# Military and Strategic Affairs

Volume 5 | No. 2 | September 2013

**Processes of Military Decision Making**
Dudi (Yehuda) Alon

**Korea's Wartime Command: Sovereignty, Security, and Independence**
Alon Levkowitz

**Military Contrarianism in Israel:
Room for Opposition by the Chief of Staff to Politicians**
Yagil Levy

**Who Will Stop the Robots?**
Liran Antebi

**The Military Secretary at the Junction of Israel's Security Decisions**
Shmuel Even

**The Revolutionary Guards and the International Drug Trade**
Sami Kronenfeld and Yoel Guzansky

**Cyber Weapons and International Stability**
Guy-Philippe Goldstein

**Don't Terminate: Deter to Prevent**
Uri Rechav

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 5 | No. 2 | **September 2013**

**CONTENTS**

**Processes of Military Decision Making** | **3**
Dudi (Yehuda) Alon

**Korea's Wartime Command: Sovereignty, Security, and Independence** | **21**
Alon Levkowitz

**Military Contrarianism in Israel: Room for Opposition by the Chief of Staff to Politicians** | **39**
Yagil Levy

**Who Will Stop the Robots?** | **61**
Liran Antebi

**The Military Secretary at the Junction of Israel's Security Decisions** | **79**
Shmuel Even

**The Revolutionary Guards and the International Drug Trade** | **105**
Sami Kronenfeld and Yoel Guzansky

**Cyber Weapons and International Stability** | **121**
Guy-Philippe Goldstein

**Don't Terminate: Deter to Prevent** | **141**
Uri Rechav

# 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)

# Processes of Military Decision Making

## Dudi (Yehuda) Alon

This essay examines the prevalent theoretical approaches to decision making and surveys practical models appropriate to the military setting. It discusses and compares the relative advantages and disadvantages of each model, and then makes recommendations about their application to the military decision making process. Currently, two major approaches, the rational and the cognitive, offer an orderly process that may help military leaders make better decisions. Neither is yet complete. Each approach offers its own set of concepts to attain the chief products of the decision making process. These sets of concepts blur the real differences between the approaches and draw one into a debate that does not deal with essence. In addition, both approaches tend at times to take the tools and the ideas and over-develop them into hobbling, constraining techniques, thereby missing the fruits that could have been reaped by a more informed, tempered use of them as ideas. Thus finding a bridge between the approaches that recognizes the advantages and disadvantages of each and makes a temperate, judicious use of the respective tools can allow us to enjoy the best of both worlds.

**Keywords:** decision making; situation assessment; strategic planning; strategic military leadership

> Orderly processes of decision making are supposed to give the decision makers – and those who are charged with evaluating their conduct – means to construct and oversee good judgment that will be helpful in reducing the risk of uncontrolled reliance on emotion, unfounded intuition, impulsive response, and personal or political considerations liable to be disruptive to an orderly routine.
>
> The Winograd Commission Report, p. 54

Lt. Col. (ret.) Dudi Alon served as head of the joint doctrine branch in the IDF Doctrine and Training Division.

Military and Strategic Affairs | Volume 5 | No. 2 | September 2013

## Introduction

It is impossible to overstate the importance of the decision making process for the military leader tasked with fulfilling a mission imposed on him by the political echelon. The quality of the decision making process among the upper command levels is among the factors determining the army's success in attaining the desired political goals, and some claim it is even more important than the combat itself.[1] Similarly, more than anything else, history tends to associate successes and failures with the quality of the situation assessment and the decisions made by the military commander in preparation for operations and in their execution.

Is military leadership an art or is it an orderly, organized analytical process? Is it the result of brilliance and intuition or of calculated, logical deduction? Or is it a combination of these and other factors? What are the major obstacles in the attempt to provide a process to guide military decision making using an orderly format so that the commander and the members of his staff can make decisions in an effective, harmonious, synchronized way? This essay examines the prevalent theoretical approaches to decision making and, with that as background, surveys practical models deemed appropriate to the military setting. The essay discusses and compares the relative advantages and disadvantages of each model, and then makes recommendations about their application to the military decision making process.

## The Essence of the Doctrine in Planning Military Operations

The key issues a commander and his staff face when planning operations are decisions regarding definition of the operation and definition of the method to execute it. To make these decisions, the command must understand the intention and goals of the upper echelon regarding the specific operation. While there are concomitant secondary processes, the core of the planning and its major outcomes lies in defining the task and the way to accomplish it.[2]

The mission is defined by the commander on the basis of a command or directive from the upper echelon or on the basis of his own initiative given his understanding of the situation and the responsibility with which he has been charged. Deciding on how to use force to fulfill a mission is an expression of the commander's military leadership. In order to execute a decision making process the commander must gain an in-depth

understanding of the operational problems and formulate the solutions that will attain the mission's goals in the most efficient and effective way possible.

Military doctrine tries to provide a process of decision making for the planning of operations to generate these two products, that is, definition of the mission and definition of the method, along with other aspects required of the command, from receiving operational tasks from superiors to giving operational tasks to subordinates. The decision making process is usually presented as a model consisting of steps and outcomes. A direct continuation of the decision making process during planning is the operational command and control process, but that is beyond the scope of this essay.

## Theoretical Approaches

One may divide the many models in this field into two major currents and approaches.

a. *The rational-philosophical current*[3] relies on logic as its primary tool, i.e., calling for as good an analytical assessment as possible of the strengths, weaknesses, opportunities, and risks. The rational current perceives the decision making process as a logical analysis in order to identify the optimal alternative for action.
b. *The cognitive-psychological current* relies on all cognitive processes of the human mind – analytical reasoning alongside intuition-based thought. This current sees the decision making process as bringing the military leader to an awareness or sudden insight about the desired method of operation. The tools at work are cognitive, designed to create the natural conditions for the "eureka moment" while avoiding the pitfalls of human reasoning in general and reasoning under pressure in particular.

As yet neither current is fully grounded in comprehensively articulated theories, but research efforts are being invested in both.

### *Rational Approach Models*

The most popular models provide a series of sequential steps of analytical thought in which alternatives are weighed according to their advantages and drawbacks. In the simplest terms, these models expand on three basic steps: analysis of the problem in light of the worldview of the decision maker; proposal of possible solutions and choice of the most effective

alternative by means of analytical thought; and implementation.[4] One of the simplest models outlines the following steps:

a. Define the situation and the desirable outcome.
b. Suggest possible solutions.
c. Compare and assess the alternatives.
d. Choose an alternative.
e. Develop a comprehensive plan.

Other rational models of decision making processes expand on this to a greater or lesser degree. Alongside the model of the process itself, some auxiliary models for helping the decision making process have been developed, such as diagrams of the influential factors and their relationships, SWOT (strengths, weaknesses, opportunities, threats) analyses, decision trees, risk management, scenario simulations, and other emerging tools. Suggesting alternative solutions and comparing them is a typical stage of rational processes. The best alternative is assessed in an analytical, logical process that considers opportunities and risks vis-à-vis success, cost versus benefit, and possible unintended consequences.

Criticism of models of this type contends that it is impossible to examine the entire gamut of possibilities; it is impossible to assess the development of future events; and any such assessment is in any case subjective, requires data that is usually unavailable, and demands an extended period of time. The principles of war are often abstract and in a state of mutual tension (e.g., the need to concentrate force versus the need for security and reserves). At times, one has a good idea of the method of operation that will be chosen already at a very early stage of the decision making process as the result of natural cognitive processes, and weighing other alternatives presents as a tiresome and unnecessary burden.

***Cognitive Approach Models: Recognition-Primed Decision Making***

Other models are based on psychological research underway since the 1980s in recognition-primed decision making, designed to study the way in which professionals, especially in the military, make decisions in practice. The natural way in which people make decisions is as follows: one identifies a problem and looks for a solution; when an intuitive idea rises to the surface of consciousness it is "screened" by thought. If the scenario solves the problem, the solution is adopted; if the solution is assessed as one that will not solve the problem, the individual tries to adjust it. If this

also fails, the solution is abandoned and the next solution is tested using the same method. Ultimately the individual adopts the first solution whose "screening" in the imagination is assessed as solving the problem.

Running the solution in the imagination as if it were a screenplay occurs because of mental patterns that have developed in an individual's mind as a result of previous knowledge and experience. According to this model, there is no comparison among alternatives; rather, the solution is put to a cognitive test in light of the individual's intuition. Individuals who make decisions become experts in their fields thanks to repeated learning, exercises, and experiences in cognitive decision making processes that hone their knowledge and experience, and therefore also sharpen their ability to hit on the right solution intuited in this manner.

On the basis of this theory, a model for recognition-primed decision making includes the following stages:[5]

a. One's superiors have issued instructions or one recognizes on one's own that it is necessary to make a decision.
b. The commander studies the mission and the variables affecting it and affected by it, analyzes the mission, and conceptualizes a method of operation. This is the key stage in the model. What is unique about this model is that all actions occur together. If the commander has confronted similar situations in the past, the process may be rapid. If it is difficult to present only a single method of action, then several alternatives may be proposed, requiring that one of them be chosen.
c. The staff examines and develops a method of action. At this point, the staff may think of a preferred method and must develop it in addition to the method it is examining based on the commander's instructions.
d. A war game is staged. Beyond actual testing, the importance of the war game is the thorough encounter with the enemy's possible methods of action.
e. A plan and/or a command are developed.
f. The model is not unidirectional and it is necessary to go back to previous steps when a tested method of action fails to attain the desired results.

The model combines intuition – a very important tool in choosing the method of action – and a rational process, which is a key tool in testing the effectiveness of a method of action.[6] There is no doubt that the model is effective in situations in which the decision maker has much prior experience in similar situations, has been trained to handle them,

participates in tactical drills, or makes decisions under time and pressure. But much criticism has been leveled at this model. It entails implications for paradigms presented in the previous context of current reality (analogical reasoning) and as a result it is possible that something other than the most appropriate method is chosen to confront the different new reality (fighting the next war with the solutions used to win the previous war).

