship with its shareholders, investors, suppliers, customers, and all other stakeholders.

Finally, there is an inherent difficulty in assessing the financial worth of intellectual property. Clearly it is not necessarily reflected in the value of the investment that went into creating it, and this is probably the most precise statement one can make on the subject. The value of future income denied to a company as the result of information theft through cyberspace is entirely subjective and grounds for wild speculation.

For these and other reasons, it is extremely difficult to assess the cumulative damage caused to an organization as a result of commercial espionage in cyberspace. This difficulty is intensified when one tries to assess the financial damage the phenomenon causes the state, and thus assessments of damage to the state from commercial espionage in cyberspace vary wildly.

Methods of Assessing Commercial Damage

Various studies of the costs of commercial espionage have attempted to propose methodologies for damage assessment. The vast gaps in knowledge stemming from the above mentioned reasons as well as the

inherent difficulty in closing those gaps pose an obstacle to any attempt to assess the scope of the phenomenon.

It is customary to divide the cost of cyberspace crime into three main categories:[20] *defense cost*, such as security, compliance with standards, and insurance; *direct cost*, such as damage to functionality, repair of the damage, loss of work time, resolution of the breaches, reconstruction of information, direct losses to the business, compensation to customers, fines, and legal issues; and *indirect cost*, such as loss of customer trust, loss of future business and income, or damage to the company brand.

The various approaches to damage assessment are based on surveys and theoretical analyses. In the studies based on surveys, sample groups of executives and IT specialists in commercial ventures are asked to provide damage assessments, from which overall assessments are extrapolated. The problem with this approach is the profound gap between the respondents' understanding of the issue and the scope of the phenomenon in practice. This gap is even more pronounced given that the sample group is liable to be biased. Those who have suffered painful attacks tend not to share their experiences and are therefore likely not to participate in surveys of this type. Accordingly, the studies must correct for these factors, which in itself has a dramatic effect on understanding the scope of the phenomenon.

The theoretical approach uses a model based on calculations drawing on open data, hypotheses, and assessments by information security experts, businesspeople, economists, and law enforcement agencies. This model too suffers from a gap between the quality of available information and true data; it also relies heavily on assessments. One example of such research is a study of the cost of cybercrime conducted by Detica in England.[21]

Threat assessment and measurement are critical for understanding the phenomenon of theft in cyberspace and for the optimal allocation of resources to defend against it. Therefore it is in the best interests of both commercial enterprises and states to assess the damage they face from information theft. Gen. Keith Alexander, Commander of the US Cyber Command and the Director of the NSA, has claimed that US companies lose some $250 billion annually as a result of cyber theft of intellectual property.[22] Citing a report published by Symantec, he said, "Symantec placed the cost of IP theft to the United States companies [at] $250 billion a year, global cybercrime at $114 billion annually ($388 billion when you factor in downtime)."[23] A report by the Commission on the Theft of

American Intellectual Property estimates that the damage caused by cyber theft exceeds $300 billion a year.[24]

Countries other than the United States are also trying to assess the scope of the phenomenon. The Federal Office for the Protection of the Constitution in Germany assesses that German companies annually lose $28-71 billion and 30,000-70,000 jobs because of foreign economic espionage. South Korea has reported that the costs of economic espionage carried out by foreign entities in 2008 totaled $82 billion, compared to $26 billion in 2004. According to this report, 60 percent of the victims were small to medium-sized companies, and half of the cases of commercial espionage could be traced to China. In 2007, the Japanese Ministry of Economy, Trade, and Industry undertook a survey among 625 exporting companies and found that more than 35 percent of them reported the loss of some technology, and that more than 60 percent of the reported incidents were linked to China. Official sources in Great Britain have assessed that attacks on computer systems, including industrial espionage and theft of commercial information, cost the British private sector some $34 billion a year. More than 40 percent of this sum stems from the theft of intellectual property, such as specifications, formulas, and proprietary company information.[25]

Table 1: Assessments of Damage Resulting from Economic Espionage in Select Countries

Country	Assessment of annual damage (in $ billion) caused by theft of commercial information and intellectual property	Scope of damage in terms of percent of GNP
United States	250-300	1.67-2
South Korea	82	7.3
Germany	28-71	0.8-2
Great Britain	34	1.4

At the same time, those offering the estimates did not explain how they had arrived at their damage assessments, probably because of the difficulty in estimating the direct, not to mention the indirect costs of cybercrime. One must also take into account that those undertaking damage assessment studies, particularly certain information security companies, are liable to have a vested interest in inflating the scope of the phenomenon.

A study published by McAfee in July 2013[26] attempted to address the complexity of assessing the cost of cybercrime. The study questions published cost assessments and offers lower assessments than the official estimates of damage to the US economy. The study does not include definitive assessments of the cost of such damage, but points out, for example, that the upper limit of damage to the US economy claimed by one method of assessment is anywhere between 1/2 to 2 percent of the GNP,[27] whereas another method of assessment places it at lower than 1 percent of the GNP.[28]

Commercial Espionage in Israel

As a state rich in advanced technology, Israel is particularly vulnerable to threats in cyberspace in general and commercial espionage in particular. A great deal of Israeli export relies on companies highly dependent on intellectual property, thereby making Israel a target for the theft of this sort. Furthermore, the role of industries based on innovation and unique intellectual property in the Israeli economy is very significant. Israel is a global leader in startups, which invites further motivation for commercial espionage against Israel. In addition, the commercial sector in Israel has little awareness of the risks of cyberspace espionage and prefers convenience, functionality and exploitation of business opportunities rather than security. Presumably, therefore, as in other developed countries, commercial enterprises in Israel – especially those developing unique knowledge – are targets for commercial espionage and the theft of intellectual property. Of the 141 companies attacked by the Chinese attack formation APT1, as described by Mandiant, three were Israeli.[29]

Israel was a world leader when it came to understanding cyberspace-based threats to critical infrastructures, but not when it came to grasping cyber threats to the business world. As early as 2003, the state established the National Information Security Authority,[30] charged with securing Israel's critical infrastructures against cyberspace attacks and preventing the theft of state secrets. The Israeli business sector and the public at large did not benefit from similar attention, and currently no organization has the responsibility of protecting these entities against commercial espionage in cyberspace. As a result, Israel today lags behind many other countries in the world, including the United States, when it comes to protecting the business sector. Other countries reached the conclusion that state-

sponsored protection of national commercial assets is a high priority and that they are responsible for providing the scaffolding for responding to cyberspace threats to the economy in general and the private sector in particular. This realization has led to the establishment of one or several state agencies charged with leading state-sponsored defensive activity in cyberspace in order to strengthen overall protection in the field.[31]

It is hard to assess the damage caused to the Israeli economy by commercial espionage. There is no obligation to report the discovery of information-gathering tools in company computers, other than minimal guidelines for the population registry and regulation for special sectors, such as banks and bodies within the purview of the National Information Security Authority, and with respect to the authority overseeing security in the defense establishment. Furthermore, in Israel, companies are under no legal obligation to report the loss of sensitive business information,[32] and there is no organization charged with defending the business sector in cyberspace, whose job it would be to collect such information and use it in order to draw conclusions and strengthen overall defensive responsiveness. Consequently, the likelihood of identifying commercial espionage in cyberspace in Israel and accurately assessing its scope is very slim. This state of affairs presumably also accounts for the dearth of reports on theft of commercial information and intellectual property from Israeli companies.

Despite the difficulty of assessing the damage caused by attacks in cyberspace, Israeli businesses and organizations are presumably just as exposed to commercial theft as those of other developed nations, both because of Israel's image as a global leader in the development of innovative knowledge and because of the lacunae in defense and protections noted above. Even using conservative estimates – namely, that commercial theft in cyberspace accounts for one percent of the GNP – the annual damage of such crime in Israel reaches roughly $2.5 billion. Preliminary research on the damage of commercial espionage in Israel, undertaken for the National Cyber Command by Meidata, a market research company, assesses the annual damage to the Israeli market from commercial espionage to be in the $1-3 billion range. There is no doubt that damage on this scale, which increases from one year to the next, requires a national response and justifies significant investment in the defense of companies and

organizations under attack, which currently bear the lion's share of the cost of commercial espionage.

Conclusion

The State of Israel, with its high level of security awareness, was a pioneer in understanding the security risk developing in cyberspace, even before any damage to its critical infrastructures was actually identified. Nonetheless, to date the danger posed by the theft of trade secrets and intellectual property from commercial companies in Israel has not been recognized as a significant threat to the country's stability, even after clear evidence has emerged proving that nations and criminal syndicates, equipped with the most sophisticated tools in existence, use cyberspace to commit commercial espionage and that this state of affairs has far reaching economic ramifications for commercial companies and countries.

The economic threat to commercial companies from commercial espionage has been defined by the head of the US intelligence community as a concrete threat against the United States of the highest order, ranked ahead of terrorism and the proliferation of WMDs. The cost of damage incurred from commercial espionage in cyberspace is high and on the rise, and it is borne primarily by the business community. According to various studies, the component represented by the cost of commercial espionage is the most dominant in the total of all types of cyberspace crime.[33] Israel, whose economy is to a large extent driven by innovative knowledge, is also vulnerable to the threat of cybercrime, including commercial espionage.

It is very difficult to assess the damage incurred by commercial espionage in cyberspace. Therefore we see a very broad range of assessments generated by a variety of reports. The difficulty in assessing damage empirically and the extensive reliance on assessments by experts seeking to address major gaps in the quality of collected data constitute obstacles to all methods of assessing the damage caused by commercial espionage and account for the vast discrepancies among various damage assessments. Nonetheless, these assessments are necessary in order to understand the impact of commercial espionage, and they provide the basis for states' comprehension of the phenomenon and their attempts to thwart it.

A strong methodology that would provide the tools for reliable assessments of the damage discussed by this essay is highly necessary.

Development of this methodology would increase awareness of the need to improve protection against the threat and the ensuing damage. Toward this end, first and foremost it is necessary to improve the ability to gather reliable information about the phenomenon by means of mechanisms for reporting cyberspace incidents. Furthermore, it is necessary to develop better assessment tools that address existing gaps between reports and assessments surveying the number of incidents and resulting damage on the one hand, and reality on the other. This is an inherent gap in knowledge, because in most cases the attacked parties are not aware that they have been attacked and that information about their business has been stolen; they are therefore incapable, even after the fact, of linking damage to their business to information theft about which they knew nothing in the first place. In addition, improving the overall civilian responses in cyberspace in Israel, while also establishing an agency charged with responsibility for the matter, could allow for the development of a comprehensive doctrine for addressing commercial theft in cyberspace based on a broad view of national needs.

The goal of this essay is to shed light on the phenomenon of commercial espionage in cyberspace and the damage it causes to the Israeli economy. In the absence of in-depth studies of the phenomenon, its precise scope remains elusive, but it is reasonable to conclude that it has a significant impact on the Israeli economy and is steadily increasing. The response to the phenomenon must include a range of efforts, including but not limited to the following: focused research on the scope of the phenomenon and a breakdown by sector; improved security for the business sector; the development of a cyberspace security industry; and state-sponsored measures providing a response to commercial espionage throughout cyberspace, including cooperation and arrangement with other states suffering similarly from the phenomenon.

Commercial espionage in cyberspace demands a complex response and requires tremendous resources. Raising the level of awareness regarding the phenomenon, both in the business world and among the decision makers in Israel, appears to be a necessary precondition for engaging in efforts to reduce the damage caused by cybercrime in general and by commercial espionage in particular. It will then be possible to bring Israel's defensive cyberspace capabilities to bear against the entire gamut of threats.

Notes

1 Nicole Perlroth, "Nissan is Latest Company to Get Hacked," *New York Times*, April 24, 2012, http://bits.blogs.nytimes.com/2012/11/30/study-may-offer-insight-into-coca-cola-breach/?_r=0.

2 Carrie Lukas, "It's Time for the U.S. to Deal with Cyber-Espionage," *US News*, June 4, 2013, http://www.usnews.com/opinion/articles/2013/06/04/chinas-industrial-cyberespionage-harms-the-us-economy.

3 For example, by making changes to computerized command and control systems of industrial processes so that damage is caused to the industrial process or to the industrial systems themselves.

4 Francois Paget, "2014 Threats Predictions: Cybercrime and Hacktivism Will Continue to Grow," McAfee Labs, January 8, 2014, http://blogs.mcafee.com/mcafee-labs/2014-threats-predictions-cybercrime-and-hacktivism-will-continue-to-grow.

5 The most prominent example of surveillance carried out entirely in cyberspace is the global PRISM system of the NSA, whose existence came to light thanks to Edward Snowden's revelations. The NSA's surveillance was allegedly carried out for the sake of the security and safety of US citizens. However, there are reports charging that industries of interest to the United States, especially in the field of advanced security capabilities, were also placed under surveillance. See Glenn Greenwald and Ewen MacAskill, "NSA Prism Program Taps in to User Data of Apple, Google and Others," *The Guardian*, June 7, 2013, http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data; and Scott Shane, "No Morsel Too Minuscule for All-Consuming N.S.A.," *New York Times*, November 2, 2013, http://www.nytimes.com/2013/11/03/world/no-morsel-too-minuscule-for-all-consuming-nsa.html?pagewanted=1&_r=0.

6 Mandiant Report, "APT1 Exposing One of China's Cyber Espionage Units," February 2013, http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.

7 See, for example, the successful cyber attack in 2011 on Lockheed Martin with the aim of stealing plans for the advanced F-35 stealth aircraft.

8 Office of the National Counterintelligence Executive, *Foreign Spies Stealing US Economic Secrets in Cyberspace, Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011, Annex B – West and East Accuse China and Russia of Economic Espionage*, October 2011, http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf.

9 Ibid., p. 4.

10 *Foreign and Economic Espionage Penalty Enhancement Act of 2012*, House of Representatives Report 112-610, 2012, http://www.fas.org/irp/congress/2012_rpt/ecoesp.pdf.

11 James R. Clapper, Director of National Intelligence, "Unclassified Statement for the Record on the Worldwide Threat Assessment of the US Intelligence

Community for the Senate Select Committee on Intelligence," January 31, 2012, p. 8, http://www.intelligence.senate.gov/120131/clapper.pdf.

12 James R. Clapper, Director of National Intelligence, "Statement for the Record on the Worldwide Threat Assessment of the US Intelligence Community, Senate Select Committee on Intelligence," March 12, 2013, http://www.intelligence.senate.gov/130312/clapper.pdf.

13 In January 2014 Mandiant was bought by FireEye.

14 Devlin Barrett, "U.S. Outgunned in Hacker War," *Wall Street Journal*, March 28, 2012, http://online.wsj.com/article/SB10001424052702304177104577307773326180032.html.

15 In most cases, the security tools are standard commercial tools.

16 Mandiant Report, "APT1 Exposing One of China's Cyber Espionage Units."

17 "America's Top Cyberwarrior Says Cyberattacks Cost $250 Billion A Year," *International Business Times*, July 13, 2012, http://www.ibtimes.com/americas-top-cyberwarrior-says-cyberattacks-cost-250-billion-year-722559.

18 Mandiant Report, "APT1 Exposing One of China's Cyber Espionage Units."

19 In the report, the company notes that it investigated dozens of advanced attack formations, of which more than 20 had similar characteristics and all originated in China. For reasons of its own, the company chose to relate to only one such formation in its report.

20 R. Anderson, C. Barton, R. Böhme, R. Clayton, M. van Eeten, M. Levi, T. Moore, and S. Savage, "Measuring the Cost of Cybercrime," in *Workshop on the Economics of Information Security*, WEIS, 2012, http://weis2012.econinfosec.org/papers/Anderson_WEIS2012.pdf.

21 Detica, *The Cost of Cyber Crime*, A Detica Report in partnership with the Office of Cyber Security and Information Assurance in the Cabinet Office, UK, 2011, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60942/THE-COST-OF-CYBER-CRIME-SUMMARY-FINAL.pdf.

22 "America's Top Cyberwarrior Says Cyberattacks Cost $250 Billion A Year."

23 Emil Protalinski, "NSA: Cybercrime is the Greatest Transfer of Wealth in History," *ZDnet*, July 10, 2012, http://www.zdnet.com/nsa-cybercrime-is-the-greatest-transfer-of-wealth-in-history-7000000598/.