In his book *War and Strategy*, Yehoshafat Harkabi defines analogical reasoning as a central factor in strategic errors. The assumption that the method of operation that proved itself in the past will still be suitable under different circumstances is motivated by psychological urges making the different and unfamiliar into the seemingly familiar. Such reasoning is grounded in stereotypes and hides behind the slogan of "learning from experience." It focuses on the similarities between the past and the present facing the decision maker. Israel's approach toward Egypt in 1973 is an example of analogical reasoning.[7]

The quality of decision making improves with more previous experience and knowledge, but relying on past experience and prior knowledge can also be the decision maker's undoing. While there is much value in learning the lessons of the past, it would be a mistake to dictate prescriptions of action that were right in a specific context for use in a different context.[8] In *Why Don't We Learn from History?* Liddell Hart wrote: "History has limitations as *guiding* signpost, however, for although it can show us the right direction, it does not give detailed information about the road conditions. But its negative value as a *warning* sign is more definite. History can show us what to *avoid*, even if it does not teach us what to do—by showing the most common mistakes that mankind is apt to make and to repeat."[9]

Current refinements of cognitive models emphasize two major directions designed to overcome the inherent fallacies of cognitive processes. The first is the use of tools encouraging an environment conducive to generating good ideas (brainstorming, war games, and so on). The second is knowledge of the fallacies and traps set by human thought processes for analytical processes in order to find ways to cope with them, such as countering the human tendency to analogical reasoning, which as noted tends to seek similarities and blur differences between the new condition and situations stored in one's bank of experience, or the tendency to make irrational decisions in conditions of uncertainty.[10]

## Contemporary Military Decision Making Models

What follows is a brief overview of two contemporary models applied in military settings that deal with desired decision making processes at the highest echelons of the military commands.

***Standard Procedure: A Rational Process***

The first model is the standard military model presented to all ranks in the familiar literature on offensive doctrine.[11] This rational model includes six basic steps:

a. *Receiving the mission*: Whether it comes from superiors or is the result of the commander's own initiative, the commander must first define the mission. At this point, it is important to attain a very clear understanding of the superiors' intentions and the ramifications for subordinates.
b. *Analyzing the mission*: A situation assessment is constructed in light of the directives of the superiors, previous staff assessments, facts, and assumptions. This assessment includes a formulated mission as well as the factors capable of affecting it and their ramifications. Staff research is carried out as necessary. The situation assessment is not merely a collection of facts, but rather a complete analysis of the possible implications of carrying out the mission.
c. *Developing possible methods of operation*: Based on the situation assessment, several ideas for methods of operation are raised on how to complete the mission.
d. *Evaluating the methods of operation* through war games and analysis.
e. *Deciding on the method of operation*: The possible methods of operation are compared (not one against the other but in terms of their ability to fulfill the mission), and on that basis the method of operation is chosen.
f. *Finalizing the plan and /or command*.

The situation assessment, which starts with the completion of the first step and ends with the choice of the method of operation in the fifth step, is the most critical part of the process and is performed by the commander with the assistance of his staff. Indeed, constructing a situation assessment is part of the definition of the problem. Doctrine stresses and expands on the need for comprehensive data collection, in-depth analysis, and identification of the enemy's weaknesses, all with the commander's direct involvement.

The process of selecting the method of operation in fact entails selecting the solution. Doctrine stresses the application of the doctrine of warfare and its principles, application of the principle of stratagem, analysis of the influential factors from the end to the beginning, analysis of methods of operation from the beginning to the end, and more.

***Commander's Appreciation and Campaign Design: A Cognitive Model***

The commander's appreciation and campaign design (CACD) decision making process was presented systematically to the US military in early 2008 by the Training and Doctrine Command (TRADOC).[12] The cognitive planning process was tested by specifically formulated experiments carried out in 2005-2007 as well as in the field.

Underlying the proposed process is the idea of design as a thought process that precedes planning. Architects design buildings in their imagination while taking into consideration the structures' function, environment, and so on, long before they sit down to draft the actual plans. On the basis of knowledge, experience, and talent, they come up with a unique though general solution to the essence of the building, and only then do they sit down to carve out the spaces, openings, and infrastructures. The model posits a similar function by the military leader: the architect of the current mission sees the mission globally, his vision consisting of the mission as a totality of a core idea and steps before the actual process of planning. The opposite of the design process is the engineering process, a fundamentally more rational process. According to its developers, the design process is more suitable for adopting an approach to complex problems, whereas the engineering process is more suitable to the step at which one takes the products of the design and attempts to turn them into a practical plan. Design is an art, whereas engineering is more scientific in its application. The designer of a new car comes up with a complete model that provides an esthetic and functional solution to the consumers' needs in the environment in which it will be driven; in tandem, engineers will plan the car by breaking the design down into the smallest constituent parts of every subsystem and raw materials that will eventually come together to constitute the whole. In practice, military planners deal both with design and engineering in different proportions depending on the type of the problem. When the problem is very complex, the artistic aspect must

be more dominant in the solution, and more reliance on a design-based approach is required.

According to the proponents of CACD, the classical tools of military design – analyzing the power centers and weaknesses in a search for an operational solution – are better suited to the problems associated with classical clashes between armies but not at all suited to the range of situations of conflict, and certainly not to the confrontations typical of the present and foreseeable future. Therefore, a more design-oriented view is required. According to CACD proponents, current military decision making processes are technical, rational, based on systematic processes, and propelled by the belief that one can rationally optimize methods of action and choose the best one; they are burdened by too many details and are too analytical (since planning is often the work of mid-level staff ranks that are experts in analysis involving many details).

More than ever before, the characteristics of modern warfare require that planners carry out cognitive design functions. It is therefore necessary to adopt systemic patterns of reasoning stressing the whole picture and the synthesis among the details to produce a holistic view of the solution to the problem. The advocates of the approach claim that one of the major problems with commanders at present is their difficulty in defining and describing the operational problem; here too, the more design-oriented process is needed. The main tool in the design of missions is discourse[13] – open, wide-ranging debate that synthesizes ideas and viewpoints by means of competing ideas.

The CACD process is based on the following:

a. *The commander's assessment*, which aims to generate a broad, shared understanding of the operational problem in its widest aspects and in particular to understand the unique context of the problem under discussion. The commander's assessment consists of two non-consecutive sub-stages that are cyclical, integrative, and iterative throughout the greater assessment stage. The first is creation of a framework for the operational problem through an understanding of the strategic context, a synthesis of strategic guidelines, a systemic description of the problem, the identification of trends, the formation of assumptions, and definition of the mission. The second is an analysis of the mission, which entails describing the conditions that must be attained in order to fulfill the strategic guidelines, define the mission's

targets, define the potential links in the system where it can be affected, and change the system's process as desired.

b. *Design of the campaign*, which is the stage of developing the concept in general terms and expressing the main idea of the mission without going into great detail. The purpose is to define how the mission will be accomplished by describing the commander's intention (the "what" and the "why"), describing the general approach (how, where, and who) in terms of stages, organizing the operations in time and space, as well as whatever auxiliary efforts are needed, setting up command and control, and so on.

c. *Development of the plan*. CACD is one of many variations of processes based on a situation analysis according to the doctrine of systems and papers written in the field of the art of design,[14] each one of which has different emphases in the flow of the process.

***The Standard Process vs. CACD***

In the models presented above, different emphases are placed on the way the decision making process occurs, but these differences are not the essential distinctions between the two types. Indeed, many of the emphases in one model may find appropriate expression in the other. For example, the cognitive process also includes the situation assessment and doesn't purport to find the solution only through discourse and reasoning. Conversely, the rational process does not rule out processes of creative thinking, discussion, and competition of ideas, and in fact values them considerably.

One of the tools the cognitive approach emphasizes is the holistic or systemic view, an approach of reasoning that looks at reality in its entirety by examining the sum total of its parts (synthesis). For its part, the systematic view – separation and deconstruction – is suited to the rational approach using analytical reasoning. Here too, this is merely an emphasis and not the essential difference.

CACD stresses original thinking, critical thinking, and creativity at every stage of the process. It does not encourage finding patterns that worked in the past and projecting them onto the present. Rather, it stresses the effort to define what is different about the present on the basis of an in-depth familiarity with the past. The stress to identify the different, singular context of every mission, however, is not exclusive to the cognitive process

and is the essence of the construction of the situation assessment and formulation of conclusions based on factors of influence in the standard process.

It also seems that the call of CACD proponents for a sharp discussion of the operational problem and its solution as well as the approach encouraging competing ideas does not stem from the cognitive nature of the process. These properties are not exclusive to one type or another, but are rather organizational cultural properties that should always be encouraged in organizations irrespective of the decision making process adopted.

In addition, the design notion is not unique to CACD: the standard process developing the optimal method of operation and selection entails a design stage even if it isn't called that. The situation assessment is the design stage in the standard process. The selected method of operation in the standard process is the whole mission as seen in the mind's eye of the commander and the way the mission fulfills the task given influential circumstances. While proponents may see the design process as unique to CACD, the design notion is deeply embedded in developing processes of methods of operation and choosing the final method in the standard process without stressing and analyzing the design-based nature these processes entail.

Rather, the fundamental difference between the approaches lies in the essence of the cognitive versus the rational processes. The cognitive process defines the operational problem and the solution, while stressing recognition-primed, intuitive reasoning in addition to rational thought. Both processes recognize the advantages and limits of intuition and the fallacies and traps of human thinking processes. Yet while the rational process tries to skirt these influences and limitations by imposing rational thought and analytical reasoning, the cognitive process tries to face them head-on and undertake a thought process that encourages intuition through awareness of its pitfalls.

The two approaches are not polar opposites. The cognitive approach cannot be called irrational or a process based only on intuition that writes off analytical reasoning. In this sense, the cognitive approach is much broader, containing the rational aspect of thought. Indeed, the cognitive process uses tools of reasoning: relating to operational problems in their situational contexts; asking what situation needs to be attained; creating a

process of defining the setting and the limits of the problem in order to elicit solutions (framing); recommending thinking outside the box and asking if the problem has been correctly defined and the right questions asked (reframing); using reflective thinking – thinking about thought – while recognizing the traps of thought in analytical processes and avoiding them (such as natural distortions in risk assessments or the natural tendency to think analogically).

The rational process is based on a quantified comparison, if only in a qualified way, between cost, utility, and risk, and on finding the most effective method of operation. The process encourages systematic thinking and an analysis of alternatives, an analysis of the criteria of what constitutes success and failure, and an examination of every method of operation in light of these criteria and the chances for success.

The very deep and real divide between the approaches may be demonstrated using some examples. In the IDF staff manual of 1956, in a paragraph on methods of reasoning, the rationalist approach had the following to say about intuition: "Of course, intuition is nothing but a completely personal and subjective matter, something that one senses. It can only be tested in hindsight, in light of the results. It is therefore not a doctrine that can be taught."[15] In other words, intuition may enter decision making processes, but it is impossible to teach anyone how to elicit intuition. Rationalists do not deny that intuition is used in decision making and do not try to oust it from the process, but their way of incorporating it is by choosing commanders who have proved themselves to have good intuition and train them for leadership. By contrast, the cognitivists encourage the use of intuition based on solid knowledge and experience that meet the test of orderly critique, and is not assimilated in unquestioned fashion. General Charles Krulak, commander of the US Marine Corps in 1995-1999, expressed this approach in the conclusion to his essay "Cultivating Intuitive Decision Making": "Advances in information technology will never clear Clausewitz's 'fog of war' to the point where the analytical model is timely enough to guarantee victory. Marine Corps leaders, therefore, need to develop confidence in their own intuition – an intuition rooted firmly in solid character."[16]

Thus while the two processes recognize that excellence in military leadership is an expression of the artistry and professionalism of the leader, there is a difference in the emphases placed in order to lead, with

the cognitive process stressing the nurturing of thought processes that help manifest this excellence (such as discourse) and the rational process stressing the application of the principles of planning proven by past experience, such as principles of mission planning reflecting simultaneity, depth, timing, rhythm, and many other factors. Neither approach rules out the principles of the other approach; the difference is only one of emphasis. Moreover, the cognitive process will stress the development of the commander based on the understanding that the solution in battle builds on his personal capabilities, the extensive knowledge he has amassed (knowledge of the principle of warfare doctrine, military history, analysis of battles, and other knowledge required by a professional soldier of his rank), and the extensive experience he has gathered in missions, training, simulations, war games, and so on. In contrast, the rational-analytical process stresses the development of tools, concepts, and methods, i.e., if we outline the right method and construct clear tools for the commander, and uniquely conceptualize the problem and solution, the outcome will necessarily be better.

## Discussion

The two major approaches to decision making, the rational and the cognitive, place the need to undertake a thorough clarification of the essence of the operational problem given its unique context at the front and center of the planning process and develop the optimal operational solution in light of the conclusions of that clarification process.[17] But the two approaches are still far from comprehensive theories for the application to decision making. While the advocates of the respective approaches in the military establishment tend to distinguish between the processes and even negate the effectiveness and relevance of the competing approach, it would behoove decision making commanders and their staff to draw from the best of both worlds. To do so, it is necessary to overcome two basic, natural obstacles.

The first obstacle consists of debating terminology rather than essence. Each approach seemingly has its own concepts. At the end of the decision making process, the products are meant to answer the same basic questions: what must the military leader achieve and how does he intend to achieve it? Therefore, the debate of whether we should conceptualize the products as a process of situation assessment generating a mission and method,

or as a design-based process generating a commander's assessment and the design of a campaign, or as a strategic planning process leading to operational planning, diverts us from what is actually important. We must avoid the pitfall of debating terminology: while each side in the debate projects a legitimate claim to supremacy, it often imputes flaws in the concepts used by the other. The debate is not over the nature of the final products but over the processes that lead to and generate products in a better way. In every debate over terminology and conceptualizations, it is necessary to question whether the debate is over the essence of the decision making process or is a politically charged, organizational turf war.

The second obstacle lies in the danger of using the tools proposed by either of the approaches to an absurd extreme. An analysis of the methods of operations based on the rational approach must not be carried out by over-analyzing the criteria and testing them and over-quantifying the importance of each one. It cannot be done under the conditions of chaos and uncertainty typical of the battlefield. To the same extent, the tools of the cognitive approach taken from the systems doctrine can be used ad absurdum, such as the attempt to describe reality on the basis of a systemic approach of the knotty texture of influencing factors, sub-factors affecting the whole, and an overloaded system of interrelationships, and in light of this purport to work on the system's weaknesses in order to achieve the desired operational outcome. Another example of taking the cognitive approach to an absurd extreme can be seen in the over-conceptualization and over-abstraction of language before the Second Lebanon War in the name of creative thought.[18]

It is unlikely that the next few years will produce a magic device generating great military strategy. This ability will remain the province of creative human experts in their field. Turning general conceptual ideas into recipes, laden with sub-processes and details, removes the point of an idea that makes sense and transforms it into a wearisome, Sisyphean burden that narrows one's vision. The use of tools must be limited to times when they can be useful, and they should be used deliberately, sparingly, briefly, generally, and in a way that makes it possible to distinguish between what is important and what is not.

A process that combines the two approaches described above and used by the decision maker and a small team of senior officers providing advice when consulted would recognize and act according to the cognitive

approach in order to define the mission and the method of operation. At the same time, the larger staff would use the rational approach anchored by synchronizing meeting points to ensure everyone is on the same page. In general, such junctions would include:

a. First junction – defining the task. After he recieves the government's instructions and clarifies them with the political echelon (as a goal), the commander defines the military mission and imparts it to his staff.
b. Second junction – situation assessment. The commander, with the help of his staff, will determine the situation assessment.
c. Third junction – choosing the method of operation. The commander, with the help of his staff, looks at the alternatives and decides between them.
d. Fourth junction – final selection of the method of operation. The commander selects the method on the basis of staff work, including all the results of analyses and war games applied to the methods of operation.

These junctions are not a doctrinal innovation in situation assessments, and they will be followed by the generally accepted stage of developing a plan. But while the staff operates along the rational model in approaching these junctions, the commander will carry out his work at the same time, using the cognitive approach with the help of a small team of senior officers. In the process, the commander's ideas and conclusions will be introduced and analyzed by rational means by the entire staff. Drawing the general outline at each intersection is a process that is essentially design-based, while the consequent detailed breakdown of analyses, following the design part, complements the planning.

The questions of what must be attained and how it can be attained must accompany every process at every stage and intersection. While stages 1-2 stress the clarification of the problem and stages 3-4 the solution, they must be kept in mind throughout the process and each considered in light of the other.

Appropriate use of "goal" (what must be attained in the context of the political echelon), "mission" (the required military achievement), and "method" (how the army attains it) products will parallel a process producing strategic purpose and staff ideas. There is no importance to the terms used in practice; what matters is that the officers participating in the process understand the process in which they are engaged. It is only

natural that strategic design would dominate the first part of the process, and that later on, thinking would be more systematic when dealing with planning. However, determining the exact point between the two levels or stages is best left to historians and researchers and should not concern officers in charge of design and planning.

Developing cognitive abilities must be a central piece of commander training. This is not a new recommendation, and it must be done by creating a knowledge base of general principles taken from a wealth of past examples, case studies, and specific training in decision making (war games). To this list must be added training in the use of reasoning, awareness of human consciousness, and thought processes, especially as these function under stress. It is necessary to teach commanders all that is known about the functioning of consciousness during decision making, especially under stressful conditions, just as we teach pilots the way that consciousness interprets vision and the optical illusions that may stem from these processes.

## Conclusion

Commanders who are about to make use of the forces at their disposal in order to attain a military objective must make decisions about the optimal method of operation that will achieve that objective. To do so, they must clarify and answer two fundamental questions: What must be achieved? How do we achieve it? Currently, two major approaches, the rational and the cognitive, offer an orderly process that may help military leaders make better decisions. Neither is yet complete. Each approach offers its own set of concepts to attain the chief products of the decision making process. These sets of concepts blur the real differences between the approaches and draw one into a debate that does not deal with essence. In addition, both approaches tend at times to take the tools and the ideas and over-develop them into hobbling, constraining techniques, thereby missing the fruits that could have been reaped with them by a more informed, tempered use of them as ideas.

Whether we like it or not, commanders will use cognitive processes that are not only rational when they make decisions, because that is the nature of thought. Finding a bridge between the approaches that recognizes the advantages and disadvantages of each and makes a temperate, judicious use of the respective tools can allow us to enjoy the best of both worlds.

## Notes

I would like to express my gratitude to Lt. Col. Boaz Zalmanovich for his comments and suggestions on reference material. All responsibility for the contents of the essay, however, is entirely my own.

1 See a debate on the issue in "Victory at the Strategic or the Tactical Level" in Yehoshfat Harkabi, *War and Strategy* (Tel Aviv: Maarachot and the Defense Ministry Publishers, Tel Aviv, 1990), pp. 477-81.

2 In this section, I have tried to avoid using prevalent terms that would be coined differently according to different decision making processes (such as "strategic goal," "objective," and so on).

3 The distinction between the philosophical and the psychological approaches is proposed because the first has been studied and developed in recent years, especially in academic settings of analytical philosophy, and the second has been studied in academic settings of the social sciences.

4 Drawn from John Pollock, "Rational Decision Making in Resource-Bounded Agents," PhilPapers, 2004, http://philpapers.org/rec/POLRDI.

5 Karol Ross, Gary Klein et al., "The Recognition Primed Decision Model," in *Military Review,* July-August 2004, p. 7.

6 Gary Klein, "Naturalistic Decision Making," *Human Factors* 50, no. 3 (2008): 456−60.

7 Harkabi, *War and Strategy*, p. 585.

8 Harkabi, *War and Strategy,* p. 591.

9 B. H. Liddell Hart, *Why Don't We Learn from History?* (New York: Hawthorn Books, 1971); see http://infohost.nmt.edu/~shipman/reading/liddell/c01.html.

10 Prof. Daniel Kahneman and Prof. Vernon L. Smith won the 2002 Nobel Prize for Economic Sciences for having discovered that decision makers tend to act irrationally when they assess the risks and opportunities under stress and ignore statistical rules in favor of their intuition. See Daniel Kahneman and Amos Tversky, "Prospect Theory − An Analysis of Decision under Risk," *Econometrica* 47, no. 2 (1979): 263-91.

11 U.S. Army FM 101-5, Ch V and JP 5.0, Ch IV, http://www.fs.fed.us/fire/doctrine/genesis_and_evolution/source_materials/FM-101-5_staff_organization_and_operations.pdf.

12 TRADOC pamphlet 252-5-500, "Commander's Appreciation and Campaign Design," version 1.0, 2008, http://www.tradoc.army.mil/tpubs/pams/p525-5-500.pdf.

13 The term "discourse" is used in the original US military documents.

14 See, for example, Stefan J. Banach and Alex Ryan, "The Art of Design − a Design Methodology," *Military Review,* March-April 2009, pp. 105-15.