24 The IP Commission Report, *The Report of the Commission on the Theft of American Intellectual Property*, http://www.ipcommission.org/report/IP_Commission_Report_052213.pdf.

25 Office of the Counterintelligence Executive, *Foreign Spies Stealing US Economic Secrets in Cyberspace*.

26 McAfee, *The Economic Impact of Cybercrime and Cyber Espionage*, Center for Strategic and International Studies, July 2013, http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime.pdf.

27 Ibid., p. 14.

28 Ibid., p. 15.

29 Mandiant Report, "APT1 Exposing One of China's Cyber Espionage Units."

30 The National Information Security Authority, established in accordance with a December 2002 government decision, is subordinate to Israel's General Security Services.

31 Overall responsibility for national defense in the United States falls on the Department of Homeland Security, which works in very close cooperation with the Department of Defense (which includes intelligence agencies, such as the National Security Agency and the Office of the National Counterintelligence Executive, that are very active in defending cyberspace against attacks and commercial espionage), the Federal Bureau of Investigation, and the Department of Justice.

32 Cyberspace theft from publicly held companies in Israel, which is liable to affect their activities or assets, might give rise to an obligation to inform the stock exchange, as such information could potentially affect the considerations of reasonable investors in deciding whether to buy or sell their company shares.

33 Detica, *The Cost of Cyber Crime*, p. 3.

Blood and Treasure: On Military and Economic Thinking

Saul Bronfeld

In memory of Reserve Captain Avner Ben Eliezer, a brilliant economist in the Research Department of the Bank of Israel, who fell in defense of the Budapest outpost in the Yom Kippur War as a deputy company commander, Battalion 141, reserve Brigade 204

This article argues that there is little difference between military thinking and true economic thinking, which is different from accounting-budgetary thinking. Most of the substantive disagreements between military commanders and economists stem from objective difficulties in predicting the future and quantifying the important components of risk, cost, and benefit. Other disagreements result from vested interests or mere egotistical issues. The article will also explore the problematic manner in which the defense budget is drafted, specifically, the lack of clear directions from the cabinet regarding national security posture and priorities and the absence of significant military bodies outside the defense establishment. Reforms instituted in the United States during Robert McNamara's term as Secretary of Defense and as a result of the Goldwater-Nichols Act of 1986 are instructive in this regard. In 2007, the Brodet Committee attempted to change the process for drafting the defense budget, but was not successful.

Keywords: defense economics, defense budget, risks, cost-benefit, Robert McNamara, Pinhas (Siko) Sussman, Brodet Committee

Saul Bronfeld served as CEO and chairman of the Tel Aviv Stock Exchange from 1991-2013. He holds an MA in Security Studies (2005, summa cum laude) from Tel Aviv University and is an adjunct lecturer in the Faculty of Management at Tel Aviv University.

Background

An observer of the annual ritual of deliberations on the defense budget is liable to reach the conclusion that economic and military thinking are two parallel disciplines, and that never the twain shall meet. The military has been known to quip that "economists know the price of everything and the value of nothing," and "Iran is the adversary, and the Ministry of Finance is the enemy." In their unending dispute with economists, military leaders can draw on Professor Edward Luttwak, one of the greatest military thinkers, who contended that "in the realm of strategy...economic principles collide with the demands of war-effectiveness."[1]

In turn, economists retort that "the army is prepared to ruin the economy and society in order to maintain its beloved order of battle," and that "a cut in the defense budget will only prevent waste and will not harm defense."[2]

The debate between military commanders and economists is not merely academic or a question of semantics. It is a disagreement over allocation of resources and national priorities that stems from differing assessments of strategic risks, different world views, and also from parochial interests, as well as egotistical issues.

This article will attempt to present economic thinking in the proper light, arguing that when true economic thinking is applied, as opposed to accounting-budgetary thinking, there is almost no difference between the two disciplines – economic and military. The article will also show that a significant part of the substantive debate between military commanders and economists results from objective difficulties in predicting the future and in quantifying important components of cost and benefit. Finally, the article will argue that the main reason for the stormy nature of deliberations on the defense budget is the problematic process of drafting the budget: the lack of orderly cabinet deliberations and clear guidelines concerning national security posture, objectives, risks, and priorities, and the lack of civilian agencies that assist the government and the Knesset in drawing up the policies and budget. Reforms instituted in the United States during Robert McNamara's term as Secretary of Defense and as a result of the Goldwater-Nichols Act of 1986 are instructive in this regard.[3] In 2007 the Brodet Committee attempted to change the process in Israel, to no avail.

Fundamental Similarities between the Military and Economic Disciplines

On the face of it, there should be no difference between military thinking (by a "commander") and economic thinking (by an "economist"). The military command echelon presents the required achievements to the commander and equips him with limited resources to carry out the mission. The commander is expected to use thinking processes (algorithms, as it were) to produce a plan of action that will achieve the desired objective, which is usually worded in terms of captured territory, lines reached, destroyed enemy forces, and timetables. The resources placed at his disposal are military units of various sizes and different types. A good example is the preparation of the Moked plan in the first half of the 1960s to attack Egypt's military air fields; the Israeli Air Force used this plan to destroy the Egyptian Air Force on June 5, 1967, thus sealing the fate of the Six Day War. The plan was a good example of military thinking – a sophisticated algorithm that, with the help of a limited number of aircraft, led to great achievements, even exceeding expectations.

Economists are expected to use an algorithm to produce a profitable business plan. The investors (shareholders) provide the economist with a budget to set up a new factory or develop a new product, and they expect the economist to achieve a certain rate of return on investment within a pre-defined period. Thus, for example, Israel Corporation made hundreds of millions of dollars available to the CEO of Better Place in the hope that it would succeed in selling electric cars based on an innovative logistic system.

Both examples involve the application of algorithms by the commander or the economist in order to delineate the optimal path towards a goal, be it a military objective or profitability target. In each discipline the algorithm, which represents the theory relating to the issue that must be addressed, combines with the personality of the executive, be it the commander or the economist.

For our purposes, it is important to underscore the similarity of the environments in which the commander and the economist operate. First and most important, both work in a hostile environment. By definition, the military operates against an adversary that seeks to prevent it from implementing its plans (and kill the commander and his men as well), while the commander never has all the intelligence required. Similarly, the

economist works in a hostile environment, which includes competitors who are sometimes very cruel ("cut-throat competition"). The more successful the economist is, the greater the competitors' incentive to harm him. He must predict their response, even though some of them he does not know at all. Furthermore, large profits make the economist vulnerable to challenges from labor organizations, tax authorities, other regulators, social activist organizations, and class action lawsuits.

Second, the commander and the economist live with uncertainty and are constantly required to predict what their opponent and those around them will do. The commander has incomplete information but must still assess his opponent, including the opponent's capabilities and methods of operation, and even variables such as the weather. Assessing the adversary's intentions and the rationale for his actions is not a simple matter, as the history of the Yom Kippur War demonstrated: Israel paid a very heavy price for failing to understand the strategic rationale of President Sadat, even though it had good intelligence regarding the capabilities of the Egyptian military.

The need to cope with a hostile environment under conditions of uncertainty translates into a strong correlation between the military objective or the required return and the risk involved. This correlation is captured in the saying that a person who wants to eat well should invest in stocks, while a person who wishes to sleep well should invest in bonds.

Landing troops behind enemy lines is a clear example of the correlation between yield and risk: the IDF's crossing of the Suez Canal in October 1973 was the most important success of the Yom Kippur War, even though initially there was a strong risk that the force crossing the canal would be cut off and encircled. (The IDF high command had concluded that the risk involved in attempting a crossing prior to October 14, 1973, before the Egyptian armored divisions had crossed into Sinai, was too great, and rejected recommendations that entailed crossing the canal earlier.) Also worth noting is the Entebbe operation to free the hostages of the Air France plane hijacked to Uganda in 1976, which was very risky but ended with unprecedented success (unlike Operation Eagle Claw, the US attempt to free the hostages in Tehran in 1980).

There are many familiar examples of the close economic correlation between risk and return. Investments in oil prospecting, hi tech, and foreign markets involve great risk, but when they succeed, they yield large profits.

However, for every company like Check Point, which became the global leader in cyberspace security, there are many companies like Better Place, which in effect consumed hundreds of millions of dollars and ultimately filed for bankruptcy.

Parenthetically one might add that for both disciplines, the close correlation between accomplishments and risks creates dizzying successes and resounding failures. Both are subject to the phenomenon of perfect hindsight, in the negative sense. In the military, perfect hindsight refers to the conclusions that should have been drawn from raw intelligence that can pinpoint precisely the adversary's first signs of breaking as well as the optimal moment to initiate the counterattack. Those with perfect hindsight are never surprised in retrospect. In economics, the after-the-fact geniuses always know the right time to enter or leave the stock market. They always know how to earn a profit, after the fact.

The Similar Toolboxes

Military and economic endeavors are human, intellectual tasks. In both, the operators must cope with limited resources and use algorithms that weigh the cost and benefit of alternative methods of operation and choose the best of them. The commander chooses a certain path in the hope that it will be optimal for conquering a target or thwarting an attack, and the economist chooses an option that he believes will improve the cost-benefit ratio. Given the similar processes described above, it is no wonder that the commander and economist have similar toolboxes, as the following examples illustrate.

The Combined Arms Battle and the Diversified Investment Portfolio

The military concept of integrating branches and corps on the battlefield has a long history, as does the concept in economics of not putting all your eggs in one basket. Diversification of investments and the integrated battle achieved sophisticated conceptualization in the twentieth century, but they have always been part of the old practice: "A man should always divide his wealth into three equal parts: one third for real estate, one third for commercial stock, and one third on liquid assets," according to the Talmudic sage Rabbi Isaac. Hundreds of years earlier, armies were already integrating their infantries with cavalry and chariots, the bow with the sword, the spear, and the stone, and the land forces with ships.

The variety of weapons has increased over the course of history, as has the range of investment instruments, but the principle guiding the two disciplines has remained similar: integration in the army, like diversification of investments, turns the whole into more than the sum of its parts. The different types of integrated battle were intended to expose an adversary that was well prepared for one type of weapon system to a crushing blow from a different system. For example, a modern integrated air defense system appeared for the first time in the Vietnam War (and immediately afterwards, in the War of Attrition in Israel). It included various types of radar, ground-to-air missiles, anti-aircraft artillery, and fighter jets. American planes that attempted to attack targets in North Vietnam from a high altitude had difficulty coping with the missiles, and when they attempted to attack from a low altitude, they encountered deadly anti-aircraft fire. At the same time, the enemy's fighter jets intercepted the attack aircraft, forcing them to jettison their bombs. The combined engagement of all of North Vietnam's air defense assists resulted in a situation in which the benefit of the air strikes on North Vietnam was small while the costs, in terms of loss of American air crews and aircraft, was very high.

An investment portfolio containing assets with various risk-return profiles that offset each other's volatility, preventing a steep drop in the value of the portfolio during an economic downturn on the one hand, and a surge in its value during an upswing on the other, is of crucial importance. Although the fundamental logic underpinning the integrated battle is not the same as that of investment diversification, the result is the same: in both disciplines, the integration or diversification improves the ability to cope with the complexity and uncertainty of confronting a hostile environment.

Israeli history provides many examples in both fields: the lack of artillery and armored infantry in the Yom Kippur War caused heavy tank losses on the Suez Canal front. In contrast, the conquest of the Egyptian positions in Umm Katef in the Six Day War is a good example of a battle integrating infantry with armor, artillery, and a heliborne force. In economics, there is no lack of examples of unbalanced investment portfolios that inflicted a heavy blow on their owners. This is what happened in the crisis of the "regulated" bank shares in Israel during the late 1983, in the hi tech stock crash in 2000, and in the burst of the real estate bubble in 2008. On the

other hand, an investor holding government bonds can always get cash even at the height of a crisis, by selling them without a loss.

Risk Management

Over the past generation advanced quantitative methodologies that use sophisticated statistical tools have been developed for risk management, but these methodologies are effective only in those few areas in which there are numerous observations. Because of the tremendous importance of risk management, for lack of an alternative it is often implemented using qualitative tools as well, even though these do not meet the strict definition of the concept. Non-quantitative risk management has assumed various forms in the military: scenario-based thinking, sensitivity analysis, "red teaming," the devil's advocate function, cases and responses, and more. On many subjects, especially in the realm of strategy, risk management is qualitative, since it is not possible to quantify the probabilities of the scenarios and the damages caused when negative scenarios come to pass.

The situation in economics is not much better, even though there are a number of areas in which quantitative risk management can be applied (for example, the world of insurance and the hedging of certain financial risks through the use of options and future contracts). In both disciplines, risk management involves on the one hand assessing the probability of various scenarios and the possible results in every scenario, and on the other hand, what is called "risk appetite" (that is, willingness to take a risk in order to achieve a certain goal). We can view the assessment of probabilities as a professional measure carried out by the military staff (or the management), and risk appetite as a decision by the political leaders who direct the commander or by the shareholders who guide the economist. Risk appetite determines the point where one wants to be, taking into account the close correlation between risk and returns.

An example from the military realm is the decision by the political leaders in 1976 to launch an operation to free the hostages at Entebbe in spite of the great risk involved in such a complex operation. An opposite example is the Israeli government's decision not to respond to Egypt's ceasefire violations in the Suez Canal in August 1970, among them Egypt's positioning of its ground-to-air missile batteries near the canal. It would appear that after three years of the War of Attrition, Israel's risk appetite was very small.

Risk appetite in economics is reflected, for example, in a real estate company's willingness to finance its activities through loans ("degree of leverage"). The greater the credit leverage, the greater the expected profitability from real estate investments. However, as evidenced in the crisis of 2008, high leverage led to bankruptcy for many companies.

The Principles of War and Economics

The conceptual similarity between the two disciplines and their common toolbox are reflected in the similarity of principles guiding commanders and economists, which differ only in semantics. The following examples illustrate this point:

a. *Time to market* is an economic principle that emphasizes the importance of both initiative and speed, which introduce a new product into the market even if its development has not yet been completed. The benefit of being first is enormous, as it provides an advantage over competitors. Therefore, it is worth taking the risk that the first product to enter the market will be criticized for not being sufficiently developed. The parallel military principle is to take advantage of the fog of battle and strike quickly, even with one company, and achieve something that even a brigade would find difficult to achieve in a later, orderly battle. Here, too, there is a risk that if the assaulting force is too small, it will be destroyed.

b. *The law of diminishing marginal returns* states that increasing input does not always increase output at a similar rate. As every student of economics knows, increasing the number of workers in a certain field does not increase the yield at the same rate (and could even reduce it – "negative marginal return"). A similar military principle prevents a commander from using his reserves for reinforcement in a battle that is deadlocked, and holds that he should consider using the reserves in a more effective way instead, with a different area or at a different time.

c. *Reward and punishment*: Those who take the initiative and weigh the risks correctly are rewarded in economics by large profits and bonuses, and in the army, through citations and promotion. In contrast, economic failure leads to bankruptcy, and failure in the military leads to a demotion rather than a citation (and sometimes also to death in battle).

d. *The law of comparative advantage* holds that an entity should specialize in activities in which it has an advantage over the competition. The classic, long-standing example for Israel – though less applicable today – was the idea that Israel should focus on growing oranges and tourism and stay away from energy-intensive industries. The military application of the law is reflected in Israel's security concept, which dictates a doctrine based on a rapid maneuvers and advocates not becoming entangled in a war of attrition. This law became an important concept in planning force structures, as evidenced by an article by Maj. Gen. (ret.) Isaac Ben-Israel describing the tension between the desire to utilize comparative advantage to the fullest and the need to provide a response to the enemy's force structure and doctrine.[4]

e. *Timing and location are everything*: The deliberations of a commander in a defensive battle are similar to those of an investment manager during a stock market crisis. An investment manager must decide when to enter the stock market and how to identify stocks whose price has dropped below what is reasonable. The deliberations of a commander concerning the timing and location of a counter-attack are very similar to those of the investment manager. In addition, a commander deliberates whether to beef up the attack force with reserves from other sectors and thus expose them to the attack. The same applies to the investment manager, who debates whether to use only the cash in his possession, or perhaps to take a loan in order to buy stocks that appear at that time to be very inexpensive. Leveraging can lead to large profits if decisions about the timing of entry into the stock market and the choice of stocks turn out to be correct. Otherwise, leveraging could lead to enormous losses.