15 Training Branch, Staff Work, 1956, p. 15.

16 Charles C. Krulak, "Cultivating Intuitive Decision Making," *Marine Corps Gazette*, May 1999,

http://www.au.af.mil/au/awc/awcgate/usmc/cultivating_intuitive_d-m.htm.

17 Some would claim (in a well-built theoretical setting) that one must not develop the main debate in clarifying the operational problem, but that one must focus on the method. In my understanding, dealing with both levels does not mean one precludes the other, rather that both are necessary for a proper process of planning.

18 The examples illustrate how to bring a theoretical approach to the brink of absurdity rather than a desire on my part to indicate the weaknesses of the cognitive approach specifically.

# Korea's Wartime Command: Sovereignty, Security, and Independence

**Alon Levkowitz**

This article deals with South Korea's security policy and its strategic relations with the United States. It analyzes Seoul's policy vis-à-vis wartime command over the years, particularly the influences of complex internal and external elements. The article describes how and why the transfer of command in wartime was delayed for many years, and addresses the influences of former South Korean President Roh Moo-hyun, the military forces, the South Korean media, and North Korea in the process.

Keywords: South Korea; North Korea; United States; alliance; joint command; military

## Introduction

The debate concerning the balance between South Korea's dependency on the United States and its aspiration to develop an independent security policy has intensified in the past two decades. An important example of this process can be seen in the negotiations and agreements concerning the transfer of wartime command from the American forces in Korea to Korean hands. This process, which was supposed to occur in 2009, was delayed over the years, and is now due to begin in 2015.

Wartime operational control is important to discuss for various reasons. First, it influences the 686,000 South Korean soldiers and the 28,000 US soldiers stationed in the Korean Peninsula. It also indirectly influences over one million North Korean soldiers. Second, wartime operational control affects the shape and future of the US-South Korea military alliance, and

Dr. Alon Levkowitz specializes in Korean studies. He teaches in the Department of International Relations at Hebrew University and the Asian Program at Bar-Ilan University.

could influence future military relations between Washington and other allies in the region. Third, it is a symbol of South Korean sovereignty, and an indicator of the country's perception of its own security independence in years to come.[1]

The public dispute over the need to decrease dependence on the US and the desired pace of this process involves the Korean political parties and security forces. This dispute reveals two conflicting groups − the "liberal/reformists," who support a more independent policy and call for a rapider transition of incremental security independence, and the "conservatives," who support Korea's continued US-dependent policy with a slower security independence transition that will allow Korea to better prepare itself for the future.

The debate over wartime command not only allows us to analyze these important fault lines in Korea's political and public spheres, but also gives us a better understanding of the dilemma that the "liberal/reformist" camp is confronted with. On the one hand, the camp embraces the deep-rooted belief in the merits of engagement, which has been promoted by the two previous presidents, Kim Dae-jung (1998-2003) and Roh Moo-hyun (2003-2008) since the historic summit of the two Koreas (2000). On the other hand, the camp is also driven by the constant fear of being left without the American security umbrella.

The internal debate concerning wartime command has manifested itself in different political and public realms, involving technical, legal, political, and military arguments. This article will initially outline the wartime command issue, and later elaborate on the connection between wartime command and the broader concept of self-reliance. It will also explore the implications of wartime command issues for the evolving United States-Republic of Korea (US-ROK) relationship, and examine how the latest North Korean provocations influenced the process.

## What is the Wartime Command Issue?

On September 14, 2006, President Roh Moo-hyun and President George W. Bush agreed in principle on deactivating the Combined Force Command (CFC). This new phase provided South Korea more independence in its security relations with the US[2] and allowed both sides to subsequently continue negotiations on the multiple facets of the issue. Although it was Seoul that initiated the call for the change of command, it also requested

to delay the transfer until 2012, when Washington attempted to schedule it for 2009. This time difference was not a technical issue; it demonstrated the differences between Seoul and Washington's concepts of security relations, as well as Seoul's perception of its dependency on the US.

In 2007, when Seoul and Washington agreed to postpone the wartime command to 2012, Secretary of Defense Robert M. Gates said:[3] "We are preparing for a historic transition in 2012, when the Republic of Korea military will take wartime command in the defense of their own country, and US forces will assume a supporting role." In 2012, however, President Lee Myung-bak and President Barack Obama agreed to delay the transition again, this time to 2015.[4] One should understand that the wartime command transfer is a very complex process that includes several components, such as the implementation of the command structure, the change of military plans, updating the deterrence strategy of North Korea, and much more.

The transfer of wartime command to South Korea has been under discussion since the early 1990s. In 2002, South Korea and the US started a round of talks on the issue as part of the discussions regarding the new framework of the ROK-US alliance. The issue originates from the Korean War, when South Korea voluntarily placed the operational control of its military under the American-led UN Command (UNC).[5] Following the war, operational control was handed over to US forces in Korea (USFK) as part of the ROK-US Mutual Security Agreement (MDT). With the creation of the Combined Forces Command (CFC) in 1978,[6] wartime command was placed under the authority of the CFC commander.[7] In 1994, peacetime control of the Korean forces was transferred to South Korean hands, but wartime control still remained under the control of the ROK-US Combined Forces Command, which was led by a four-star US general.[8]

When the Korean War broke out in 1950, the South Korean government had no choice but to be fully dependent on US and UN forces due to its limited military capabilities as it would not be able to win the war and deter another North Korean attack by itself. This attitude affected the South Korean decision to accept US command in the event of war by signing the postwar Mutual Defense Treaty. Indeed, during the Cold War era, the alliance with the US remained the bulwark of South Korea's security.[9]

Despite the end of the Cold War and the geostrategic changes in Northeast Asia, Washington signaled that it still mistrusted Korea's capacity for full independence by granting the South Korean army control

only during peacetime. To Seoul, this meant it would continue to be dependent on the US for its security, leaving its sovereignty incomplete.

One should indeed ask whether the South Korean forces are ready for the change of command, and why South Korea did not prepare itself for the possibility of assuming complete command earlier. The first factor is that of the regional environment: as long as the Cold War and the tension in the Korean Peninsula persisted, the United States and South Korea had no incentive to change their military relations. The second factor is economic: for South Korea, building an independent deterrent force would have been much more expensive than maintaining its relationship with the US. The third factor is psychological: over the last decade, South Korea has sought to develop its own military intelligence and surveillance capabilities as part of its incremental security independence process. It appears, however, that South Korea cannot overcome the fear of independently handling its own security after being dependent on the US for the past 50 years. Important and influential groups in South Korea do not believe the time is right to accept independent security responsibilities, or to pursue full military independence. This does not mean that they object to limiting South Korea's dependency on the US, or to Korea becoming fully independent; they merely prefer to postpone the process until Korea is ready to be less dependent.

It should be noted that until the beginning of the millennium, Washington did not support a more independent South Korean security policy. During the Cold War era, Washington feared that Seoul would be drawn into another Korean conflict. By increasing Seoul's dependency on Washington, it simultaneously increased America's control over Korea.[10] Another example of Washington's constraint on Seoul's security policy can be seen in the range limitations of South Korea's missiles. Washington allowed South Korean missiles to reach up to 180 kilometers until 2011, when the range limit was extended to 800 kilometers, allowing Seoul to better deter North Korea.[11] Seoul was then able to show off a new cruise missile following the North Korean nuclear test in February 2013. South Korea's possession of better deterring missiles it was previously prohibited from having demonstrates an improvement in the US-South Korea deterrence policy.[12]

There are a number of reasons as to why Washington is prepared to relinquish wartime command to the Koreans after refraining from doing

so for many years. From the bilateral perspective, it is important to note that Washington is no longer concerned Seoul will react irrationally, as it did during the Rhee Syngman ("March to the North") and Park Chung-hee presidencies, thereby eliminating its concern that Seoul might be dragged into undesired conflicts.[13] Other important reasons behind Washington's stance on the issue can be found in its geostrategic considerations, which include the reorganization of the US Global Defense Posture[14] and its overall policy of increasing the cost-sharing burden of its allies around the globe. Pyongyang has not been able to invest in its army for the past two decades due to its shrinking economy. The gap created between Pyongyang's army and the current high standard of Seoul's military capabilities has surely also made the decision easier for American decision-makers.

## Wartime Command and the Concept of Self-Reliance

The wartime command issue did not stay in the realm of professional military decision making. Instead, it became a subject for public debate in South Korea as part of President Roh Moo-hyun's promotion of the concept of self-reliance.[15] An example of how President Roh raised the issue is evident in his speech given on August 15, 2003 at the 58th Anniversary of the Korean National Liberation:[16] "During my remaining term in office, I intend to help lay a firm foundation for our armed forces to be fully equipped with self-reliant national defense capabilities within the next 10 years. To this end, the armed forces will solidify the capacity for intelligence and operation planning as well as readjust armaments and the whole national defense system."

South Korea has long been conflicted between its goal of achieving maximum independence as a sovereign country and its security needs, which require continued dependence on the United States.

The subject of South Korea's self-reliance and its ability to independently defend itself was first raised by President Park Chung-hee[17] in the 1960s. It was then reiterated throughout the 1970s after the withdrawal of some US forces from Korea as part of Seoul's response to the Nixon Doctrine,[18] and as well during President Park's response to President Jimmy Carter's plan to withdraw all US ground forces from Korea. When South Korea raised the issue of self-reliance during the Cold War era, it was more a negotiation tactic aimed at winning concessions from the US, but when the issue was raised again by President Roh Moo-hyun, the strategic environment

differed greatly from the one during President Park Chung-hee's era. With the end of the Cold War, the Soviet Union and China, which were North Korea's allies, normalized diplomatic and economic relations with South Korea, and the southern economy far outpaced that of the north.

For many years, the issue of self-reliance was predominantly handled behind closed doors by American and South Korean civilian and military officials.[19] President Roh opened the debate to the public and political spheres, and the issue made headlines on the front pages of South Korean newspapers. As a part of his agenda to transform inter-Korean and ROK-US relations, President Roh acted to change the attitude toward wartime control from a technical security issue to a national symbol of Korea's sovereignty.[20] The issue became a part of the discussions concerning Korea's need to develop self-reliant capabilities. In President Lee Myung-bak's term, the issue of self-reliance continued to be discussed in public,[21] but the media coverage at that point was more limited than in President Roh's term.

President Roh placed special emphasis on the psychological element of Korea's security dependence on the United States. This was manifested in his speech on August 15, 2007, which was given at the 62nd Anniversary of Korea's liberation:[22] "To date, my Administration has made an effort to overcome the nation's psychological dependence on the United States while strengthening its potential for self-reliant defense. Guided by this strategy are the transfer of wartime operational control, redeployment of the US Forces Korea, relocation of Yongsan Garrison, and vigorous progress in implementing the National Defense Reform 2020. Self-reliant defense and the ROK-US alliance must go forward hand in hand. From this day onward, as it has in the past, the ROK-US alliance will grow into even more robust ties based on mutual respect and close cooperation."

According to President Roh's concept, Korea should not just achieve the objective goal of strengthening its military might, but also overcome the subjective disbelief in its own strength and independent capabilities. Achieving this should be done in parallel to the discussions with the US over this issue.

The internal Korean debate regarding the transfer of wartime command to Korean control raised serious questions:[23] What are the implications of the change of command for the Mutual Defense Treaty between Korea

and the US? Will American forces continue to be stationed in Korea, or will they withdraw? Will the US assist South Korea if North Korea invades it after the command change? And what might be the implications of the change of command on the relationship between North and South Korea, and will it decrease the tensions in the Korean Peninsula?

Some of these questions were raised by the opposition to President Roh's policy, who feared that the change of command will prompt Washington to completely withdraw its forces from South Korea. As Representative Park Jin from the Grand National Party (GNP) said:[24] "It is clear that the government's efforts to exercise unilateral authority to control its troops will help undermine the Korea-US alliance and eventually result in the full withdrawal of US troops from the Peninsula." Others sought to impede President Roh's plan by searching for alternative pitfalls in order to delay the command change.

## The Internal Debate

There are many internal debates within South Korea itself regarding the wartime command transfer. Table 1 charts the main issues that are brought up.

### *The Media – Newspapers*

Korean newspapers play an important part in the internal political and social debates, as well as in the discussions on democracy and US-Korea relations.[25] The media is controlled by the "big three" newspapers: *Chosun Ilbo, Dong-A,* and *JoongAng*, which comprise 80 percent of the market and are very conservative. During his presidential campaign, President Roh was not supported by the conservative media. He had to contend with them and circumvent them by reaching his supporters through the internet.[26] While more liberal newspapers such as *Hankyoreh* supported the President's "self-reliant" policy on the wartime command issue, the "big three" criticized it.[27]

*Chosun Ilbo*, for example, harshly criticized President Roh's wartime command issue: "It is becoming clear that we can no longer trust the president and his aides to handle the matter alone... Roh is a minority president struggling with the lowest approval rating ever for a Korean chief executive."[28]

**Table 1: The Arguments for and against the Change of Command under President Roh**

| Issue | Oppose | Support |
|---|---|---|
| Who's who? | Conservative party members and political groups; retired defense ministers; retired high ranking officers; the "big three" newspapers. | The outgoing President Roh; members of President Roh's cabinet; reformist political forces; *Hankyoreh* newspaper. |
| Legality | President Roh lacks legal authority to pursue this policy. | Article 74(1) of the South Korean constitution authorizes this policy. |
| US commitment to Korea | The change of command will weaken Washington's commitment to Seoul. | The change of command will not undermine Washington's commitment to Korea's security. |
| US-Korea alliance | This will be the first phase of the termination of the alliance. | The alliance will become more egalitarian. |
| Complete US withdrawal | This is the first step of a complete withdrawal of US forces from Korea, akin to 1949. | This will not affect the withdrawal of US forces from Korea. |
| Korea's military and intelligence capabilities | Korea does not have sufficient capability to assume command. It will suffer from "intelligence blindness." | The US will continue to support Korea until it develops its own capabilities. |
| Desired pace | Slower. | Faster. |
| North Korea's reaction | Might interpret this in the wrong way. | Will see this as a sign of decrease of tension in the Peninsula. |

This was not the only editorial article that criticized President Roh on the relations with the United States, the wartime command, and his North Korean policy. *JoongAng* also published several articles that coincided with the other two conservative newspapers and disagreed with President Roh on these issues.[29] On the other side of the political spectrum, *Hankyoreh* published articles that supported President Roh's wartime command policy and stressed South Korea's nationalism and its need to become self-reliant.[30] The public debate between the conservative and liberal newspapers demonstrates the ideological gap between both camps on the wartime command issue. This debate reflects the newspapers' attitude on the Seoul-Washington security relations, and South Korean dependency on Washington.

*Legality*

The legal issue was mainly raised by politicians, retired high-ranking military officers, and conservative political parties who questioned President Roh's legal legitimacy to negotiate the transfer of wartime command with the US. Professor Moon Chung-in showed that Article 74 (1) of the Republic of Korea Constitution permits the President to negotiate these issues with the US:[31] "The President is Commander-in-Chief of the Armed Forces under the conditions as prescribed by the Constitution and Law."

The legal objection to President Roh's negotiations with Washington on the command issue was mainly used when the impeachment process against President Roh was held within the constitutional court.[32] Although the foundation of this argument seems somewhat shaky, it can be perceived as a legitimate democratic tool that the opposition parties used in order to impede President Roh's policy. The legal issue was not raised again by the opposition under President Lee Myung-bak's term, who delayed the transfer to 2015. Lee's successor, President Park Geun-hye, will have to pursue and synchronize South Korean forces with US forces in Korea. This synchronizing process, "Strategic Alliance 2015," had begun with the decision to delay the process and to prepare the gradual coordination between the South Korean and US forces.[33] The issues of sovereignty and of the tensions between Seoul and Washington regarding the command transfer, North Korea, and the alliance were set aside under President Lee, although they were originally emphasized during his campaign and through the beginning of his term. Instead, the security cooperation between the US and South Korea took center stage.[34]

*US Commitment to Korea and the US-Korea Alliance*

Will the change of command lead to the end of the alliance with the US, and will it undermine the American commitment to Korea? As Representative Park Jin of the GNP, one of the opponents of President Roh's policy, said:[35] "Roh is gambling with people's lives ... South Korea will become marginal following the hasty command takeover." On the other hand, the President's camp stressed that the change of command is just one element of the alliance with the US. It does not symbolize the termination of the alliance, or a weakening of America's commitment to Korea, but can be seen as another stage in a process that might lead to a changed alliance.

The question concerning Washington's commitment to South Korea's security was raised again under President Lee's term. Washington reaffirmed its security commitment to Seoul in the statement made by US Secretary of Defense Leon Panetta:[36] "The Department of Defense is already drawing up numerous measures to ensure that there is no loss in the South Korea-US joint combat readiness in preparation for the handing over of wartime operational control." The statements made by Panetta and other US officials were aimed at helping Seoul and additional US allies overcome their concerns, and as well as to reiterate that any change in command will not shake the US commitment to South Korea's security.

***Complete US Withdrawal***

The first withdrawal of US forces from Korea in 1947-1949 was a traumatic episode in Korea's modern history. The negotiations concerning the command transfer reignited fear of another US withdrawal, especially among the critics of Roh's policy who interpreted the change of command as the first step in Washington's plans.[37] In response, President Roh said:[38] "After the transfer, Washington could possibly downsize the US Forces Korea (USFK), but the number of American soldiers stationed here is not as important as the quality of their services." President Roh raised the idea of a US force withdrawal from Korea in his presidential election campaign[39] and continued debating the idea in public after his election in 2002.[40] Although the change of command was delayed after President Roh's presidency, his remarks fanned opposition fears that the plan would be implemented. The concern over complete US withdrawal is raised every time Washington reconsiders the change of allocating US forces within Asia, or the transfer of US forces from Asia to Iraq or Afghanistan.

***Military and Intelligence Capabilities***

A group of former South Korean Defense Ministers and retired high-ranking officers asked President Roh to reconsider his plan of accelerating the transfer of wartime command from the US to Korea:[41] "We ask President Roh to take heed of security experts' advice on the matter, not that of `idealists.'" These officials and Ministers questioned the nation's ability to assume wartime control at that time. They argued that South Korean forces would not be ready to assume command by 2009, and called on the

President to postpone the transfer of control to a time when South Korean forces would be better prepared.

One of the security issues that were raised by politicians and military officers was South Korea's dependency on US intelligence and surveillance. As Representative Song Young-sun, from the opposition Grand National Party and a member of the National Defense Committee, said:[42] "Building up capabilities for gathering intelligence, monitoring enemies and intercepting incoming missiles accurately is a prerequisite to South Korea's independent exercise of wartime command." Others questioned South Korea's ability to develop independent intelligence capabilities by the time the command was to be transferred.[43]

The change of command ignited criticism and planted fears as some thought it would lead Korea to "intelligence blindness." In order to overcome this, American and Korean military officers stated that Washington would continue to provide military intelligence to South Korea even after the change of command occurs, and until Korea is able to fill the vacuum with its own independent capabilities. Colonel Kang Yong-hee, the Ministry's spokesman, said:[44] "Working level officials from the two allies have agreed on a set of issues to draw up a final roadmap for the command transfer. The US side agreed to provide its advanced intelligence assets to the Korean military to fill the possible security vacuum in the Korean Peninsula after Seoul assumes a greater role in national defense." President Roh commented on this issue:[45] "Seoul and Washington will continue exchanging intelligence even after the transfer of wartime control. Is there any alliance that does not share intelligence assets?...The United States will continue intelligence gathering activities not only for us but also for its own sake. Washington will not bring down intelligence satellites due to the transfer.''

In the last decade, South Korean defense forces have been pursuing an incremental process of upgrading their intelligence capabilities, which will allow them to have independent intelligence ability. Some of the technologies and equipment that are being used were purchased from Israel.[46]

### *North Korea Reaction*

How will North Korea interpret the change of command? In the past, Seoul opposed Washington's desire to withdraw its forces from Korea, stating

that Pyongyang might interpret this move as an opportunity to launch an attack as it had done prior to the Korean War.[47]

The anticipated North Korean reaction has been assessed differently by the political camps: President Roh, who continued President Kim Dae-jung's Sunshine Policy, estimated that the change of command would reduce tensions in the Korean Peninsula. The conservatives, on the other hand, warned that Pyongyang might interpret this move as weakness, which would escalate tensions in the Peninsula.