The Difference between the Disciplines: "It Is Good to Die for Our Country"

Many commanders claim that the readiness to die for one's country and comrades-in-arms distinguishes military thinking from the rationales of other disciplines. In contrast, economic thinking assumes that human actions are guided by the desire for economic achievements (along with obedience to the law and normative behavior based on generally accepted social values), and in the world of economics there is no situation in which people sacrifice their lives for the good of the organization to which they

belong. According to this argument, the situation in the military is special: a considerable part of the training of soldiers is geared toward inculcating in them adherence to the combat mission, to the point of potentially sacrificing their lives.

Yet the very substantial difference between military culture and economic culture notwithstanding, this difference is significant mainly on a tactical level. Acts of heroism and sacrifice by individuals may change the results in a battle, but only infrequently can they change a military campaign, and they have even less influence on the outcome of a war. The Japanese army during the Second World War provided a powerful example of determination and willingness to sacrifice, but this sense of sacrifice did not lead Japan to victory and in fact only increased American casualties, and ultimately led President Truman to drop nuclear bombs on Japan. Willingness to sacrifice one's life is a very complex issue, and is a subject beyond the scope of this article.

What Are Economists Supposed to Do (Other than Cut Expenditures)?

The most common image of an economist is an expert at cost cutting who does not consider the damage to operational effectiveness caused by cuts. A senior infantry commander, in contrast, would claim that eliminating brigade-based training for soldiers and giving preference to corps-based training (such as that of the Armored Corps) will save money but cause serious harm to brigade cohesiveness and the fighting spirit of the infantry soldiers. Another example is provided by Professor Luttwak: he claims economists prefer that refueling tankers for US Navy task forces be as large as possible because one large ship is less expensive than two small refueling ships. According to Luttwak, this narrow approach ignores the risk of relying on one large ship: if it is damaged, the task force must return to base.[5]

The two examples offered above falsely accuse economists of not understanding that the yearning for efficiency and cost savings may harm operational effectiveness. Essentially, economists engage in optimization based on cost-benefit calculations, and economic analysis is intended to identify the full costs of the options examined and the full scope of benefits, and then compare them and select the optimal alternative. However, this is not sufficient: economic analysis must also consider the benefits and costs

that are not measurable, as well as the risks. There is an understandable tendency to criticize economists for how they address non-measurable variables. At the same time, there is insufficient appreciation of their contribution to defining and measuring the benefits, the costs, and the alternatives in the measurable areas. Defining and measuring these costs and benefits is often a very challenging task, subject to a variety of logical and empirical pitfalls, as will be described below.

Difficulties in Predicting the Future

Decisions about the future require an assessment of future costs and benefits, sometimes for periods of many years. It is difficult to predict the future. Thus, for example, the history of development and purchase of hi-tech aircraft, missiles, and ships in the United States is an ongoing story of enormous cost and schedule overruns. Israel is loth to disclose information on the development costs of weapon systems, and only the story of the Lavi fighter jet has become public knowledge. On this issue, the State Comptroller's report paints a picture that was similar to the situation in the United States.

Economic "True" Cost vs. Budgetary Cost

Until 1995, manpower costs in the IDF were calculated incorrectly: the cost of conscripts was calculated on the basis of their salaries and subsistence (food, clothing, and the like). This method of calculation underestimated manpower costs, as the budgetary cost was much lower than the economic cost, which is defined as the loss of civilian GNP, as a result of military conscription. There was a similar but less serious problem in calculating the cost of reserve duty. This cost was computed on the basis of payments received by reservists from the National Insurance Institute, which in many cases were lower than the amounts they earned and reflected the value of their GNP contribution ("economic cost").[6]

Likewise, for many years, until the 1990s, economists focused on the economic cost of foreign currency, as opposed to the official exchange rate. Thus, for example, every time the profitability of local production of weapons was examined, it was necessary to emphasize that the effective rate of exchange was significantly higher than the official exchange rate (this increased profitability of domestic production).

After the Second Lebanon War, a debate took place on the future of Iron Dome, the anti-short range rockets defense system. Opponents, most of them air force commanders, argued that it did not make sense to strike a rocket that costs about one hundred dollars with an interceptor missile that costs fifty thousand dollars (in addition to the high cost of the batteries themselves). Economists saw the issue from another angle. In their opinion, the relevant question was not how much it costs to manufacture a rocket, but what damages to property and human life and what loss of GNP result from rockets striking a built-up area. Data from the Second Lebanon War indicates that the use of Iron Dome can save several times the cost of the batteries and interceptor missiles in relation to the expenses and damages that would accrue without its deployment.

A Cost that Includes Expenditures on Operation and Maintenance

A comparison of the costs of weapon systems must take into account not only the cost of the equipment (aircraft, tanks, missiles, and the like), but also its life cycle costs (which includes development, maintenance, and wear), and spread them across the entire period of its service. As time passes, maintenance costs for the equipment rise. Therefore, it is very important to correctly calculate the cost of manpower and spare parts. (If maintenance costs are high, this means that the equipment has a low level of readiness, which makes it necessary to acquire more and thus presents as another expense.)

The Operational Benefit

Since the 1970s, there has been extensive literature in the United States on operational benefit which, among other things, includes criticism of the relentlessly rising costs of fighter jets and other advanced weaponry. The Military Reform Movement established at that time (for which Professor Luttwak is one of the most articulate spokesmen) advocated comprehensive reform in doctrine, force structure, and procurement methods. Its slogan was "more bang for the buck," a demand to maximize the operational effectiveness of every dollar in the defense budget.[7]

Cost-benefit calculations of this kind, of themselves difficult, require the help of economists and performance researchers, even though in many fields it is very difficult to quantify the operational benefit. For example, it is difficult to quantify the benefit of a small and expensive brigade

training depot, as opposed to a bigger and cheaper corps training depot. But as noted previously, economists must take the operational benefit into account, even though it is difficult to quantify.

External Economies

Economic theory conceptualizes the need to address all the results of choosing a particular alternative, taking into account their effects on third parties. This conceptualization is called external economies and external costs.

The starkest examples of external disadvantages come from environmental science. For example, the full economic cost of using internal combustion engines is not only the cost of the fuel, but also the damages from air pollution, traffic jams, accidents, and the like. Another example is the economic cost of smoking, which is not only the cost of manufacturing cigarettes, but also the damage to the health of smokers (active and passive), which leads to lost work days and an increased health budget.

A good example of external advantages in the economic-military realm can be seen in the development of unmanned aerial vehicles (UAVs), which provided the IDF with an original, innovative weapon system that has promoted many operational capabilities since the late 1970s. In addition, UAVs have become a major export. Another example is the great success in exporting precision weapons and various types of missiles, command and control systems, electronic warfare systems, advanced shells, aircraft upgrades, and armored combat vehicles. All of these are byproducts of Israeli investment in Israeli hi-tech.

These and many other examples indicate that estimates of the "defense burden" are exaggerated. The costs of military research and development appear as part of the defense budget, whereas the many economic benefits in employment and export are not reflected in the data used in discussions of this budget. In addition, the many expenses for training commanders, soldiers, and a large number of professionals improve Israeli manpower. This is also an investment that yields great returns, and it is not reflected in calculations of the burden.[8]

Smart bombs are, of course, much more expensive than "stupid" bombs, but they make it possible to save on platforms and munitions. Smart bombs have another important advantage: they greatly reduce the harm

to uninvolved civilians (third parties or innocent bystanders). Israel has faced this problem since it began to confront terrorist organizations, but it was seared into consciousness as a result of the IDF's lethal artillery fire in Kafr Qana and the Goldstone Report, which investigated IDF conduct in Operation Cast Lead. The ability to hit a pinpoint target without hurting uninvolved civilians has in recent years become a force multiplier, because it allows the IDF to employ weapon systems without becoming entangled in delegitimization, which in turn makes it difficult to use the army's full capabilities.

Quantification of Risk

How can the risk associated with two alternatives be represented? How can the probability of negative scenarios, and the possible harm they might inflict, be quantified? These are the most difficult issues that an economist must examine. As the discussion above indicates, the economist must address the risk even when it cannot be quantified.

Business uses rules of thumb that are simple but not necessarily precise in order to express risks. For example, the interest that banks charge for loans is a function of a number of economic variables associated with the purpose for which the loans are taken and the risk involved in granting the loan: the product the borrower is producing, the borrower's industry, economic history, experience in the field, and the like. Another example is the common use of extreme scenarios (stress tests) for assessing the capital adequacy of financial institutions (reminiscent of the "all of them," scenario, an important planning scenario used in the years prior to the Six Day War, which imagined a coordinated attack on Israel by all the Arab armies). Over the last generation, financial-mathematical risk management tools have been developed, but this is still a narrow field within economics and therefore concrete achievements to date in conceptualizing and quantifying business risks are still modest.

Accordingly, an economist, like a commander, must think in terms of risk. The benefits and costs calculated must also express the risks associated with the various alternatives. It is very difficult to quantify the risks, but they must be addressed and not swept under the rug.

Economic thinking, therefore, focuses not only on the cutting of expenses; it is meant to take into account the impact of savings on operational effectiveness and express it in calculations of cost and benefit.

Do economists always work this way? Not necessarily. They are liable to err because they use bad data and because of many other errors characteristic of human endeavor. Simply put, not all economists are geniuses, but neither are all commanders. Both economists and commanders must exercise judgment and use experience and intuition when they cannot obtain data or when the data is partial and includes a great deal of "noise."

What Economists Have Achieved in Practice: The United States and Israel

It is common to see the tenure of Defense Secretary Robert McNamara (1961-68) as the golden age of defense economists. McNamara and his whiz kids brought a fresh spirit to military-economic thinking, aiming to avoid redundancy and waste, introduce rationalization into development and procurement processes, and extract more defense from every dollar. One of the most famous examples of the work of McNamara and his whiz kids is the cancellation of the B-70 supersonic bomber project. This was a very expensive bomber that the Strategic Air Command wanted, even though the need for it was significantly reduced after the transition to intercontinental ballistic missiles. McNamara's economists also forced the Tactical Air Command to buy US Navy A-7 and Phantom jets fighter jets. The Phantoms were originally developed for the Navy in the 1950s and were found to be excellent planes (the Israeli Air Force continued to use them until 2005). Those same economists also contributed to the development of the F-111 light bomber, which was controversial but has stood the test of time.[9]

The basis of these and other examples was McNamara's approach to defense economics:

> It cannot be assumed that a new weapon would really add to our national security, no matter how attractive the weapon can be made to seem, looked at by itself. . . .You have to consider a very wide range of issues – the missions our forces must be prepared to perform, the effects of a proposed system on the stability of the military situation in the world, the alternatives open to us for performing the missions required.
>
> You cannot make decisions simply by asking yourself whether something might be nice to have. You have to make a judgment on how much is enough.

> I emphasize judgment because you can't even be sure yourself, much less prove to others, that your decision was precisely right to the last dollar – even to the last billion dollars. But the decision has to be made.

McNamara pointed out the considerable difference between the way in which decisions were made on these issues in his day and the way in which they had been made previously:

> Formerly, an arbitrary budget ceiling was fixed for national defense, and funds were then apportioned among the Services. Today we examine all our military needs, and then decide at what point our military strength is in balance with the requirements of our foreign policy.
>
> There are, of course, sharp differences of opinion on where we should spend our marginal defense dollars. And here is where the responsibility most clearly falls on the Secretary of Defense, because here is where it must fall not only constitutionally but under any rational system. For these decisions can only be made from the point of view of the defense establishment as a whole, not from the point of view of the individual Services. Indeed the very biggest decisions – such as the basic kinds of forces we need, and the occasions on which we might want to commit these forces – must be made at an even higher level: for they involve basic questions of national policy which transcend the interest of the Defense Department, or the State Department, or indeed any part of the government, and must be made at the Presidential level.[10]

McNamara's resignation and the weakening of the Defense Department in the wake of the failures of the Vietnam War, as well as the military and industrial establishment's opposition to centralized management of the department, led to a decline in the influence of economists in defense decision making in the United States. However, the tools introduced by McNamara for defense budget preparation are used to this day: a multi-year planning system, the Planning, Programming, and Budgeting System (PPBS), and systems analysis.

To be sure, the quantitative approach introduced by McNamara and his whiz kids had negative aspects as well. In many cases, the Department of Defense applied statistical indices that had no operational meaning, which

resulted in wasted resources and growing alienation between Washington and US forces in Vietnam.

And what about Israel? As far back as 1963, the Ministry of Defense established an economic consulting unit, headed by Dr. Eitan Berglas, which worked separately from the unit of the chief of staff's financial advisor. Berglas resigned in 1966, and was only replaced in 1969 by Professor Pinhas (Siko) Sussman. The economic advisor attempted to operate in a way that was similar to McNamara's whiz kids in Washington, but he had much less influence. One of the important projects undertaken during Sussman's time pointed to the feasibility of developing and manufacturing the Merkava tank, as opposed to purchasing the American M-60. Sussman's report on this issue was prepared in 1970 after Great Britain reneged on its agreement to supply Israel with modern Chieftain tanks, when the IDF was trying to decide which tank would replace its Centurions and Pattons.[11] Unlike Sussman, Zvi Tropp, the Defense Ministry's economic advisor in the mid-1980s, did not play a significant part in the stormy debates around the decisions on developing the Lavi jet fighter or, later, on terminating the project.

Economists in Israel dreamed of having a defense minister like Robert McNamara, who was assisted by economists and systems analysts in setting policy. This did not happen. In fact, to this day, it is the financial advisor to the chief of staff, the Planning Branch in the General Staff, and the Administration for Research and Development of Weapons and Technological Infrastructure in the Ministry of Defense that play the key roles in economic analysis of defense systems, not professional economists in the Prime Minister's Office, the Defense Ministry, or the Knesset.

Conclusion

This article has attempted to bridge between military thinking and economic thinking and show that the two disciplines are similar in their conceptual basis and that commanders and economists work in a similar manner. How is it possible, then, to explain the annual stormy deliberations on the defense budget? The main explanation is that commanders wish to achieve a large and sophisticated order of battle and that they aspire to provide Israel with the maximum possible defense output at minimum risk. On the other side are the economists, who represent the need to save on expenses – to reduce redundancy, eliminate superfluous activities,

and simply become more efficient. Every organization has this need, and certainly a large defense establishment such as Israel's. In addition, it is necessary to meet other state needs – those that contribute directly to national strength as well as those that are important to quality of life.

The two sides in the debate generally have a positive starting point. However, it is difficult for them to reach understandings and agreements because of an inability to predict and quantitatively assess the full costs and benefits (including the risks) of the various alternatives of national defense policy and the budgets derived from them. There is no dispute that Israel is exposed to threats in a number of fronts and that defense needs are both substantial and expensive. The budgetary disputes that arise every year are mainly a result of the absence of clear guidelines concerning national defense objectives, the ranking of threats, and the levels of risk on the one hand, and the needs of civil society on the other.

The description above does not tell us much that is new. During the last decades, a great deal of ink has been spilled on attempts to upgrade the process of the defense budgeting, and there is still a long way to go. The last of these attempts was the May 2007 report of the Brodet Committee, most of which is devoted to proposals for reform of procedural and administrative aspects of the budget. Essentially, the committee recommended that mediation between the budgetary demands of the military and the economic affordability "must be carried out at the political-military cabinet level after setting clear and distinct priorities for the tasks, in accordance with the possible size of the trained order of battle subject to budgetary constraints, including full responsibility for the risks of failing to provide a response, or providing only a partial response only, to the threat being analyzed and the scenario that was adopted."[12]

In order for the political-military leadership to be able to work as the committee suggests, it needs professional bodies – that are not part of the IDF or the defense establishment – to carry out staff work. The Brodet Committee also recommended that the National Security Council be the main body to coordinate the staff work on the defense budget. It repeated similar recommendations made previously by the state comptroller and the Meridor Committee from 2006.[13]

It is reasonable to assume that implementation of the Brodet Committee's recommendations would significantly reduce the decibel

level of the disputes between commanders and economists. Unfortunately, the committee's recommendations relating to the key processes for setting the defense budget were not implemented.

In conclusion, there are thus no conceptual differences between military thinking and economic thinking, but there can be professional differences of opinion in confronting specific issues because of the difficulty in quantifying costs and benefits, particularly the aspect of risk management. The raucous, nerve-wracking debate during annual deliberations on the defense budget does not result from a fundamental gap between the two disciplines. It may be attributed, first and foremost, to the political-defense leadership's management of the process, which is not orderly, and to the lack of independent military staff that does not come from the defense establishment to help the government and the Knesset. It is unfortunate that the Brodet Committee's report, which was the latest attempt at a revolution on this important issue, did not succeed in changing the situation.

Notes

The author wishes to thank Dr. Gabi Siboni, Dr. Oded Eran, and Imri Tov for their constructive comments and suggestions, which contributed greatly to the article.

1 Edward Luttwak, *Strategy: The Logic of War and Peace* (Ma'arachot Publishing, 2012), pp. 18, 62-65.

2 Aviezer Ya'ari, *Civilian Oversight of the Military in Israel* (Tel Aviv: Jaffee Center for Strategic Studies, Tel Aviv University, October 2004), pp. 46-50; Imri Tov, "The Economic Aspect of Relations between Economic and Military Officials," in *Relations between the Civilian and Military Leadership in Israel: Reciprocal Relations and Control Mechanisms*, ed. Ram Erez (Tel Aviv: Jaffee Center for Strategic Studies, Tel Aviv University, November 2003), pp. 56-60; *Report of the Committee to Examine the Defense Budget* (Brodet Committee), Jerusalem, May 2007; State Comptroller, *Annual Report 56A*, Jerusalem, 2005, p. 5.

3 Saul Bronfeld, "Reform in the Wake of Military Failures," *Ma'arachot* No. 412, May 2007.

4 Isaac Ben-Israel, "The Theory of Relativity of Force Building," *Ma'arachot* No. 352-353, August 1997, No. 354, November 1997.

5 In many of Luttwak's works, he accuses economists of failing to understand that standardization (in equipment, in manpower, and in other aspects of military activity), which contributes a great deal to efficiency, also undermines effectiveness. Edward N. Luttwak, *The Pentagon and the Art of War* (New York: Touchstone, 1985), ch. 5.

6 Saul Bronfeld, "Reserve Duty: The Difference between Economists and Army Personnel," *Ma'arachot* No. 390, July 2003. A detailed and precise presentation of ways of calculating the economic cost of military manpower can be found in Ya'acov Lifshitz, *Defense Economics* (Ministry of Defense Publishing, 2000), chs. 7, 8.

7 Dina Rasor, ed., *More Bucks, Less Bang: How the Pentagon Buys Ineffective Weapons* (Washington, DC: The Fund for Constitutional Government, 1983).

8 Eitan Berglas, "The Defense Burden and the Israeli Economy," in *The Israeli Economy: Growth Pains*, ed. Yoram Ben Porat (Tel Aviv: Am Oved, 1989), pp. 213-15.

9 Alain C. Enthoven and K. Wayne Smith, *How Much Is Enough: Shaping the Defense Program, 1961-1969* (Ma'arachot Publishing, 1974), pp. 177-94. See also a detailed description of the incident in which the Department of Defense imposed its opinion on the Tactical Air Command: Richard G. Head, "Doctrinal Innovation and the A-7 Attack Aircraft Decision," in *American Defense Policy*, eds. Richard G. Head and Erwin J. Rokke (Baltimore: Johns Hopkins University Press, 1973).

10 Enthoven and Smith, *How Much Is Enough*, pp. 151-52.

11 See the description of the establishment of the economic advisor's bureau in Yossi Argaman, *Pale Was the Night: Siko's Version* (Tel Aviv: Yediot Ahronot, Sifrei Hemed, 2002), pp. 97, 318-44.

12 *Report of the Committee to Examine the Defense Budget*, p. 18.

13 Ibid., pp. 77-79.

Iron Dome's Impact on the Military and Political Arena: Moral Justifications for Israel to Launch a Military Operation against Terrorist and Guerrilla Organizations

Liram Stenzler-Koblentz

The military and political arenas are closely linked in Israel's fight against terrorist and guerrilla organizations. Israel is a democratic country subject to legal and moral constraints and restraints, and therefore, when it initiates a military operation against such organizations, its justifications are important, as they will later affect its international legitimacy or lack thereof. This article discusses the Iron Dome system, which is designed to provide active protection for Israeli citizens. It attempts to answer the question whether there can be moral justification for Israel to launch a comprehensive military operation against a terrorist organization when it possesses such a system. The discussion of the question makes reference to a system of moral principles (*jus ad bellum*), which is part of just war theory and can help in making judgments about when there is moral justification for going to war.

Keywords: just war theory, morality, low intensity warfare, Iron Dome, legitimacy, diplomacy, just war, *jus ad bellum*

Introduction

Since the end of the Yom Kippur War, Israel has been forced to confront a change in the nature of war: a transition from conventional war between

Liram Stenzler Koblentz, a former Fox International Fellow and visiting assistant in research at Yale University, is a doctoral student in the Department of Political Science at Tel Aviv University.

regular state armies to low intensity conflict, that is, combat mainly against non-state actors (terrorist and guerrilla organizations).[1] A key characteristic of this type of conflict is the blurred distinction between the home front and the battlefront,[2] as terrorist organizations launch missiles and rockets at the Israeli home front from the heart of the civilian population, turning it into a battlefront.

Some of the non-state actors are semi-military. For example, in 2007, after Hamas took control of the Gaza Strip, it established an orderly military framework with brigades, battalions, companies, and platoons, as well as dedicated units such as a coast guard. The military framework also includes advanced weaponry, such as rockets of various ranges.[3] As a semi-military organization, Hamas is able to pose a constant threat to disrupt the lives of Israeli citizens.

Another characteristic of low intensity conflict is the impossibility of aiming for total surrender by the enemy. Physical concepts such as conquering territory and destroying divisions, which form part of conventional wars, are replaced by more fluid concepts, such as a reduction in the intensity of terrorism and achievement of a reasonable level of personal security. The objectives of combat today have a stronger psychological element than in the past, as they are intended to harm the moral and social robustness of the other side.[4]

The aim of harming the adversary's moral and social strength is reflected in comments by Yuval Bazak, formerly head of the combat doctrine division in the IDF General Staff. According to Bazak, the IDF and Hizbollah had contradictory strategies in the Second Lebanon War: while the IDF was working to demonstrate air superiority over Hizbollah in Lebanon, Hizbollah launched its rocket arsenal from within population centers and fired at the Israeli civilian front without directly confronting Israeli power. Its objective was to restrict the IDF's ability to operate by provoking the Israeli public to pressure the government to cease fighting in order to prevent further Israeli casualties and condemnation from the international community.[5]

We can apply this claim by Bazak to the conflict between Israel and Hamas as well. Hamas launches its rockets against the Israeli home front from within a civilian environment because it assumes that the IDF would find it difficult to respond with the necessary efficiency for fear of harming innocent civilians and given the constraints stemming from

Israel's democratic and moral nature.[6] If Israel does choose to take action, it is likely to deepen the sense of delegitimization within the international community, which sees it as fighting an unjust war.[7]

One of the main problems Israel faces in this context stems from the fact that it must act to protect the security of the country and its citizens by thwarting and reducing the level of terrorism, while simultaneously striving for legitimacy and backing for its operations in the international arena (which includes international organizations such as the United Nations, the European Union, and various countries). The Goldstone Report, published following Operation Cast Lead in the Gaza Strip in 2009, triggered a wave of international condemnations of Israel and made decision makers realize that legitimacy for a military operation is an integral part of the operation itself.[8] The importance of legitimacy for Israel was also addressed in a report by the Reut Institute in 2010. The report's authors argued that the Second Lebanon War and Operation Cast Lead starkly revealed the emergence of a strategic threat to Israel in the form of political and diplomatic delegitimization (such as the academic boycott in Great Britain and the Belgian boycott of a bank that has ties with Israel),[9] which could become an existential threat within a few years. This makes the military arena secondary. In the opinion of the authors, a new defense concept should be developed, one of integrated victories along several fronts (military, media, the home front, and the political-diplomatic front), all of which are interrelated in a variety of ways.[10] Certainly the military and political arenas are closely connected: because Israel is a democratic country and therefore subject to legal and moral constraints and restraints, it is important that any military operation be justified, a matter that will later affect its legitimacy or lack thereof.

This article will discuss Iron Dome, Israel's anti-rocket and anti-missile defense system, and the moral justifications[11] it provides for launching a comprehensive military operation[12] against Hamas and Hizbollah in the future.[13] The article attempts to answer the question whether it is morally justified for Israel to undertake such an operation against an aggressive terrorist organization when Israel has Iron Dome.[14] The article also aims to underscore the importance for Israel of upholding moral principles before launching a military operation that will involve the use of force, in order to secure international legitimacy and backing for the move. The discussion will be normative and will make use of a system of principles

from the realm of morality (*jus ad bellum*), which is part of just war theory and which helps us judge when going to war is morally justified. The article will not discuss questions concerning the actual methods of combat, but rather questions related to the justification for engaging in war. The issue of international law will also be addressed, but will not be a main focus.

The Iron Dome system was at the heart of Operation Pillar of Defense in the Gaza Strip in 2012, whose aim was to protect Israel's citizens from the increasing number of rockets being fired from Gaza. The operation included aerial attacks on Hamas's long range missile stockpiles, strikes against its infrastructures, and assassination of its officials, the most conspicuous of whom was Ahmed Jabari, commander of the organization's military wing. Pillar of Defense also included, for the first time, active defense of Israeli citizens through the use of Iron Dome, which reportedly had an 84 percent success rate in intercepting rockets.[15]

Israel had made use of the Iron Dome system even before Pillar of Defense, but this operation established the technology and affirmed its role as an effective means of defense against a concentrated rocket attack. The system's technological capability is a mixed blessing: while it gives Israel the ability to defend its citizens more effectively and prevent terrorist organizations from achieving their objectives, it could lead to the international community adopting more restrictive standards regarding the launch of a military operation, thereby limiting Israel's freedom of action.

The Iron Dome System: Background

Iron Dome is an active defense system designed to intercept and destroy missiles and rockets while they are still in flight and have not yet reached their destination. It provides an operational response to the threat of high trajectory weapons intended to harm Israeli population centers. This system, which strives to reduce injury and damage to the Israeli home front, complements passive defense (such as having civilians stay in protected spaces) as well as offensive military operations by the IDF on the battle front. Iron Dome was developed by Rafael (the main contractor), mPrest, and Elta[16] to protect Israeli civilians and strategic facilities from rockets with short ranges – four to seven kilometers – in all weather conditions and while confronting a large number of threats simultaneously. Because it uses radar, Iron Dome can identify the missile launch site, the missile's

ballistic trajectory, and the anticipated point of impact. On the basis of this data, it determines whether interception is necessary: if it is clear that the anticipated point of impact is a populated area or is near strategic facilities (previously designated for protection), the rocket will be intercepted by a Tamir missile.[17]

The first operational use of Iron Dome took place in April 2011, when the system intercepted rockets fired at Gaza's perimeter communities and at southern cities such as Beersheba and Ashkelon. By April 2012, Iron Dome had achieved ninety-three interceptions in various operations.[18] However, Pillar of Defense was the first extensive operation in which the IDF used the system. Four overlapping Iron Dome batteries were deployed over most of the urban areas in the southern coastal plain and the northern Negev in order to provide a response to the rockets that would be fired by the terrorist organizations from the Gaza Strip. Three days after the start of the operation, a fifth battery was deployed in Gush Dan to provide a response to the rockets that would be launched at Tel Aviv and the surrounding area.

Operation Pillar of Defense proved Iron Dome's importance as a response to the rockets fired by terrorist organizations: it has a success rate of 84 percent. Of the 1,532 rockets fired at Israel, only 500 were targeted by Iron Dome – namely, those rockets that would have struck populated areas or strategic facilities.[19]

Just War Theory and Israel's Moral Justifications for Launching a Military Operation

Just war theory is a moral framework that includes concepts, criteria, and rules. It is an agreed system of principles that serve as a basis for discussions on questions about the morality of war. The theory is divided into two main parts: the justification for going to war (*jus ad bellum*), which comprises the reasons that political leaders decide to go to war, and the justice of the conduct of the war (*jus in bello*), which refers to the methods states use during combat. A third part, called *jus post bellum* (post-war), was developed later. It includes one state's rights and obligations toward the other state after the war and during the pursuit of peace.[20]

A democratic country such as Israel, which strives to maintain morality in warfare, must act in a manner that conforms to the system of principles embodied in this theory. When examining Israel's options for responding to armed attacks by Hamas or Hizbollah against its citizens in the future,

we would do well to focus on *jus ad bellum*, which deals with the moral justification for going to war. This includes a system of principles with six parts:

a. Just cause: The state must prove that it has a justified reason for going to war.
b. Legitimate authority: The legal authority to declare war is in the hands of a person or body authorized by the state.
c. Reasonable hope of success: A state may use force and go to war only on condition that there is a reasonable chance of succeeding.
d. Last resort: A state may go to war only as a last resort and on condition that other alternatives have been tried.
e. Right intention: A state may go to war only on condition that its intentions are "pure" (for example, not for revenge) and when its intention is to promote the good and prevent the bad.
f. Proportionality: A state must prove that the benefit of the war to one side will justify the damage it will cause to the other side.[21]

A state must meet all six of these criteria in order to have moral justification for going to war.

The rocket and missile barrages against the Israeli home front by terrorist organizations in the Gaza Strip and in Lebanon constitute an attack on innocent civilians, and the government therefore has a responsibility to identify immediate measures it can take to protect their security. As such it must examine the moral principles, which are harder now for Israel's government to justify in advance of a military operation because today Israel has a system capable of providing significant protection to its citizens. In this context, application of the underlying principles is unlikely to yield a different answer, as these principles do not embody the concept of immediate defensive capability.

The Principle of Legitimate Authority

Because Israel is a democratic state, any decision to launch an operation will generally be taken by ministers of the political-security cabinet, the forum that is authorized to make decisions even without convening the government plenum. Such an operation will generally be announced by the Prime Minister, the Defense Minister, or both.[22]

The Principle of Reasonable Hope of Success

Before the Second Lebanon War was launched, excessively ambitious goals were set for this campaign, despite the absence of an orderly discussion on the subject. Presumably, the fact that lessons were indeed learned from the failures of that war means that in the future, before it launches a military operation, the political leadership will consult extensively with defense officials in setting the goals of the operation. In general, these will be limited goals that decision makers believe the IDF can achieve, and their purpose will be to remove the immediate threat to Israeli citizens and to increase Israel's deterrent capability by striking at the terrorist organizations' infrastructures and weapons stockpiles.[23]

The Principle of Right Intention

When Israel, as a moral, democratic state, initiates a military operation, its goal must be to thwart offensive operations against it, now and in the future. An assessment of Operation Pillar of Defense indicates that its goals were to strengthen the IDF's deterrence; to strike hard at the Hamas rocket arsenal; to deliver a harsh blow against Hamas and other terrorist organizations; and to minimize harm to the Israeli home front.[24] In other words, the operation was geared toward current and future defense of the citizens of Israel.

In contrast to these three principles, which are unlikely to change, there are three other principles that the international community might examine more stringently than in the past given that Israel will make use of Iron Dome to provide better protection for its citizens.

The Principle of Just Cause

A state has a moral obligation to protect its territorial integrity and political sovereignty as well as the life and freedom of its individual residents.[25] The scenario of a rocket attack, which could place Israel's citizens in extreme danger, would require the government to do everything in its power to protect its citizens. International law, a tool whose purpose is to minimize violence in the international arena, also addresses the importance and centrality of the act of self-defense, relying on the tradition of just war.[26] The UN Charter, in article 2(4), prohibits the use of force or the threat of use of force by one state against another state, or against its territorial integrity or political independence. However, it recognizes exceptions, the

foremost being article 51,[27] which allows a state to use force for self-defense in response to an armed attack against it.