The North Korean provocations during President Lee Myung-bak's presidency, such as the sinking of the Cheonan (2010), the Yeonpyeong artillery attack (2010), the missile/satellite launch (2012), and the third nuclear test (2013), led to the strengthening of military cooperation between the US and South Korea.[48] Both states share the same interest to prevent any unintended escalation that might lead to a regional conflict, including the pursuing of the command transfer, a process that might be used by Pyongyang to increase tension within the Korean Peninsula. Pyongyang continues to threaten that if the UN Security Council approves sanctions against it, its third nuclear test of 2013 would not be its last nuclear or long-range missile test.[49] The newly elected South Korean President, Park Geun-hye, will have to work closely with President Obama in order to prevent Pyongyang from dragging the Korean Peninsula to an undesired conflict, following the newly expected provocations.

## Conclusions

The negative reactions regarding President Roh's efforts to accelerate the process of wartime operational control transfer to Korean hands are difficult to explain. These reactions come from substantial sections of the political and military establishments in South Korea. One would expect that the President's concept of self-reliance, backed by the US statement that South Korea is capable of handling wartime operational control, would gain support from Korean political and security forces. The reality, however, is different.

President Roh succeeded in highlighting an important issue – the psychological element of the Korean fear of abandonment – but even his administration got cold feet when it came to setting a date for the transfer of wartime command. Facing fierce criticism of the plan by conservatives, President Roh asked the American administration to extend the transfer's

deadline from 2009 to 2012. President Lee Myung-bak postponed the process to 2015. A close look at both sides of the argument in Korea suggests that the gap between the two camps on these issues is not as wide as their passionate rhetoric suggests. It is more a matter of pace, image, and national aspirations.

Ultimately, the most important effect of this internal debate has been to expose the issue to public scrutiny. The question of South Korean readiness to accept the responsibility for wartime command enables the public to be a part of the process of redefining Korea's self-image and its relationship with the US. Roh's presidency ignited the internal political debate, while President Lee's term pacified the public debate, and improve relations with Washington. In the long run, it is likely that Roh's nationalistic argument concerning self-reliance will sink in and influence public opinion, helping the Korean political and military establishments to move toward security independence. The debate reveals that the change will have to include a close assessment of the objective military capabilities as well as the psychological elements of Korea's ability to stand on its own.

The change of wartime command is a delicate and complicated process. It involves the South Korean political arena, relations between South and North Korea and the United States, consultations between Seoul and Washington, and changes in South Korea's military command and legislation. In the best of circumstances, the Republic of Korea will move forward in an incremental process of achieving its own security independence. This, as always, will depend on Washington's commitment and on the military tension within the Korean Peninsula.

On October 6, 2008, a few months after his election, President Lee Myung-bak's spokesman said that "The Lee administration is determined to reevaluate and complement a 2006 bilateral agreement calling for South Korea to reclaim wartime operational control of its forces from the United States by 2012."[50] This policy led to postpone the command transfer 2015. President Park Geun-hye is expected to maintain the good security relations between Seoul and Washington, which will include the continuation of the wartime command transfer.[51] President Park will have to balance between her promises to strengthen the alliance with Washington, engage North Korea, and deter Pyongyang from creating further provocations.[52] In addition, President Park will perhaps have to readjust the balance between her three promises if Pyongyang's military provocations continue.

## Notes

1 Weimin Wang and Xin Hua, "Redefinition of the ROK-US Alliance and Implications for Sino-ROK Relations: A Chinese Perspective," *The Korean Journal of Defense Analysis* 24, no. 3 (2012): 289.

2 Yong-ok Park, "Post-CFC Korean Security: Key Issues and Suggestions," *The Korean Journal of Defense Analysis* 19, no. 2 (2007): 6.

3 Robert M. Gates, "Speech at Sophia University" (Speech, Tokyo, Japan, November 09, 2007), http://www.defenselink.mil/speeches/speech.aspx?speechid= 1192.

4 Eun-jung Kim, "S. Korea, US Reaffirm 2015 Deadline for Wartime Operational Control Transition," *Yonhap*, October 23, 2012.

5 Kyung-young Chung, "An Analysis of ROK-US military command relationship from the Korean War to the Present" (MA thesis, Fort Leavenworth, Kansas, 1989); Sung-ki Jung, "Korea-US Alliance Will Grow Stronger," *The Korea Times*, November 14, 2007.

6 Robert G. Rich, *US Ground Force Withdrawal from Korea: A Case Study in National Security Decision Making* (Washington, D.C.: Foreign Service Institute, 1982), p. 18.

7 Du-hyeogn Cha, "ROK-US Command Relations Adjustment: Issues and Prospects," *Korean and World Affairs* 30, no.4 (2006): 488.

8 Richard C. Bush, III, and Bruce E. Bechtol, Jr., "Change of US-ROK Wartime Operational Command," *The Brookings Institution,* September 14, 2006, http://www.brookings.edu/research/articles/2006/09/14southkorea-richard-c-bush-iii.

9 Robert D. Blackwill and Paul Dibb, eds., *America's Asian Alliances* (Cambridge: The MIT Press, 2000); Joon-seung Lee, "US-South Korean Military Alliance and Security on the Korean Peninsula" (MA thesis, Yonsei University, 1996.)

10 Stephen S. Walt., *The Origins of Alliances* (Ithaca: Cornell University Press, 1987): ch. 3; In the past, Washington constrained some of Seoul's attempts to develop its independent deterrent capabilities, such as extending the range of its missiles, or developing its own nuclear program. Hyung-A Kim, *Korea's Development under Park Chung Hee* (London: Routledge, 2004), pp. 193-199.

11 K. J. Kwon, "South Korea Says US Agrees to Extend Seoul's Ballistic Missile Range," *CNN,* October 7, 2012, http://edition.cnn.com/2012/10/07/world/asia/south-korea-us-announcement/index.html.

12 Sang-hun Choe, "South Korea Shows Military Muscle in Sparring with North," *The New York Times,* February 14, 2013, http://www.nytimes.com/2013/02/15/world/asia/south-korea-shows-military-muscle.html?_r=0.

13 Yong-pyo Hong, *State Security and Regime Security: President Syngman Rhee and the Insecurity Dilemma in South Korea* (London: St. Martin Press, 2000).

14 Tae-gyun Park, "Backdrop of Debate on the Takeover of Wartime Operational Control," *Korea Focus*, September 28, 2006.

15 Scott Snyder, "A Comparison of the US and ROK National Security Strategies: Implications for Alliance Coordination toward North Korea," in *North Korea: 2005 and Beyond*, eds. Philip W. Yun and Gi Wook Shin (Stanford: Walter A. Shorenstein Asia Pacific Research Center, 2006), ch. 8.

16 President Moo-hyun Roh, "The 58th Anniversary of National Liberation" (Speech, August 15, 2003). http://web.sungshin.ac.kr/~youngho/data/security2/e-Roh-030815.htm

17 Kamiya Fuji, "The Korean Peninsula after Park Chung Hee," *Asian Survey* 20, no. 7 (1980): 744-753; Hyung-A Kim, *Korea's Development under Park Chung Hee*, 97.

18 Taik-young Hamm, "The Self-Reliant National Defense of South Korea and the Future of the US-ROK Alliance," *Nautilus Institute Policy Forum Online*, 08-49A (2006) http://nautilus.org/napsnet/napsnet-policy-forum/the-self-reliant-national-defense-of-south-korea-and-the-future-of-the-u-s-rok-alliance/#axzz2XRz7Ha9e.

19 Yong-ok Park, "Post-CFC Korean Security," p. 8.

20 Ha-jin Hwang, "Just Say No (To Roh)," *The Wall Street Journal,* September 14, 2006.

21 Chi-dong Lee, "S. Korea, US to Delay Wartime Command Transfer, Speed Up FTA," *Yonhap News*, October 26, 2010, http://english.yonhapnews.co.kr/national/2010/06/27/12/0301000000AEN20100627002400315F.HTML.

22 President Moo-hyun Roh "The 62nd Anniversary of the National Liberation of Korea" (Speech, August 15, 2007), http://www.newswire.co.kr/newsRead.php?no=274368.

23 Yong-ok Park, "Post-CFC Korean Security," p. 8-10.

24 Sung-ki Jung, "Ex-Defense Chiefs Oppose President," *The Korea Times*, August 10, 2006.

25 Ki-sung Kwak, *Media and Democratic Transition in South Korea* (New York: Routledge, 2012), ch. 4; Gi Wook Shin, "The Media and the US-ROK Alliance: The South Korean Case," *EAI Working Paper*, no.14 (2011): 6-12.

26 Eui-hang Shin, "Presidential Elections, Internet Politics, and Citizens' Organizations in South Korea," *Development and Society* 34, no.1 (2005): 25-47.

27 Ki-sung Kwak, *Media and Democratic Transition in South Korea*, pp. 78-79.

28 Dae-joong Kim, "Call a Referendum on Wartime Control," *Chosn Ilbo*, August 11, 2006, http://english.chosun.com/site/data/html_dir/2006/08/11/2006081161020.html.

29 Jae-bum Kim, "Give World a Stake in Wartime Command," *JoongAng*, December 4, 2006, http://koreajoongangdaily.joinsmsn.com/news/article/article.aspx?aid=2853041; Myo-ja Ser, "Ex-Military Leaders to Challenge Roh," *JoongAng,* December 25, 2006, http://koreajoongangdaily.joinsmsn.com/news/article/article.aspx?aid=2862877.

30 "Experts Address Misconceptions about OPCOM Transfer," *Hankyoreh*, June 25, 2010, http://english.hani.co.kr/arti/english_edition/e_

national/427466.html; "US-Korea Alliance Needs Sovereignty," *Hankyoreh,* October 25, 2004, http://legacy.www.hani.co.kr/section-001100000/2004/10/001100000200410250651001.html.

31 Chung-in Moon, "Misunderstandings on the Transfer of Wartime Operational Control," *Nautilus Institute Policy Forum Online*, 06-71A (2006) http://nautilus.org/napsnet/napsnet-policy-forum/misunderstandings-on-the-transfer-of-wartime-operational-control/#axzz2XRz7Ha9e.

32 On March 12, 2004, the South Korean National Assembly voted to impeach President Roh. Two months later Roh returned to the Blue House after the decision of the Constitution Court on May 14, 2004 to reject the impeachment.