When Israel undertakes a military operation against terrorist organizations that have attacked it, as it did in Operation Pillar of Defense, it is justified by the right of self-defense, as affirmed by the Israeli Foreign Ministry when it asserted the obligation to defend its citizens and eliminate the strategic threat they face.[28] This right to self-defense resurfaced after the start of the campaign in comments by Israel's ambassador to the United Nations, Ron Prosor, who noted that in previous months, he had warned countless times about the possibility of escalation in the south if Israeli citizens continued to be the victims of terrorist attacks by Hamas. According to Prosor, the UN Security Council had chosen to remain silent and do nothing. The ambassador added that Israel has the right and the obligation to defend its citizens and that it would not play Russian roulette with their lives.[29] A significant and important portion of the international community, including the United States and the European Union, supported this right. US President Barack Obama stated that Israel has the right to defend itself from the ongoing rocket fire, and the EU declared that there is no justification for deliberately firing on innocent civilians and that Israel has the right to protect its population from such attacks.[30]

Self-defense is also subject to restrictions. On this matter, a distinction must be drawn between a moral action taken in the name of self-defense and an immoral action. The morality of an action is assessed through questions such as whether the state's response to an attack was indeed necessary and whether it was proportionate.[31] These questions lead to the following two principles: the principle of last resort and the principle of proportionality.

The Principle of Last Resort

Before deciding to launch a military operation, the government of Israel has a moral obligation to consider whether it has done all it can to protect Israelis fully in a way that will actualize its right to self-defense on the one hand, yet prevent the use of military force on the other. If it answers in the affirmative, it will be easier for Israel to morally justify launching a military operation.

What alternatives are available to the government of Israel for preventing missile strikes? The first option is to use Iron Dome to intercept missiles

directed at Israel and, at the same time, to take non-military measures against the attacker, that is, political sanctions and political-diplomatic measures. Political sanctions include restricting fishing zones or closing border crossings through which goods are imported to a given area (an example of this is the sanctions imposed on the Palestinians after rockets were fired at Israel in March 2013).[32] As for political-diplomatic measures, the most obvious one is to appeal to the UN Security Council and ask it to condemn the operations of the terrorist organizations and call for an immediate cessation of rocket fire against Israel (an example of this is the appeal by Israel's UN ambassador for a condemnation of rocket fire against Israel in April 2013).[33]

This path of political-diplomatic measures, along with defensive measures and the refraining from offensive measures, seems unrealistic for several main reasons:

a. An active defense system like Iron Dome cannot provide "hermetic" protection for residents of Israel because of a lack of technical capability in two areas: First, the system cannot intercept missiles within a range of four kilometers, which means that most of the Gaza perimeter communities (in the case of missiles fired by Hamas) and many communities along the northern border (in the case of missiles fired by Hizbollah) cannot be protected by Iron Dome. Second, the system has a not insignificant rate of failures in intercepting missiles aimed at Israel (an example is its lack of success in intercepting Grad rockets fired at a residential area in Eilat in April 2013).[34] In addition, in spite of Iron Dome's existence, Israelis still have to stay in protected spaces during an attack, and sometimes they are still wounded in such a situation. (An example is the moderate injuries sustained by a resident of the Sha'ar Hanegev Regional Council area, who was in a protected space during the successful interception of a rocket fired from the Gaza Strip).[35] The system also cannot completely prevent side effects from the firing of missiles. Examples include harm to the mental health of civilians and physical damage to civilians injured by fragments from the interceptor missiles. Other possible adverse effects include millions of shekels in economic damage to Israel[36] because of the closure of schools, the loss of days worked by parents, the closure of places of entertainment, the mobilization of reserve soldiers, and damage to private homes, businesses, infrastructures, greenhouses, and crops in open spaces.

Iron Dome also cannot be used over an extended period of time because of the cost of the interceptor missiles, estimated at some $40,000-$50,000 per missile.[37] In addition, there is concern that the terrorist organization will learn and internalize the system's weaknesses, and if the system does not perform well, it will undermine Israel's deterrent capability.[38]

b. It is not possible to thwart the rocket threat through defensive action only. Offensive actions and operational prevention complete the response to rocket fire directed at Israel's citizens.[39]
c. Israel's ability to deter terrorist organizations could be eroded. If there is no military response, these organizations are liable to feel that they can continue to fire missiles at Israel in order to disrupt the daily life of Israeli citizens.
d. The government could lose legitimacy among Israel's citizens if they feel unprotected and frustrated by its impotence against an aggressive terrorist organization. The loss of legitimacy could bring down the government, and thus, presumably it would do everything in its power to avoid that.
e. Diplomatic measures such as turning to the UN Security Council will usually not produce operational results that will assist in stopping the fire, as evidenced by the number of resolutions condemning Israel because of the Palestinian issue over the years, compared to the negligible number of resolutions condemning the Palestinians.[40] Another example is Ambassador Prosor's comments about the Security Council's impotence in the face of Hamas missile fire.[41]

The second alternative is for the government to use military force, that is, to launch a military operation against those who fire the rockets. Here too we can distinguish between two types of operation. The first is a targeted operation in response to offensive actions by terrorist organizations, such as an aerial attack on terrorist cells or on various targets, including terror infrastructures, smuggling tunnels, and weapons manufacturing sites.[42] The second is an extensive operation, that is, a comprehensive military operation. A targeted military action to thwart the missile fire might give rise to two main problems:

a. The rocket arsenals of Hamas and of Hizbollah may be very large, and therefore, a targeted strike by Israel would not cause any real damage to the two organizations' missile firing capabilities and would not lead

to a long term solution to the problem. According to IDF assessments, Hizbollah alone possesses more than 40,000 rockets.[43]

b. Hamas and Hizbollah are liable not to be deterred by an IDF operation. A targeted Israeli military action could create limited deterrence and fail to stop the rocket fire and the erosion of Israeli deterrence.

On the eve of Operation Pillar of Defense, Israel was careful to argue that in spite of the periods of escalation that preceded the action (in April, August, and October 2012), it had made every possible effort to respond to the missile fire with restraint.[44] Israel noted that it had used the Iron Dome system, which was intended to minimize damage to the property and lives of Israelis, as well as targeted operations in the Gaza Strip, such as an aerial attack in October 2012 on a terrorist cell that was in the final stages of preparing to fire rockets at Israel.[45] Only when it became clear to decision makers that the rocket fire was increasing and the danger to Israeli citizens was not diminishing did they realize that Israel must launch a military operation.

A future rocket attack on an Israel equipped with the Iron Dome system will further highlight the importance of the principle of "last resort." As a result of Israel's ability to protect its citizens and to minimize damage to them, the international community will expect Israel to be more cautious than in the past when exploring the option of launching a military operation. It will expect Israel to devote more time to examining alternatives other than Iron Dome in order to protect its citizens. However, given the weaknesses of the other options, as discussed above, it will then be possible to morally justify launching a military operation.

The Principle of Proportionality

In the future, before Israel makes a decision to launch a military operation against terrorist organizations, the international community will ask it to prove that the goal and results of the operation, which are legitimate in and of themselves – preserving the welfare, life, and property of Israeli civilians – morally justify the anticipated physical damage (injury or death) and the property damage to Palestinian or Lebanese civilians. Israel's use of Iron Dome highlights this principle. Even before the system was in use, the asymmetry between Israel and Hamas was evident, particularly in terms of the disparity in military capability and consequent harm to innocent Palestinian civilians. This asymmetry has now increased even further:

not only do most Israeli citizens[46] have the ability to protect themselves passively (by staying in a protected space), in contrast to the Palestinians, but Israel also has the ability to protect its citizens actively (though not "hermetically").

The fact that Hamas deliberately chooses to operate from civilian population centers in order to push Israel into a corner and cause it to attack innocent civilians does not detract from the moral argument that Israel must justify the harm it would cause to those Palestinian civilians. Israeli military action against a terrorist organization alongside the use of Iron Dome could lead to arguments that Israel is better able to defend its citizens and their property than in the past, whereas its military operation could cause death and suffering to Palestinians who are unable to protect themselves (and whom Hamas has no desire to protect). Thus, any future Israeli military action against the terrorist organizations in the Gaza Strip is liable to lead to Palestinian civilians being presented as the underdog, more so than in the past.

Armed conflict between Israel and the Palestinians will result in much damage and many casualties among the Palestinians and more limited damage and fewer casualties on the Israeli side, as is typical of asymmetric conflicts between a strong party and a weak party. This situation is liable to cause the international community to doubt Israel's moral considerations and thus to weaken the legitimacy of Israel's military operation. Such asymmetry is starkly apparent, for example, in the number of those killed and wounded during Operation Pillar of Defense. On the Israeli side, six civilians were killed and 269 wounded (a figure that also includes those suffering from shock).[47] Among the Palestinians, 167 were killed and 1,200 injured (87 of those killed were non-combatants, 69 were combatants, and the status of the others is not clear).[48]

In the final analysis, although Israel has a greater ability to protect its citizens, it lacks the ability to ensure their wellbeing without an offensive solution. Neither the passive protection options nor the Iron Dome active defense system can provide full and immediate security to Israeli citizens.[49] Therefore, Israel has moral justification for taking military action, even if doing so could endanger civilians on the other side.

Conclusion and a Look to the Future

According to Prime Minister Benjamin Netanyahu, delegitimization of Israel is one of the greatest moral failings of our time.[50] This delegitimization results from international denunciation of Israel's activities in several areas, not only the military realm. However, the central role security plays in Israel makes this the main issue.

Morality and legitimacy are fundamental parameters that are closely connected to the military domain. Terrorist organizations know this, and they seek to undermine Israel's moral strength. Israel, which is sensitive to the loss of life of its citizens, is sometimes forced during IDF operations to harm innocent civilians on the other side in order to protect its own citizens. Such harm will result in the international community's failing to grant legitimacy to IDF operations and in delegitimization of the State of Israel.

If Israel aspires to succeed not only militarily,[51] but also in explaining its policies and in the political-diplomatic realm – that is, in receiving legitimacy and backing for its operations from the international community – then it must constantly maintain a balance between its most important role, protecting the safety and security of its citizens, and preserving its moral character. This quality is reflected, inter alia, in an operation that is in accordance with the set of principles of just war theory in all aspects of the launch and conduct of a military operation. In the opinion of Professor Michael Walzer, not only are statesmen and soldiers aware of the moral aspect of war; most indeed wish to act and to be seen to act in a moral way.[52]

This article sought to examine the extent to which in the future Israel will adhere to the moral principles that justify launching a military operation. It assumes that because Israel has the Iron Dome system, the international community might deny the legitimacy of such an operation. Accordingly, when Israel did not have a real defensive tool that could protect large areas, the necessity of a military operation was clearer and left Israel with more moral leeway. Now that Israel can endure more massive rocket fire than in the past with much less harm to property and human beings, it will have to prove three main points to the international community before it undertakes military action:

a. That its reason for initiating the operation is justified.
b. That before it chose the military option, it carefully examined other courses of action that do not involve the use of force.

c. That the benefit of the operation to Israel's citizens justifies the harm that could be caused to the opposing side.

Examination of these issues indicates that even though Israel has Iron Dome, it is morally justified in launching a military operation against a terrorist organization that is firing rockets at it. There are two main reasons for this. First, a ceasefire cannot be achieved without using preventive and offensive measures. Second, Iron Dome is not a magic bullet. It does not enable "hermetic" protection of the Israeli home front and cannot prevent the side effects of missile fire.

At the same time, the State of Israel's moral justification for initiating a military operation does not justify conduct of warfare from the IDF's perspective. Presumably, because Israel made do with an aerial operation and avoided a ground operation in Operation Pillar of Defense,[53] the hostilities ended with the (relative) support of the international community intact: many leaders, first and foremost the President of the United States, supported Israel's right to self-defense. This support was also evident in a poll conducted by CNN, which showed that 57 percent of the respondents in the United States thought that the military operation in the Gaza Strip was justified, while 24 percent opposed it.[54]

The decision to avoid a ground operation can be credited mainly to Iron Dome, which helped protect the Israeli home front more effectively than in the past and thus helped reduce public pressure on the government. This in turn gave the government more time to make decisions.[55]

The discussion above indicates that Israel's main problem now is actually liable to relate to the type of operations undertaken during the fighting. These correspond with the second part of the principles of just war theory, the manner of fighting (*jus in bello*). Henceforth, Israel will need to be much more careful than in the past in terms of the amount of force it uses and the duration of a military operation, so as not to cause too much harm to the other side. Such harm could increase the imbalance between the two sides and thus lead the international community to deny the legitimacy of Israel's actions.

We can expect that in a future Israeli military operation against terrorist organizations, the approach used during Operation Pillar of Defense – an air attack followed by negotiations with the mediation of a third country in order to avoid a ground operation – will likely be used again. This would allow Israel to achieve the goals of the operation while maintaining

international legitimacy. Such a scenario could provide an opening for a future discussion regarding the moral justification of measures taken by Israel during combat when it has a defensive system available in the form of Iron Dome.

Notes

1 Giora Eiland, "The Changing Nature of War: Six New Challenges," *Strategic Assessment* 10, no. 1 (2007): 15-22.

2 Baruch Nevo and Yael Shur-Shmueli, *Morality, Ethics, and Law in Wartime* (Jerusalem: The Israel Democracy Institute, 2003), p. 14.

3 "Hamas Strengthening and Force Buildup," General Security Services, December 2008, http://www.shabak.gov.il/publications/study/pages/gaza-hamas-terror-report.aspx.

4 Nevo and Shur-Shmueli, "Morality, Ethics, and Law," p. 15.

5 Yuval Bazak, "Responding to the Need for International Legitimacy: Strengthening the IDF Strike Force," *Military and Strategic Affairs* 3, no. 2 (2011): 3-5.

6 See the comments by a Palestinian civilian following Operation Cast Lead in "Palestinian Civilians in the Gaza Strip to *Corriere della Sera*: Hamas Wanted the Israelis to Shoot at Our Homes," *Haaretz*, January 22, 2009, http://www.haaretz.co.il/news/politics/1.1242826.

7 See comments by the UN interpreter on the large number of draft resolutions condemning Israel at the UN, http://www.nrg.co.il/online/1/ART2/522/689.html.

8 "Review: Roundtable on 'Between Cast Lead and Pillar of Defense' – A First Look at the Implementation of International Law," *Law and Business*, Radzyner School of Law, Interdisciplinary Center, Herzliya, March 6, 2013, http://idclawreview.wordpress.com/2013/03/06/cast_lead_cloud_pillar_2013/.

9 According to the report, the delegitimization of Israel is a denial of the legitimacy of Israel's existence as a Jewish state and of the Jewish right to self-determination. In addition, the report states that the erosion in Israel's status in the world has strategic ramifications, one of which is reduced leeway for Israel in the use of military force.

10 *The Delegitimization Challenge: Creating a Political Firewall: A Conceptual Framework in the Political-Diplomatic Arena of National Security* (Tel Aviv: Reut Institute, January 30, 2010), pp. 14-15, 42, 45.

11 This question also depends on the state's level of obedience to international law, but this article highlights the moral question.

12 This article uses the term "comprehensive military operation" in order to draw a distinction between such an operation and a targeted military action.

13 This article discusses only the possibility of missile fire by Hamas and the other organizations in the Gaza Strip, as well as by Hizbollah in Lebanon,

because Iron Dome is intended to cope with a considerable number of these missiles.

14 This article does not pretend to argue that a defensive system is meant to replace offensive capabilities during combat, because the success of a given operation comes from combining the defensive component with the offensive. However, there is importance to the manner in which the international community examines Israel's moral justifications for initiating an operation.

15 Some experts claim that the system's rate of success was much lower than 84 percent. See Reuven Pedatzur, "How Many Rockets Did Iron Dome Really Intercept?" *Haaretz*, March 9, 2013, http://www.haaretz.co.il/opinions/1.1954176. This article is based on official data presented by the IDF. See "Summary of Operation Pillar of Defense: All Events, Hour by Hour," IDF, November 20, 2012, http://www.idf.il/1133-17568-he/Dover.aspx.

16 IDF Spokesman, "The Changing Face of Battle: The Challenge of High-Trajectory Weapons and the Active Defense System of the State of Israel," IDF Spokesman's Research, Strategies, and Initiatives Branch, January 2011, pp. 5, 27, 45.

17 Rafael, *Iron Dome: Defense System against Short-Range Artillery Rockets*, http://www.rafael.co.il/marketing/SIP_STORAGE/FILES/6/946.pdf.

18 Yiftah S. Shapir, "Lessons from the Iron Dome," *Military and Strategic Affairs* 5, no. 1 (2013): 82.

19 Interview by the author with Foreign Ministry official, January 16, 2013; Yossi Nissan, "Pillar of Defense − The Numbers: This Is the Extent of the Damage the IDF Caused Hamas," *Globes*, November 22, 2012, http://www.globes.co.il/news/article.aspx?did=1000800368.

20 Asa Kasher, "Operation Cast Lead and the Just War Theory," *Azure*, Spring 2009, http://www.tchelet.org.il/article.php?id=437; Michael Walzer, *Just and Unjust Wars* (Tel Aviv: Am Oved-Sifriyat Ofakim, 1984), p. 31; Cecile Fabre, "Cosmopolitanism, Just War Theory and Legitimate Authority," *International Affairs* 84, no. 5 (2008): 963.

21 Carl Ceulemans, "The Moral Equality of Combatants," *Parameters* 37 (Winter 2007-8): 99, http://www.carlisle.army.mil/USAWC/parameters/Articles/07winter/ceuleman.pdf.

22 Operation Pillar of Defense was announced by the Defense Minister and the Prime Minister. See Omer Dostri, "Operation Pillar of Defense − Learning from Mistakes of the Past," *News1*, March 28, 2013, http://www.news1.co.il/Archive/003-D-78451-00.html.

23 See the comments by then-Defense Minister Ehud Barak on the objectives of Operation Pillar of Defense in Nitzan Erlich, "Watch: Netanyahu in Message to Hamas: 'We'll Continue to Defend Our Citizens,'" *Kikar Hashabbat*, November 14, 2012, http://www.kikarhashabat.co.il/D7%A6%D7%A4%D7%95-%D7%A0%D7%AA%D7%A0%

D7%99%D7%94%D7%95-%D7%9E%D7%A6%D7%99%D7%92-%D7%90%D7%AA-%D7%9E%D7%98%D7%A8%D7%95%D7%AA-%D7%94%D7%9E%D7%91%D7%A6%D7%A2.html.

24 See comments by Ehud Barak at the press conference at which the assassination of Ahmed Jabari was announced, October 14, 2012, http://ehudbarakhaatzmaut.blogspot.com/2012/11/blog-post_5508.html.

25 Walzer, *Just and Unjust Wars*, p. 69.

26 Orna Ben Naftali and Yuval Shani, *International Law between War and Peace* (Ramot Publishing, Tel Aviv University, 2006), p. 23.

27 For these documents see the UN Charter, http://www.un.org/en/documents/charter/chapter1.shtml and http://www.un.org/en/documents/charter/chapter7.shtml.

28 "Operation Pillar of Defense," Foreign Ministry, November 14, 2012, http://www.mfa.gov.il/MFAHeb/Israel_Policy/Operation_Pillar_of_Defense_141112.htm.

29 Assaf Gabor, Ahikam Moshe David, Uri Binder, and Avi Ashkenazi, "Ahmed Jabari Assassinated: Operation Pillar of Defense Underway," *Maariv NRG*, November 14, 2012, http://www.nrg.co.il/online/1/ART2/415/591.html.

30 For comments by Barack Obama on Israel's right of self-defense, see http://www.israelandstuff.com/obama-discussed-details-of-operation-pillar-of-defense-with-netanyahu-on-friday; Itamar Levin, "EU: Israel Has Right to Self-Defense," *Channel 1 News*, November 19, 2012, http://www.news1.co.il/Archive/001-D-314635-00.html.

31 Ben Naftali and Shani, *International Law*, p. 82.

32 The sanctions imposed on the Palestinians as a result of the rockets fired at Israel during President Barack Obama's visit in March 2013 were a reduction in the fishing zone permitted to them, from six miles from the coast to three, and the closure of the Kerem Shalom border crossing to traffic carrying goods to the Gaza Strip. "IDF Responds to Rocket Fire This Morning: Fishing to be Restricted to Area in Effect before Pillar of Defense," *Channel 2 News,* March 21, 2013, http://www.mako.co.il/news-military/security/Article-419e4e0f95e8d31004.htm.

33 See comments by Israel's ambassador to the UN Ron Prosor, in a letter to the Security Council and the UN secretary general, asking the Council to condemn the rocket fire from the Gaza Strip at the end of the Passover vacation. Yitzhak Ben Horin, "Israel's UN Ambassador: Security Council Should Condemn Rocket Fire," *Ynet*, April 5, 2013, http://www.ynet.co.il/articles/0,7340,L-4364311,00.html.

34 Amir Buhbut, "Iron Dome Identifies but does not Intercept Launches from Sinai," *Walla*, April 17, 2013, http://news.walla.co.il/?w=/551/2633842.

35 Neri Brenner, "Rocket Salvos: One Moderately Wounded at Factory in Sha'ar Hanegev," *Ynet*, June 23, 2012, http://www.ynet.co.il/articles/0,7340,L-4246070,00.html.

36 According to BDI, a business information company, the cost of Operation Pillar of Defense to the Israeli economy was some 1.1 billion shekels a week. See Ora Koren, "Exclusive: Cost of Operation Pillar of Defense to Economy Estimated at 1.1 Billion Shekels a Week, *The Marker*, November 18, 2012, http://www.themarker.com/news/1.1867734.

37 Shapir, "Lessons from the Iron Dome," p. 85.

38 Author's interview with Defense Ministry official, January 16, 2013.

39 IDF Spokesman, "The Changing Face of Battle," p. 5.

40 An examination conducted by an organization named If Americans Knew indicates that between 1955 and 2013, at least seventy-seven UN resolutions were passed condemning Israeli operations in the context of the Palestinian issue and only one against the Palestinians. See http://www.ifamericansknew.org/stat/un.html.

41 See comments by UN ambassador Ron Prosor prior to Operation Pillar of Defense about the Security Council's silence on the massive rocket fire directed at Israel. Delegation of Israel to the UN, "Comments by Israel's Ambassador to the United Nations in the Security Council Emergency Session following the Escalation in the South," Israel Foreign Ministry, November 14, 2012, http://www.mfa.gov.il/MFAHeb/Diplomatic+updates/Events/Remarks_by_Ron_Prossor+_-_Security_Council_emergency_meeting_141112.htm?DisplayMode=print.

42 For example, IAF attacks on terror facilities in the area of Beit Lahiya and Gaza after rockets were fired at Israel in April 2013. Roni Daniel, "For the First Time in Six Months, IDF Attacks in Gaza," *Channel 2 News*, April 3, 2013.

43 IDF Spokesman, "The Changing Face of Battle," p. 20.

44 "Operation Pillar of Defense," Foreign Ministry, November 14, 2012.

45 "Terror Cell that Fired Rockets at Israel Attacked," IDF, October 14, 2012, http://www.idf.il/1133-17296-he/Dover.aspx.

46 As of 2012, more than 70 percent of Israelis had some kind of protected space in which to stay during an attack, http://www.ynet.co.il/home/0,7340,L-3076-18039-31221738,00.html.

47 General Security Services, "Annual Summary of Figures and Trends in Terrorism and Prevention for 2012," *General Security Services Terrorism Portal*, 2012, http://www.shabak.gov.il/publications/study/Pages/summary2012.aspx.

48 "B'Tselem Figures: Scope of Damage to Civilians Increased Significantly in the Second Half of Operation Pillar of Defense," B'Tselem, May 8, 2013, http://www.btselem.org/hebrew/press_releases/20130509_pillar_of_defense_report; Nissan, "Pillar of Defense – The Numbers."

49 During Operation Pillar of Defense, despite the use of Iron Dome, 6 Israelis were killed and some 270 injured. Fifty-eight rockets fell in built-up areas (indicating that if Israelis had not listened to instructions from the Home Front Command and entered the protected space when the siren went off,

the casualties on the Israeli side could have been much higher). General Security Services, "Annual Summary of Figures and Trends"; Nissan, "Pillar of Defense – The Numbers."

50 Comments by Netanyahu to the Jewish Agency Board of Governors, http://antisemitism.org.il/article/77534/%D7%A0%D7%AA%D7%A0%D7%99%D7%94%D7%95-%D7%93%D7%94-%D7%9C%D7%92%D7%99%D7%98%D7%99%D7%9E%D7%A6%D7%99%D7%94-%D7%A9%D7%9C-%D7%99%D7%A9%D7%A8%D7%90%D7%9C-%D7%94%D7%99%D7%90-%D7%90%D7%97%D7%AA-%D7%9E%D7%94%D7%9B%D7%A9%D7%9C%D7%99%D7%9D-%D7%94%D7%9E%D7%95%D7%A1%D7%A8%D7%99%D7%99%D7%9D-%D7%94%D7%92%D7%93%D7%95%D7%9C%D7%99%D7%9D-%D7%A9%D7%9C-%D7%96%D7%9E%D7%A0%D7%A0%D7%95.

51 Success in this case means deterring the enemy for the long term, reducing the damage that terrorist organization can cause to civilians and to property, and restoring quiet for the long term.

52 Walzer, *Just and Unjust Wars*, p. 29.

53 See comments by President Obama in favor of an Israeli action but against a ground operation in the Gaza Strip. Shai Ben Ari, "Obama against Ground Operation in Gaza: Better Not to Do It," *Channel 2 News*, November 18, 2012, http://www.mako.co.il/news-military/israel/Article-eceffb77da31b31004.htm.

54 "CNN Poll: Most Americans Support Operation Pillar of Defense," *Ynet*, November 19, 2012, http://www.ynet.co.il/articles/0,7340,L-4308639,00.html.

55 Mark Thompson, "Iron Dome: A Missile Shield that Works," *Time*, October 19, 2012, http://nation.time.com/2012/11/19/iron-dome-a-missile-shield-that-works/.

Russia's Security Intentions in a Melting Arctic

Lincoln Edson Flake

As the only non-NATO littoral state in the Arctic, Russia's policies have great relevance for the region's security environment. A series of military deployments and announced upgrades to infrastructure and weapon systems since 2007 have led to speculations that Moscow seeks to re-militarize its Arctic sector in anticipation of a warmer climate in the region. Using strategy documents and policy pronouncements since 2008 as instruments of analysis, this paper considers Moscow's security intentions in a climatically changing Arctic. The findings reveal that Russia is not on course to reconstitute its prior military strength in the Arctic and is generally disinclined to initiate an arms race. Instead of supporting a "Great Game" confrontation, Russia's military footprint in the Arctic is increasingly linked with the Kremlin's controversial jurisdictional assertions.

Keywords: Russia, Arctic, military, climate change, maritime jurisdiction, militarization, state strategies

Introduction

Since the record-breaking 2007 summer ice melt, two narratives have dominated analyses of Russia's Arctic strategy. The first to take root was based on a zero-sum, confrontational approach, according to which

Lincoln E. Flake is a research fellow with the US National Intelligence University based at the Institute of International Security and Intelligence, University of Cambridge, and is also a visiting scholar at the Wolfson College, Cambridge. The research for this article was conducted at the Scott Polar Research Institute (SPRI). The opinions expressed here are the author's alone. They do not represent those of the National Intelligence University, Department of Defense, or the United States government.

Russia acts unilaterally to achieve its expansionist strategic interests. The theatrical planting of a Russian flag on the North Pole seabed and provocative bomber flights along NATO's Arctic frontier in 2007 were two early data points for this pessimistic appraisal of Russian motives. The second narrative has developed more recently and argues that the Kremlin appreciates that its own interests are best served through bilateral and multilateral compromise. Evidence in support of this argument has been plentiful recently and includes the 2010 Russia-Norway maritime delineation agreement on the Barents Sea and the Arctic Council's first binding treaties, on search-and-rescue in 2011 and oil-spill response in 2013.

Concurrent with these narratives are differing assessments of Russia's military intentions in the Arctic. As climate change opens up a more accessible theater of operations in the Arctic for the world's navies, littoral states are increasing the tempo of military maneuvers in the region. Russian activity is especially pronounced, out-pacing all other Arctic nations in terms of military forces operating in both the air and maritime realms. Some commentators have noted the risk of instability and the potential for an arms race between the four NATO rim states and Russia as a result of numerous interstate disputes, most of which involve lucrative economic opportunities such as fishing, energy extraction, and transportation.[1] In 2010, NATO's Supreme Allied Commander for Europe, US Admiral James Stavridis, cautioned that the struggle for Arctic resources could ignite a new "cold war" in the region.[2] Other commentators have downplayed the threat of conflict and the risk of militarization by emphasizing that security enhancements since 2007 constitute logical and peaceful preparations for a more navigable Arctic.[3]

The competing narratives have come about largely as a result of Russia's erratic Arctic policies following the 2007 ice melt. Belligerent rhetoric by Putin and other Russian officials contrasted with conciliatory moves at the bilateral level and in the multilateral forum of the eight-member Arctic Council. To some extent, this pattern continues as evidenced by Vladimir Putin's comments to the Russian Defense Ministry Board in February 2013 in which he accused the West of methodical attempts to alter the strategic balance and warned of a militarized Arctic.[4] In spite of such rhetoric, in the past two years the Kremlin has issued a wealth of policy statements, investment decisions, and military commitments related to the Arctic,

providing ample data to separate bluster from intent. Russia's security intentions are no longer shrouded in secrecy or obscured in mix messages.

This article addresses the question of Russia's military objectives in the Arctic in order to gauge not only the likelihood of a regional arms race but also to draw broader conclusions concerning the trajectory of Moscow's security policy in the Arctic.

Contextualization

Before evaluating recent developments, it is necessary to put Russian military advances in the Arctic since 2007 into perspective. At first glance, Russian activity appears disconcerting. In August 2007, Russia resumed strategic bomber flights by Long Range Aviation assets over the Arctic after a 15-year respite. This was followed by a decision to form two specialized Arctic brigades, and more recently to base MiG-31 long-range interceptors at Rogachyovo Air Base, near Belushya Guba on the Novaya Zemlya archipelago. In February 2013, the Northern Fleet's Naval Aviation began flying patrol missions on a permanent basis in the Arctic latitudes of the northern ice ocean. In addition to ambitious ship modernization plans, including deployment of Borei-class submarines and a French-built Mistral class amphibious assault ship, the Fleet will expand the zone of combat patrols of strategic submarines in the Arctic beginning in 2014.[5] Recently, in September 2013, Vladimir Putin announced plans to reopen Soviet-era military bases in the Arctic.[6]

Notwithstanding the flurry of announcements related to the Arctic in recent years, when these security moves are viewed through various contexts, they appear much less ominous. First, contemporary activities need to be judged against historical patterns of fluctuating military readiness and capabilities in the Arctic. Prior to World War II, the Arctic had very little strategic military utility, with Czarist, and then Soviet planners only gradually gaining an appreciation for the security opportunities and threats the Arctic presented. The Soviets established the Northern Flotilla in 1933, upgrading it to fleet status in 1937, but maintained a faint military footprint in the immediate post-World War II period.[7] It was not until the nuclear arms race that the region became a priority in military planning, as Soviet submarines roamed the Arctic under cover of ice as a virtually unassailable strategic force. Consequently, the late Soviet-era witnessed an enormous shift of capacity to the Northern Fleet, with bases operating out

of the Murmansk-Kola area. The fleet surpassed the Baltic and Black Sea Fleets, and by 1981, 57 percent of all Soviet submarines and 52 percent of its strategic submarines were stationed in the North.[8] By 1988, the strike power of Northern Fleet strategic and attack submarines was estimated to be greater than the other three fleets combined.[9] Similar increases in aviation, non-strategic naval capacity, and surveillance competency occurred from the 1960s to the mid 1980s along the Soviet Arctic coastline.