33 Michael Raska, "RMA Diffusion Paths and Patterns in South Korea's Military Modernization," *The Korean Journal of Defense Analysis* 23, no. 3 (2011): 380.

34 Jongryn Mo, "What does South Korea Want?" *Hoover Policy Review*, 142 (2007); O. Tara, "US-ROK Strategic Alliance 2015," *US-Korea Policy Newsletter* 2, no. 9 (2010).

35 Sung-ki Jung, "Ex-Defense Chiefs Oppose President," *The Korea Times*, August 10, 2006.

36 He-suk Choi, "US Reaffirms Wartime Command Transfer Plans to S. Korea," *The Korea Herald,* July 30, 2012.

37 Alon Levkowitz, "The 7th Withdrawal – Has the US Forces' Journey Back Home from Korea Begun? " *International Relations of the Asia-Pacific* 8, no.2 (2008): 131-148.

38 Song-wu Park, "Korea Can Take Wartime Control Now," *The Korea Times,* August 9, 2006.

39 President Roh was blamed for fanning anti-Americanism before the election as a means to boost his chances.

40 Alon Levkowitz, "The 7th Withdrawal."

41 Sung-ki Jung, "Ex-Defense Chiefs Oppose President."

42 Sung-ki Jung, "Transfer of Wartime Command Premature," *The Korea Times*, July 09, 2006.

43 Sung-ki Jung, "Washington plans to Transfer Wartime Command by 2009," *The Korea Times,* July 19, 2006.

44 Sung-ki Jung, "US to Share Military Intelligence after Command Transfer," *The Korea Times*, August 17, 2006.

45 Song-wu Park, "Korea Can Take Wartime Control Now."

46 Anonymous, "El-Op Delivers South Korean Spy Camera," *Flight International* 167, no. 4967 (January 11-17, 2005): 27.

47 Alon Levkowitz, "The 7th Withdrawal."

48 Tae-seop Bahng, "One Year after the Cheonan Sinking: Wartime Operational Control and the Future of South Korea's Defense," *SERI Quarterly* 4, no. 2 (2011).

49 Rick Wallace and Scott Murdoch, "North Korea Threatens Bigger Nuke Tests," *The Australian,* February 13, 2013, http://www.theaustralian.com.au/news/world/north-korea-faces-backlash-over-nuke-test/story-e6frg6so-1226576535664.

50 Jeong-ju Na, "Lee Wants to Delay Reclaiming Wartime Control from US," *The Korea Times,* October 7, 2008.

51 J.S. Chang, "(LEAD) Park Calls for Upgrading S. Korea's Alliance with US," *Yonhap*, January 16, 2013, http://english.yonhapnews.co.kr/national/2013/01/16/13/0301000000AEN20130116010151315F.HTML.

52 Mark E. Manyin, Mary Beth Nikitin, Emma Chanlett Avery, Ian E. Rinehart, and William H. Cooper, "US-South Korea Relations," *Congressional Research Service,* (February 5, 2013): 1-4.

# Military Contrarianism in Israel: Room for Opposition by the Chief of Staff to Politicians

**Yagil Levy**

This article offers a structural analysis of the relations between the military and the political echelon on the basis of theories concerning the military's bargaining space vis-à-vis the government. It contends that when the military perceives the conduct of politicians as harmful, it has a tendency to resist by demonstrating its independence and attempting to thwart the politicians' will. The form and intensity of the military's opposition is derived from the intersection between the level of perceived harm done to the military and the power relations that exist among the echelons. The military demonstrates over-independence and resistance, and expands its power the more it views the harm done to it as significant and the more politicians who hold executive governmental positions require its "legitimization services" in the face of opposition, or when the military realizes politicians will refrain from restraining it due to a fear of delegitimization by the opposition.

**Keywords:** Professional autonomy; exchange relations; legitimacy; military contrarianism; civil oversight; military restraint

In January 2013, the Israeli public was outraged by a report the state comptroller published on what was known as the Harpaz Affair. A document allegedly forged by Col. (res.) Boaz Harpaz detailed a strategy on how to appoint Major General Yoav Galant, Commander of the Southern Command, as the new Chief of Staff of the Israel Defense Forces (IDF). Those drafting the document were driven by the goal of discrediting Galant

Prof. Yagil Levy is a member of the faculty at the Open University.

and undermining his candidacy. The document was exposed by the media in August 2010 and opened a Pandora's Box of bad relations between Defense Minister Ehud Barak and Chief of Staff Lieutenant General Gabi Ashkenazi.

In examining the affair, the state comptroller found that the chief of staff's bureau had gathered slanderous material on the defense minister and his associates. This was done with the partial knowledge of Chief of Staff Ashkenazi in a manner that was not consistent with the duty to subordinate the military to the political echelon.[1] In a *Haaretz* editorial, it was even stated that "civilian control of the military is the problem at the heart of the crises that has divided Israeli society, the political system, and the media" from the time of David Ben Gurion's dismantling of the Palmach underground organization until today.[2] As explained by Ashkenazi's aide, the chief of staff's bureau attempted to protect the chief of staff and his ability to function in light of the action taken by the defense minister's bureau, which was perceived as impairing the chief of staff's ability to function professionally.[3]

This is, however, not the first time that the chief of staff acted in a contrarian fashion toward the defense minister or the prime minister. The Harpaz Affair then serves as an invitation for a broader analysis of the mode of conflicts between IDF chiefs of staff and the politicians under whom they serve, as well as the methods selected by chiefs of staff to oppose politicians.

This article offers a structural analysis of the relations between the military and the political echelon on the basis of theories concerning the military's bargaining space vis-à-vis the government. I will argue that when the military perceives the conduct of politicians as harmful, it has a tendency to resist by demonstrating its independence and attempting to thwart the politicians' will. The form and intensity of the military's opposition is derived from the intersection between the level of perceived harm done to the military and the power relations that exist among the echelons. The military demonstrates over-independence and resistance and expands its power the more it views the harm done to it as significant and the more politicians who hold executive governmental positions require its "legitimization services." These services are necessary, for example, to support moderate political measures in the face of opposition from the right, military action in the face of opposition from the left, or

when the military realizes politicians will refrain from restraining it due to a fear of delegitimization by the opposition. The chief of staff's mode of contrarian behavior is divided between direct contrarianism—modes of resistance that are relatively strong and open to the public—and indirect contrarianism—a moderate pattern of resistance that frequently seeks tools outside the immediate area of the parties' dispute. The first part of this article will present the theoretical framework, while the second part will illustrate the argument within the Israeli context.

## The Military's Space for Action

One of the main theoretical questions is what leads the military to accept civilian authority, a phenomenon that arose in Europe in the seventeenth century. The most comprehensive structural explanation is provided by the theory of state formation, which asserts that with the appearance of gunpowder and mass conscription the military became dependent on civilian institutions to finance its operations and support recruitment. This dependency was gradually translated into civilian control, as a massive military cannot raise an abundance of resources by itself, and herein lies the conspicuous difference between the modern military and the feudal military. When the military is not dependent on civilian institutions' mobilization of society's resources for its maintenance, the civilian control of the military weakens. This also explains the relative independence of the military in Asian, African, and Latin American countries during the 1950s-1980s, when the military was often directly financed by outside powers and did not need the state institutions to mobilize society's resources for its maintenance.[4]

Oversight of the military can therefore be conceptualized in terms of exchange relations between the military and civilian institutions: the military accepts the subordination and the limitations placed on its autonomy in exchange for resources that are mobilized by civilian state institutions. These resources range from material resources, such as budgets and manpower, to legitimacy resources, that is, mobilizing legitimacy for war and the use of force.[5] It should be emphasized that this is not a formal or explicit exchange relationship in which each party is aware of the assets it is trading. Instead, the exchange relationship is of a structural pattern in which each side's satisfaction with the emerging situation leads it to institutionalize the exchange relationship and expand

it until it is fixed within the civil political culture. As legitimacy resources play a role, politicians may often adopt a military worldview in exchange for the military's acceptance of their authority.[6]

Dissatisfaction of the military with the exchange relations appears when it subjectively perceives these relations as unbalanced. Such dissatisfaction develops in one of the following situations: (1) The military feels that it is not receiving material or legitimacy resources in a manner suited to its tasks; (2) The military's room for autonomous action is constricted by politicians; (3) Political-cultural processes threaten the military's identity or its organizational interests, such as democratization or liberalization, which challenge the militaristic character of society and its status; (4) The military is given tasks in which it is likely not to succeed, and as a result, a doctrinal dispute develops and intensifies as the military's concerns increase regarding its future organizational interests that could be harmed by failure; (5) Politicians do not respect the military leadership personally or institutionally.[7]

A perception of an unbalanced exchange could lead the military to resist political authority in different ways. This resistance can range from a bureaucratic conflict between the military command and the politicians, as often takes place in Western democracies (in the United States, this is known as a "crisis in civil-military relations"), or a military coup, as happened particularly from the 1950s to 1970s in non-democratic societies. This article, however, comes to examine the type of moderate conflicts that characterize democracies like Israel.

Since explicit disobedience is not legitimate in democratic systems, the military can perform certain acts to show its dismay, such as a military figure's resignation due to disagreements with the political echelon's orders, or a failure of the military to carry out orders by means of foot dragging. Another option is to publicly express a position that challenges the politicians' positions or decisions, and to mobilize other forms of support in the attempt to thwart the will of the elected politicians. One of these forms of mobilization is the recruitment of retired senior officers—at the military's initiative, or at the initiative of others but where the military benefits—who speak for those in uniform. Indeed, the military's right to speak out against a policy that it opposes has been subjected to disputes among American scholars and military personnel since the Vietnam War.[8]

The military's dissatisfaction grows the more its dispute with the politicians is doctrinal or organizational and the more this dispute concerns a wide range of military institutions and not just personal relations between military personnel and politicians. The more intense the dispute is, the greater the ability of the military commanders to justify their contrarian behavior.

Whereas the military's motivation to resist its superiors is derived from the perceived level of violation of the exchange relations, the level of the military's opposition is derived from the balance of power among the echelons, and can be assessed by the military's dependency on civilian institutions. High dependency may dictate restraint, but when the civilian institutions have a limited ability to hurt the military's flow of resources or object to its operations, this dependency becomes especially low. This situation occurs when politicians are dependent on the military as well. In other words, a high level of dependency by politicians on the military weakens the dependency of the military on the politicians and increases the military's independence.