In the 1990s, the pendulum swung back dramatically as a result of the collapse of the Soviet Union, which left "Russia's massive Arctic military infrastructure to decay and rot."[10] Capabilities in radar coverage, aviation, and naval patrol were gutted. The situation on the ground did not change noticeably with the departure of Boris Yeltsin and the arrival of Vladimir Putin in 1999. From 1993 to 2003, the Air Force did not receive a single strategic bomber and only received three between 2004 and 2009.[11] Katarzyna Zysk points out that as late as 2006, capacity was still being drained from the Arctic for the sake of more urgent strategic problems, as evidenced in the disbandment of the Vorkuta-based Independent Arctic Border Detachment and the transfer of its human and material resources to the North Caucasus region.[12] The atrophy of the Soviet military presence during the 1990s and early 2000s acted to essentially demilitarize the region. A comparison of the fleet's order of battle in 1986 and 2013 illustrates the extent of the deterioration (table 1).[13]

Table 1. Northern Fleet Order of Battle, 1986 and 2013

	Surface Vessels	Submarines	Naval Aviation
1986	100	170	400
2013	41	43	119
Combat ready	12-29	8	57

Notwithstanding recent moves, the Northern Fleet remains a shell of its Soviet strength. A 2013 Russian analysis of the Northern Fleet capabilities surmised that the fleet is only 25-30 percent capable of supporting Russia's peacetime obligations and could only assemble a surface strike group of two or three small missile ships in the event of combat with enemy surface forces in the littoral zone.[14] The current state of Russia's military infrastructure and radar monitoring of its Arctic coastline is not much

better. Contemporary improvements to the Northern Fleet, therefore, commenced from a very dismal starting point. Even if all ambitious targets are met, which is highly improbable in light of post-Soviet precedents and current budgetary constraints, the outcome would likely be to merely arrest the further deterioration of capabilities.

Second, when Russia's security moves in the Arctic are placed in the context of the nation's larger trend to reform and modernize its armed forces, they appear less grandiose. In 2008, Russia embarked on one of the most ambitious military reforms, reorganization, and equipment modernization programs in its history, in which the Arctic is but one component. The plans call for more than 20 trillion rubles ($650 billion) by 2020 to completely overhaul its military hardware so that "by 2015, the proportion of the new generation of weapons should be 30 percent, and by 2020 reach 70-100 percent."[15] In contrast to other post-Soviet efforts, the current program has considerable political will behind it as evidenced by overall military spending in 2012 increasing by 24 percent – a jump of nearly $90 billion or 113 percent from 2003 military expenditures.[16] Military spending is envisioned to jump 18 percent in 2014 and 60 percent from 2014-2016. The defense budget portion of the Russian GDP is envisioned to grow from 3.1 percent in 2012 to 3.9 percent in 2016.

The impact of this reform program on the Arctic has been surprisingly subtle. Reorganizations and increased training tempo in the Arctic have occurred in line with overall efforts in the Russian military since 2008, and the nominal improvement in Russia's Arctic military footprint is largely proportional to the overall increase in military spending in recent years. However, by some measurements, the Northern Fleet has actually trailed the other fleets. For instance, the overall tonnage of the Russian fleet dropped from its 1990 peak of 2.6 million tons (Mt) to 1 Mt by 2008, before increasing slightly to 1.07 Mt by 2012. Correspondingly, the number of vessels dropped from 406 to a low of 119, and by 2012 only recovered to 131.[17] Yet the Northern Fleet tonnage continued to drop from 2008 to 2012 from 583,000 to 545,000 tons as well as its ship total.[18] In addition, the Northern Fleet suffers from the same missed deadlines and inefficiencies as the other fleets, which hamper modernization efforts. In a meeting on July 29, 2013 on state orders for the navy, Vladimir Putin admitted that State Armament Program-2020 (SAP-2020) objectives would not be met as ships set for commission after 2015 have to be determined by SAP-2025.[19]

Despite discussion of a strategic re-orientation to the Arctic in some Russian security circles, the Northern strategic direction does not appear to be receiving significantly more attention at present than the other three strategic directions. While Russia's first two next-generation ballistic missile submarines, the *Yury Dolgoruky* and *Alexander Nevsky*, were recently given to the Northern Fleet instead of the Pacific Fleet as originally planned, the first two French-built Mistral-class amphibious assault ships will be sent to the Pacific Fleet. Furthermore, it is important to consider that the modernization that is occurring is not a harbinger of malevolent Arctic intent. The mission of the Northern Fleet, particularly during the Soviet era, was not exclusively tied to achieving naval superiority in the Arctic, but rather with maintaining unobstructed access to the Atlantic and viable nuclear deterrence. The prospect of seasonally ice-free Arctic waters will undoubtedly result in a more Arctic-centric mission for the Fleet, but the potential for Arctic conflict is unlikely to be affected as a result of the moderate improvements envisaged for the Northern Fleet.

Finally, Russia's moves appear less exceptional when placed in the context of overall circumpolar security upgrades. Russia's Arctic neighbors are also augmenting their security presence in the Arctic as a result of climate change exposing their once inaccessible coastlines to human activity. While these improvements occur in tandem with Russian force upgrades, there is little evidence that they are occurring because of Russian decision making. Canada has announced plans to launch a new fleet of up to eight Arctic off-shore patrol ships and establish an Arctic training base in Resolute Bay and a deep-water berthing and refueling facility at Nanisivik. It also intends to create a 500-strong army unit comprising four companies of 120 troops apiece for Far North operations, and hold its largest-ever military exercise in the region.[20] Norway and Denmark have followed suit with their own realignments and equipment upgrades. Even so, in 2012, Frederic Lasserre et al. conducted a quantitative analysis of the Arctic coastal states' navies and concluded that "the overall picture of Arctic military evolution is one of limited modernization, limited increases or change in equipment."[21]

Clarity of Strategic Goals

With these perspectives as a backdrop, the military aspects of Russia's Arctic strategy can be better appreciated. Fortunately, the fog around

Russian security intentions in the Arctic has gradually lifted in recent years. The nationalist messaging and provocative gestures that permeated Russia's Arctic policy during Putin's second presidential term (2004-2008) have given way to a more thoughtful approach. Gestures such as the resumption of strategic bomber flights from the 37th Air Army, which were likely motivated by non-strategic rationale, have lost utility. For instance, the formation of the two Arctic specific brigades as well as the redeployment of an aviation group of MiG-31 interceptors to the Soviet-built Rogachevo airfield have recently both been pushed back, with the initial announcements labeled as "politically-motivated" and detached from real needs by Russian media.[22] More recent activity has had less to do with international optics and much more to do with supporting strategic goals.

Climate change, and in particularly the realization that its long Arctic coastline could be fully exposed to ice-free summers, appears to be the primary driver of change in Kremlin policy. Russian activities, in the security, economic, political, and legal realms, have increased in unison with reduction in sea ice. Strategy documents as well as official rhetoric since 2007 have been infused with an explicit sense of urgency linked to the ice melt. This stands in contrast to the 1990s and early 2000s when the climate change factor was only tangentially addressed in official political discourse related to the Arctic. The growing prospect of ice-free conditions has focused Moscow's attention. Apart from the drastic seasonal reduction in sea ice cover, the ice that remains is mostly younger, thinner ice sufficiently porous to allow penetration by sunlight, thus "further accelerating the melting of the entire sea ice area."

Moscow's preoccupation with the Arctic is understandable as the region is much more significant for Russia's present and future economic vitality than it is for any other Arctic nation. The Arctic accounts for approximately 20 percent of Russia's GDP and 22 percent of total Russian exports. Over 90 percent of its nickel and cobalt, 60 percent of its copper, and 96 percent of its platinoids come from Arctic mines. The melting ice exposes the vast amount of hydrocarbon wealth of the Arctic basin. According to figures published by the Institute of Oil and Gas Problems, Russia will be pumping up to 30 million tons of oil and 130 billion m3 of natural gas out of its Arctic shelf by 2030.[23] In addition to hydrocarbon wealth, the Arctic offers lucrative transportation routes. The Northern Sea Route (NSR) extends

across the Arctic Ocean seas (Kara, Laptev, East Siberian, and Chukchi) off the Russian Arctic coast and is the shortest route from Europe to the Far East. Furthermore, receding ice exposes Russia's largely unmanned and unmonitored 17,500 kilometer coastline to piracy, illegal fishing, and smuggling.

The shift away from nationalist-tinged talk of militarization toward a more practical emphasis on preparing for increased human and economic activity in the Arctic is best illustrated by comparing the *2000 National Security Concept, 2001 Maritime Doctrine,* and *2001 Basics of State Policy of the Russian Federation in the Arctic Region* with the *2008 Fundamentals of State Policy of the Russian Federation in the Arctic in the Period up to 2020 and Beyond* and the *2009 National Security Strategy.* The content and tone of the documents are distinctly different. The former documents contained abrasive rhetoric focused on activities linked to Russia's military security, Cold War concepts of strategic balance, NATO rivalry, and zero sum competition in the Arctic. The 2001 Arctic Policy paper maintained that "all types of activity in the Arctic are tied to the interests of defense and security to the maximum degree." In contrast, the latter two focused on the prevention of smuggling, terrorism, and illegal immigration through enhanced constabulary competence. Their content centered primarily on increased human activity and resulting economic development and avoided suggesting that Russia harbors ambitions to re-militarize the Arctic region.[24] Indeed, military security is not mentioned among the urgent priorities in stark contrast to the 2001 Arctic strategy in which military strength pervaded. [25] Instead, emphasis is placed on preparing the Arctic to be a "national strategic resource base" and the NSR to be an "international maritime navigation [passage] within the jurisdiction of Russian Federation." The differences between the two sets of strategy papers are also found in their applications. While the former papers had little practical bearing on security developments in the ensuing seven years as ambition did not translate into capability, the 2008 Arctic Strategy has been a fairly reliable blueprint for Russia's Arctic policies to date.

Enhancement of border security infrastructure, not military capability, has been the focus of Russian attention since the release of the 2008 Arctic Strategy. Particular emphasis is placed on coordination of effort across multiple federal entities, with the Federal Security Service (FSB) and its border guard branch taking the lead and with Northern Fleet units

in a subordinate role. In 2009, Moscow re-established units within the Arkhangelsk and Murmansk border guard to patrol the NSR in step with the 2008 Arctic Strategy plan for a comprehensive Arctic coastal defense infrastructure by 2020. A number of "dual use" facilities in the Arctic are being constructed to host commercial craft as well as vessels of both the Northern Fleet and the FSB's border service.[26] Eleven facilities will be deployed in the Arctic before 2020, and will be co-located with new "emergency-rescue centers" currently being built across northern Russia at Murmansk, Archangelsk, Naryan-Mar, Vorkuta, Nadym, Dudinka, Tiksi, Pevek, Provideniya, and Andyr.[27] In late 2013, Russia announced that these sites, as well as several other former Soviet military bases in the Arctic, will have their airfields reconstructed as part of a larger military infrastructure renewal program in the Arctic.

This infrastructure enhancement aligns with plans to deploy a combined-arms force by 2020 that will include military, border, and coastal guard units to protect Russia's economic and political interests in the Arctic.[28] Plans also call for the expansion of aerial and satellite border monitoring capabilities, centered primarily on the perennially-delayed Arktika space surveillance system, which when fully complete, will comprise four meteorological, communication, and radar satellites.[29] Expansion of the FSB's unmanned aerial vehicles and new ice-class patrol boats are also in development.[30] While these plans will likely encounter delays and budget difficulties as is common in Russia, there can be little doubt that Moscow is genuinely interested in an integrated approach to protecting what Russian academics increasingly refer to as the Arctic Zone of Russia (AZR).

Russian Arctic Interests after the Ice

While Russia's operational commitments have become increasingly clear of late, its motives remain more obscure. Some insist recent moves reveal designs "not on a military confrontation with Arctic riparian countries, but on control of illegal trafficking, terrorism, poaching, and environmental threats."[31] Yet ascribing only benign motives to Russia's security machinations in the Arctic may be too unassuming. After all, Russian officials routinely state that security advances are needed to protect against future foreign designs on Russian interests in the Arctic. In July 2013, outspoken nationalist and Deputy Prime Minister Dmitry Rogozin

listed the Arctic as one of five possible conflict scenarios in Russia's future, but did not mention the source of future tensions.[32] This type of rhetoric and the substantial efforts currently being exerted to enhance constabulary capabilities are unlikely motivated exclusively by the prospects of piracy or illegal fishing.

The moves are also unlikely to be tied to many other circumpolar disputes which affect, to some degree, Russian interests. Take for instance the issue of access to the emerging fishing stocks in the Arctic. Recent developments suggest that the matter has little bearing on Russia's security posture. Russia already has exclusive and undisputed rights to all living organisms in the water column to 200 nautical miles (337 km) of its shoreline. Furthermore, the dispute concerning fishing in the international waters in the Central Arctic region is on course for resolution. In early 2013, Russia moved its objection to circumpolar negotiations on the issue. These negotiations are ongoing and promising. Similarly, Russia's maritime territorial issues have either been resolved, as with the Barents Sea deal with Norway in 2010, or they have entered a permanent dormant state, as in the case of the maritime boundary with the US in the Bering Sea.

The issue most cited by Russian nationalists to justify enhanced security presence is the threat of foreign claims on Russia's Arctic energy reserves. Yet such a scenario seems highly improbable. As with fishing, Russia has undisputed claim to all seabed resources in its immense Arctic economic exclusion zone (EEZ). Indeed, by some accounts, 80-95 percent of the potential resources are found in undisputed jurisdiction, with Russia's EEZ accounting for the 80 percent of the region's natural gas.[33] The international order would have to become quite anarchic for Russia's rights to these reserves to be seriously threatened. Nationalists, such as Rogozin, may have in mind perceived rights to the disputed seabed of the Central Arctic Region, but even on that subject, conflict is becoming increasingly remote. First, there is not much to fight over. Pavel Baev notes, "The top of the globe does not promise much in the way of oil and gas, even if the entire icecap were to melt. Extracting oil from the [Central Arctic Region] is not possible since there is no oil to extract."[34] Second, Moscow's commitment to work within UN procedures has been unequivocal, and most recently enshrined in the Arctic Council's 2008 Ilulissat Declaration in which all the Arctic states agreed to "the orderly settlement of any possible overlapping claims."[35] Finally, Russia's concessions to Norway in the 2010 Barents Sea

maritime agreement, recent conciliatory comments by Putin on the issue, and the simple fact that the vast majority of seabed claims do not overlap but at the North Pole, further suggests the issue is unlikely to escalate.

Defending the Northern Sea Route

The dispute that appears most associated with Russian activity since 2008 involves maritime jurisdiction over the 3,000 nautical mile-long (5,560 km) Northern Sea Route (NSR). Even as Russia has become more constructive and predicable on other disputes, it has continued to pursue a unilateral approach on the issue of navigation. Disagreement over the contested waterways off Russia's Arctic coastline lacks a clear path to resolution. The route cuts 40 percent off sailing times between Asia and Europe and is an attractive transport corridor for Asian exporting nations and sea line of communication (SLOC) for the world's navies. Yet Russia claims extra-jurisdictional control over two geographical domains in the Arctic: straits and the EEZ. Starting closer to the shoreline, Moscow insists that all key straits along the NSR are internal waters and therefore exempt from innocent passage regime. National legislation to this effect was codified by the Soviets in 1985 and endorsed by the present regime. Extending further out, Russia also asserts the privileges to regulate traffic in its 200 nautical mile EEZ, which would typically be considered high seas and outside the purview of coastal states' national legislations. It cites Article 234 of the 1982 UN Convention of the Law of the Sea (UNCLOS) which grants extra-jurisdictional rights to coastal states in ice-covered waters "for the prevention, reduction and control of marine pollution from vessels in ice-covered areas within the limits of the exclusive economic zone."[36] Both assertions rest on controversial readings of international law, with many nations, including the US, holding opposing opinions.

Taken together, these claims require foreign vessels to receive Moscow's permission and comply with burdensome and costly regulations including pilotage and ice-breaker escort, as well as specific design, equipment, and manning standards.[37] The impetus behind recent activity in the Arctic appears to be concerns over navigational rights. Russia recently moved to reaffirm these requirements in a new federal law, adopted on July 3, 2012, which defined the NSR as: "the water area adjacent to the Northern coast of the Russian Federation, comprising the internal sea waters, the territorial sea, the adjacent zone and the exclusive economic zone of the

Russian Federation and confined in the East with the Line of Maritime Demarcation with the United States of America."[38] On January 17, 2013, the Ministry of Transport issued the first updated rules on NSR regulations since 1990 and a new NSR administrative body was established shortly thereafter to oversee the rules.[39] Of particular note among the changes from the previous iteration of NSR laws issued in the early 1990s is the expanding geographic understanding of the NSR in Russian thought from a number of sea routes to its entire Arctic EEZ, encompassing nearly a fifth of the Arctic Ocean. The timing of legislative and regulatory moves with plans to enhance border patrol suggests a degree of policy synchronization. Another factor suggesting Russia's Arctic military posture is increasingly centered on the NSR, is the fact that the ice melt will have a greater impact on this dispute than any other precisely because climate change drastically affects the legal foundation of navigational claims. Greater accessibility to Arctic energy may peak coastal states' interests to acquire seabed access, but it does nothing to alter the well-established and respected laws, procedures, and mediating process. Yet concerning navigation, ice reduction undermines Russia's Article 234 argument that rests on the presence of ice to justify control. Reduction in sea ice in 2007, and again in 2012, portends a more navigable Arctic Ocean in the coming decades and with it, potential challenges to Russia's draconian regulations.

Indeed, Russian fears have been somewhat validated during the 2013 shipping season. With more favorable ice conditions, applications for NSR sailing permits have risen from a handful a few years ago to over 400 in 2013. Moscow is pleased with this development but has also had its regulatory regime challenged for the first time in nearly 20 years. In August, the Greenpeace icebreaker, *Arctic Sunrise,* was denied permission to sail the NSR three times, before proceeding without approval into the Kara Sea.[40] A day after entering Russia's Arctic EEZ, the vessel was boarded by a Russian coast guard vessel and forced to retreat out of "Russian waters." It is noteworthy that Russia rejected Greenpeace's request for transit three times on technicalities as the non-discriminatory clause of Article 234 prohibits Russia from refusing entry for arbitrary reasons, such as *Arctic Sunrise* 's stated purpose to protest Russia's energy exploration efforts in the Arctic. The incident is reminiscent of the Soviet maritime stand-off with US Coast Guard vessels attempting to traverse the NSR in the 1960s.

Both episodes, along with the tone of Russia's historic and contemporary polices on navigation along its Arctic coastline, undermine optimistic assessments. For instance, Michael Becker's 2010 assessment that the issue of NSR access will likely be resolved by negotiations and not escalate "if the ultimate interest is safe and clean commercial shipping,"[41] appears to be based on dubious appraisal of Russian interests. He cited Professor James Kraska of the US Naval War College 2007 upbeat assessment of the Northwest Passage navigation dispute. Kraska's line of reasoning may be suitable for Canada, where environmental protection concerns are likely at the forefront, but Russian motives are more intertwined with a desire to control a geo-strategic space it considers exclusively Russian.

NATO Exclusion Zone

Moscow's anxiety is not restricted solely to environmentalists, but also to foreign military vessels. Moscow's objections to Western intrusion into its Arctic sector stretch back to the 1960s and a series of mini naval standoffs with US Coast Guard vessels seeking to circumnavigate the Arctic. Russia is concerned that a more navigable Arctic will attract NATO warships to the Arctic Basin, as well as naval vessels of any flag into its EEZ. Since 2009, Kremlin officials have been outspoken in opposing NATO in the Arctic. In 2009, Russian Foreign Minister Sergei Lavrov rejected the presence of outside "military-political alliances" in the region, while Chief of the General Staff Nikolai Makarov warned a NATO audience in Iceland that the presence of Alliance warships in the Arctic would necessitate changes to Russian defense planning.[42] At the June 2013 Barents Summit in Norway, Russia's Prime Minister Dmitry Medvedev warned:

> Any expansion of NATO to include Sweden and Finland would upset the balance of power and force Russia to respond... In the 1990s after the dissolution of the Warsaw Pact Organization NATO openly broke its promise not to spread military infrastructure closer to Russia's borders. Today independent experts are concerned that NATO may use emergency and disaster preparedness measures to cover its indirect attempts to militarize the Arctic.[43]

Medvedev's decision to link the Arctic with Russia's feeling of being wronged in the former Soviet space is especially intriguing, as Kremlin policymakers likely view both regions in similar terms. Russia's

preoccupation with peripheral buffer zones goes back centuries, with the post-Soviet struggle for influence in its self-proclaimed "near abroad" being the most recent manifestation. In 2006, Russian military commentator O. Litkova went so far as to argue that "the Arctic could significantly compensate Russia for the losses she suffered as a result of the collapse of the USSR."[44] The Arctic, like the near abroad, is viewed in terms of sectorial divisions in which Russia believes that history and geography afford it exclusive right of influence. In the case of the Arctic, this belief stretches back at least to the Soviet's 1926 decree in which all territories within the extreme meridians of Russia's eastern and western borders running to the North Pole were claimed as Russian.

Russia fears that the ice melt will do to the Arctic what the fall of communism did in Eastern Europe, that is, usher in a period of NATO encroachment into their traditional space. In 2011, two leading academic voices in Russia opined:

> Officials and experts agree that NATO continues on a course toward enhancing its activity in the Arctic. What consequence will this have on Russia? In all aspects – negative.... With regard to the fierce competition for Arctic resources, NATO will squeeze Russia out, just as it squeezes Russia in other regions of Europe in the sphere of security. It is obvious that the USA, which is not party to [UNCLOS] will use NATO to strengthen its position in the region....Therefore, Russia should prepare for a difficult and long battle for the settling of its interest and legal rights.[45]

Conclusion

Russia's preparations are ongoing and clearly have a military component. Even so, Russia is not prioritizing the Arctic in its defense planning. It appears more concerned with the legal ramifications of the changing Arctic environment than with grand strategic questions of nuclear deterrence and naval force parity in the region. Consequently, security measures in the Arctic will remain closely tied to supporting specific national interests as outlined in strategy documents, most notably control over surface traffic in Russia's Arctic waters. The changing remit of the Northern Fleet is meant to augment efforts in other spheres, such as the modernization of maritime legislations and regulations, with the ultimate goal of establishing

irreversible precedent of control in anticipation of greater Arctic surface traffic. This highly nuanced security machination has been overshadowed by the more spectacular, yet less strategically significant, acts of military bluster in the Arctic since 2007.

Russia's course of action defies the competing narratives presented in the introduction of either an alarming return to Soviet-era Arctic militarization or a measured and rational response to climate change. Moscow's designs are neither entirely benign nor entirely belligerent. While moderate improvements to naval capability are occurring, current developments do not amount to a reconstitution of anything approaching Soviet-era strength. Military spending in the Arctic has suffered and benefited from the same economic swings of boom and bust that has affected the readiness of the rest of Russia's armed forces since 1991. Even with the altering deployment characteristic of the Arctic Ocean, there is no indication that this correlation will change or that Russia harbors malicious intent in the region.

At the same time, the Kremlin's perception that the region falls within its sphere of influence remains at odds with Western perception. Subsequently, Russia's cooperative attitude of late in the Arctic should not be extrapolated to all circumpolar disputes. When it comes to navigational rights, Russia's interests are not aligned with those of most Western nations. The divide between the two sides will only widen as a result of climate change. If Western nations and NATO are counting on Russia's obsession over its Arctic waters to fade away with the ice, they are likely to be disappointed.

Notes

1 Margaret Blunden, "The New Problem of Arctic Stability," *Survival: Global Politics and Strategy* 51 (2009): 121-42.

2 Terry Macalister, "Climate Change Could Lead to Arctic Conflict, Warns Senior NATO Commander," *The Guardian*, October 11, 2010, http://www.theguardian.com/environment/2010/oct/11/nato-conflict-arctic-resources.

3 Jeffrey Mazo and Sara French, "Arctic Security," *Policy Brief*, July 30, 2012, http://arcticsummercollege.org/sites/default/files/Security%20Policy%20Brief_Arctic%20Summer%20College_July%2030%202012_0.pdf.

4 Thomas Nilsen, "Danger of Militarization of the Arctic Exists," *Barents Observer*, February 27, 2013, http://barentsobserver.com/en/security/2013/02/danger-militarization-arctic-exists-27-02.

5 "Navy Plans to Start Ocean Patrol in 2014," *Moscow Vzglyad*, June 1, 2013. Tu-142 long-range anti-submarine warfare aircraft and Il-38 medium-range anti-submarine warfare aircraft will be tasked with patrolling the Northern Sea Route, taking off from naval aviation airfields located in Murmansk and Vologda Oblasts.

6 "Putin: Russia to reopen Soviet-era Arctic military base," *Reuters*, September 16, 2013, http://www.reuters.com/article/2013/09/16/us-russia-arctic-idUSBRE98F0VX20130916.

7 Michael MccGwire, "Strategic Interests in the Arctic Ocean," in *Sovereignty and Security in the Arctic*, eds. Edgar Dosman (London: Routledge, 1989), p. 24. For an in-depth look at Bolshevik Russia's interests in the Arctic see John McCannon, *Red Arctic: Polar Exploration and the Myth of the North in the Soviet Union, 1932-1939* (Oxford: Oxford University Press, 1998), pp. 22-23.

8 Willy Ostreng, *The Soviet Union in Arctic Waters* (Honolulu: The Law of the Sea Institute, 1982), p. 1.

9 Clive Archer, *The Soviet Union and Northern Waters* (London: Routledge, 1988), p. 22.

10 Pavel K. Baev, "Troublemaking and Risk-Taking: The North in Russian Military Activities," in *Russian and the North*, eds. Elana Wilson Rowe (Ottawa: University of Ottawa Press, 2009), p. 18.

11 Frederic Lasserre, Jérôme Le Roy, and Richard Garon, "Is There an Arms Race in the Arctic?" *Journal of Military and Strategic Studies* 14, no. 3&4 (2012): 1-56, p. 17.

12 Katarzyna Zysk, "Military Aspects of Russia's Arctic Policy," in *Arctic Security in the Age of Climate Change,* eds. James Kraska (Cambridge: Cambridge Press, 2011), p. 102.

13 Table data obtained from Konstantin Sivkov, "Russia's Northern Redoubt: the Fleet is Required to Reliably Protect the Country's Interests in the Arctic," *Voyenno-Promyshlennyy Kuryer*, January 16, 2013, and Pavel K. Baev, "Troublemaking and Risk-Taking: The North in Russian Military Activities," p. 23.

14 Ibid.

15 Konstantin Bogdanov, "The State Armament Program Reset," *Nasionalnaya Oborona*, November 2013, http://www.oborona.ru/includes/periodics/armament/2011/1212/14237820/detail.shtml.

16 Stockholm International Peace Research Institute, "Military Expenditure Database," http://www.sipri.org/research/armaments/milex/publications.

17 Lasserre et al., "Is There an Arms Race in the Arctic?" p. 19.

18 Ibid., p. 22.

19 Alexander Golts, "Jumping Through Military Hoops," *Moscow Times*, August 6, 2013, http://www.themoscowtimes.com/opinion/article/jumping-through-military-hoops/484178.html.

20 NATO Parliamentary Assembly Report, "Security at the Top of the World: Is There a NATO Role in the High North?," (213 DSCTC 10 E), 2010.

21 Lasserre et al., "Is There an Arms Race in the Arctic?" p. 56.
22 "Proposal to Base Fighter Group on Novaya Zemlya Seen as Premature," *Izvestiya*, February 2, 2013. A small military unit has remained at Rogachevo since Soviet times, keeping the airfield in working order. An-26 and An-72 light military transports fly there regularly, and sometimes heavy Il-76s and even wide-bodied An-22. See also Trude Pettersen, "Russian Arctic Brigades Put Off to 2015," *Barents Observer*, February 22, 2013, http://barentsobserver.com/en/topics/russian-arctic-brigades-put-2015.
23 "The Arctic: A Complex Knot of Interstate Differences," *Moscow Military Thought*, September 20, 2010.
24 Presidential Decree, President Dmitry Medvedev, "The Fundamentals of State Policy of the Russian Federation in the Arctic in the period up to 2020 and beyond," September 18, 2008, http://www.scrf.gov.ru/documents/98.html.
25 Lasserre et al., "Is There an Arms Race in the Arctic?" p. 5.
26 Mark Adomanis, "Russia Plans Massive Arctic Expansion," *USNI News*, August 9, 2012, http://news.usni.org/2012/08/09/russia-plans-massive-arctic-expansion.
27 Ibid.
28 Trude Pettersen, "Motorized Infantry Brigade to Northern Fleet," *Barents Observer*, November 26, 2012, http://barentsobserver.com/en/security/2012/11/motorized-infantry-brigade-northern-fleet-26-11.
29 Katarzyna Zysk, "Military Aspects of Russia's Arctic Policy," p. 103.
30 Ibid.
31 Lasserre et al., "Is There an Arms Race in the Arctic?" p. 6.
32 "Rogozin Discusses Five War Scenarios, Top Priorities for Military-Industrial Commission," *Moscow Rossiyskaya Gazeta*, July 3, 2013.
33 Arctic Futures Symposium 2011, "The Arctic in a Time of Change," Final Report, Brussels, October 2011, http://www.polarfoundation.org/assets/uploads/documents_files/afs_2011_report_web.pdf.
34 Pavel K. Baev, "The Arctic: A View from Moscow," Carnegie Endowment for International Peace, 2010, http://carnegieendowment.org/files/arctic_cooperation.pdf, p. 21.
35 The Ilulissat Declaration, Arctic Council, May 28, 2008, http://www.oceanlaw.org/downloads/arctic/Ilulissat_Declaration.pdf.
36 United Nations Convention on the Law of the Sea, Part XII, Section 8, Ice Covered Areas, Article 234.
37 R. Douglas Brubaker, "The Northern Sea Route Regime: Exquisite Superpower Subterfuge," *Ocean Development and International Law* 30, no. 4 (1999), p. 320.
38 Russian Federation, "Federal Law – On Amendments to Specific Legislative Acts of the Russian Federation related to Governmental Regulations of Merchant Shipping in the Water Area of the Northern Sea Route," July 28, 2012, http://www.arctic-lio.com/docs/nsr/legislation/federal_law_nsr.pdf.

39 Russian Ministry of Transport, "Rules of Navigation in the Northern Sea Route Water Area," unofficial translation by Arctic Logistics Information Office, January 17, 2013, http://www.arctic-lio.com/docs/nsr/legislation/Rules_of_Navigation_on_the_water_area_of_the_NSR_2013_Registered_12.04.13.pdf.

40 Richard Milne, "Russia Bars Greenpeace's Arctic Sunrise from Northern Sea Route," *Financial Times*, August 21, 2013, http://www.ft.com/cms/s/0/1136d6da-0a4f-11e3-9cec-00144feabdc0.html#axzz2cu7j8Pfz.

41 Michael A. Becker, "Russia and the Arctic: Opportunities for Engagement within the Existing Legal Framework," *American University International Law Review* 25, no.2 (2010): 225-50, 243.

42 "Security Prospects in the High North," seminar organized by NATO Defense College and the government of Iceland, Reykjavik, Iceland, January 28-29, 2009, http://www.nato.int/cps/en/natolive/news_49745.htm.

43 Igor Alexeev, "Demilitarizing Arctic, NATO's Positive Signal to Russia," *Press TV*, July 26, 2013, http://www.presstv.com/detail/2013/06/20/309966/nato-leaving-arctic-good-news-for-russia/.

44 O. Litkova, "Voyenno-Morskaya Ekonomika: Natsional'nyye Interesy Rossii v Moryakh Yevropeysloy Arktiki," *Morskoy Sbornik*, (June 2006), quoted in Roger Boyes, *Meltdown Iceland: How the Global Financial Crisis Bankupted an Entire Country* (London: Bloomsbury Publishing, 2009), p. 181.

45 V. N. Koneshev and A.A. Serynin, *The Arctic in International Politics* (Moscow: Russian Institute of Strategic Research, 2011), p. 134. Author's translation from Russian.

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 Security 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 on various subjects, 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
- Terrorism

Submitted articles should not exceed 6000 words (including citations and footnotes), and should include an abstract of 120 words and a list of up to 10 keywords. Only original material that has not appeared in another publication or is under consideration for publication elsewhere may be submitted. Previous issues of the journal may be accessed on the INSS site at: http://www.inss.org.il/.

For further information, please contact:
Daniel Cohen
Coordinator, *Military & Strategic Affairs*
Cyber Security Program
Tel: +972-3-6400400/ext. 488
Cell: +972-50-5772338
danielc@inss.org.il