Politicians' dependency on the military grows mainly when they need its legitimization services. As C. Wright Mills explained, the politicians bolster their support for or opposition to policies vis-à-vis their political opponents, as well as strengthen public opinion by framing military policies as being "above politics."[9] The military then helps to "sell" the policy that the politicians are seeking to promote, which has clearly been common in the American politics of recent decades.[10] Legitimization services could be necessary in curbing the opposition of "doves" to the use of force (when the military supports restraint), or alternatively, for military restraint in the face of pressures from "hawks" who lobby for a military action.

The importance of these legitimization services increases according to the level of debate concerning the military's mode of deployment, as well as the parties' aspiration to mobilize support. In this situation, the military's opinion will greatly influence policymaking, as it would be used by those politicians it serves against their opponents and provide the military with relatively broad autonomy in executing the policy. In that sense, the more the military attempts to loosen the reins of the political oversight or to disagree publicly with the government's position, the more limited will be the politicians' ability to punish it for deviating from instructions or from the rules of conduct.[11] Accordingly, the less divided the political

elite is on questions concerning the military deployment, the greater is its ability to discipline the military. Under such conditions, the military has a limited ability to maneuver between competing political groups or branches in order to raise the support necessary to advocate against the policy or instructions dictated by the government.[12]

The freedom of operation given to the military is, therefore, an asset in the exchange relationship: freedom of action (professional autonomy) is given to the military in exchange for obedience, as identified in Samuel Huntington's classic work.[13] At times, freedom of action can also be exchanged for the military's refraining from political mobilization that would thwart the will of the elected politicians, or at least reduce the extent of such mobilization if it has already begun.

Similar to the divisions within the political system, the military establishment is divided at times as well. Under these circumstances, the politicians can exploit the internal military divisions by assisting one group to persuade its opponent to bring the military to accept the politicians' position. This situation, for example, helped George W. Bush to convince the military to accept the surge strategy in Iraq in 2007.[14]

The military restraint also increases when the politicians in charge of the military have military experience. In the United States, for example, leaders who lack military experience may be prone to extend the use of force to deal with interstate conflicts that do not represent a substantial threat to national security. Unlike leaders who do have a military background, however, once leaders without previous military experience have deployed the military, they tend to place limitations on the use of force.[15] In other words, a "civilian" leadership finds it more difficult to restrain the use of force, whether the use is demanded by the military or stems from pressures by hawkish groups in the political system. In terms of the exchange relations, political reliance on the military's legitimization services is higher when "civilian" politicians are in office.

In conclusion, the military scope of options for contrarian behavior toward politicians is shaped by the intersection between the military's perception of the intensity of harm caused by the politicians and the balance of power between the military and the civilians. This theoretical framework provides the tools for explaining the IDF chief of staff's repertoire of opposition to the political leadership.

## Military Contrarianism in Israel

### *Background*

The principle of political supervision over the military was consolidated in Israel even before the formal establishment of the state in 1948, with the subordination of the main underground paramilitary organizations to political authority, largely thanks to the development of strong pre-state Jewish institutions. These funded the paramilitary organizations and recruited the human resources (volunteers) needed, thereby establishing the material dependency of the organizations on the political institutions.

In spite of this, however, friction between politicians and generals developed in the state's first years over the delimitation of authority between the military and the state's politicians. Tensions were also evident on the eve of the Six Day War (1967) when disputes over the use of force and the military's deployment arose. However, the civilian control of the military grew much tighter in years to come: The *Basic Law: The Military* (1976) established the military's subordination to the political authority. Concurrently, arrangements were established to limit the military's freedom of operation. Its ability to challenge the politicians whether by initiating a retaliatory action without explicit political approval as occurred in the 1950s, or by exerting heavy pressure to go to war like the "waiting period" of 1967 was gradually reduced.

The 1973 War and, more profoundly, the first Lebanon War (1982) marked a change in the mode of civilian control with the emergence of extra-institutional control mechanisms. Extra-institutional control is action generally taken by non-bureaucratic actors (mainly social movements and interest groups) acting in the public sphere in an attempt to bargain with the military or to restrain it, either directly or through civilian state institutions. Extra-institutional actors monitored various spheres of military activity, such as draft policy (particularly in regard to reserve duty and the service of the ultra-Orthodox and women) or action in the territories (through settler and civil rights organizations).[16] With the increasing involvement of both lawmakers and the Finance Ministry's Budget Department, oversight of the military's financial resources also gradually became stronger. These processes led military researcher Stuart Cohen to argue that the military's was becoming "overly subordinate" to civilian oversight.[17]

Nevertheless, the leeway given to the IDF—like that of any other military operating in a democratic environment—is not only derived from formal

arrangements but is also greatly influenced by the balance of power between the military and the state's civil institutions. This balance dictates rules of conduct in situations where formal rules leave gray areas, influences the formation of new formal rules, and shapes the politicians' room for action in implementing the formal tools for enforcement at their disposal. Even if the politicians are equipped with appropriate formal powers, they will not always make use of these powers to force a policy the military will oppose or is likely to oppose.

In this article's terms, civilian oversight of the IDF depends on an exchange relationship between the military and civil institutions. In this relationship, the military subordinates itself to civilian rule in exchange for the generous resources the state possesses and provides to the military, its superior symbolic status as "the people's military," and its senior partnership in shaping foreign policy, which has gradually been dominated by military modes of thought[18] (including the shaping of diplomatic processes, such as the Oslo Accords, as described below).[19] This exchange relationship has been very influential in shaping the nature of the interaction between the military and the politicians.

As noted in the theoretical section, the military's room for operation is widened to the extent that its dependency on the politicians is lower and their dependence on it is higher. There are a number of measures within this room for action that the military can take in order to influence policy and adopt a contrarian approach toward the politicians when it feels that the exchange relations have been violated, or, more particularly, that the politicians' decisions harm or could harm it. Since the politicians' dependency on the military is mainly for legitimization services, which are needed when the political system is divided on matters of the use of force and the military's deployment, it is appropriate to focus the empirical analysis on the years following the 1973 Yom Kippur War. The period prior to these years from the mid-1950s on (particularly from 1956-1973) was characterized by a relatively general consensus regarding military policy. By virtue of this consensus, starting in the early years of Israel, the arrangements for political control over the military grew tighter. While the division within the political system since 1973 played a key role in shaping the relations between the military and the politicians, it is difficult to identify any significant role played by divisions within the military on which politicians could capitalize for their benefit.

*Direct Contrarianism*

As noted, the military has the ability to demonstrate independence and expand its powers when politicians need its legitimization services. These services are required, for example, for support in moderate diplomatic moves that do not rely on broad legitimacy, such as when the Yitzhak Rabin government presented the Oslo Accords in 1993. The military criticized the Oslo parameters, which were formulated without its input, and which Chief of Staff Ehud Barak, who categorically rejected the approach of interim agreements, described as "Swiss cheese that has many holes."

But the military did not oppose the government publicly, particularly since the process was led by a military authority like Prime Minister and Defense Minister, and the former Chief of Staff, Yitzhak Rabin. As political opposition to Oslo increased and the government's need for the military's legitimization services grew, the military's role in shaping the arrangements gradually expanded. The military then had an important role in legitimizing the process vis-à-vis the right-religious front that opposed it, or at least in mitigating this opposition. Thus, after a short period in which the process was managed by Foreign Ministry personnel, Rabin entrusted the military with the task of implementing the Oslo arrangements and expanded its role to the point that the Oslo arrangements were shaped by the military and took on a military character.[20] The exchange relations were reshaped: the military gave its support to the Oslo arrangements in exchange for its role in shaping the arrangements. Chief of Staff Barak's opposition to the government remained muted and the potential for direct confrontation was eroded.

More thunderous was the opposition of Chief of Staff Shaul Mofaz to the decision by Prime Minister and Defense Minister Ehud Barak in 2000 to withdraw unilaterally from Lebanon, which was a commitment Barak made to voters during his 1999 election campaign. The military expressed its opposition to a unilateral withdrawal, as it considered it to be dangerous and therefore likely to harm its standing as a provider of security in the future, and this opposition leaked out.[21] When the government ordered the military to prepare for the withdrawal, Chief of Staff Mofaz announced publicly that "the military does not choose its missions." This statement, asserted then-Deputy Chief of Staff Major General Uzi Dayan, was a form of defiance, showing that in the event of a failure during the withdrawal processes, the military would place the responsibility for

negative consequences on the politicians.[22] Nevertheless, the chief of staff's ability to oppose the move was limited due to the withdrawal being an election promise made to the general public that overwhelmingly opposed the continuation of Israel's blood-soaked presence in Lebanon. In this case, the politicians were therefore not very dependent on the military's legitimization services.

The politicians' dependency on the military, however, increased around the same time of the withdrawal from Lebanon as the government attempted to advance the signing of a peace agreement with the Palestinian Authority. Unlike the withdrawal from Lebanon, the peace process engendered significant opposition from the right-religious front, and thus the military's legitimization services were extremely important, especially if the talks with the Palestinians led to a politically disputed deal. With the politicians' dependence on the IDF's legitimization services, Mofaz's concerns that he could be exposed to personal risks if he spoke out against the government were probably relatively mild. Although the military did not publicly express opposition to the negotiations with the Palestinians, the politicians' dependency on the military allowed Chief of Staff Mofaz to expand the scope of his indirect opposition to the government in a series of public, independent statements when disagreements between the sides arose in other areas. The most scathing display occurred when Mofaz publicly criticized the government's decision to appoint outgoing Deputy Chief of Staff Major General Uzi Dayan to head the National Security Council at the appointment ceremony itself.[23]

When the Camp David talks with the Palestinians failed and the second intifada erupted in September 2000, Chief of Staff Mofaz was already operating more independently. From the military's point of view, the exchange relations with state institutions had become unbalanced. The trends toward liberalization and demilitarization of the second half of the 1990s forced the military to compete for its identity in a new reality in which it was gradually losing its centrality within Israeli society. The military's resources were reduced with the last cut dictated by Prime Minister Barak upon his departure to the July 2000 Camp David summit. The withdrawal from Lebanon, which ultimately was perceived as a withdrawal under fire because of pressure from civil protests (and especially those staged by the Four Mothers movement), harmed the self-image of the military, and its public image as well. The imbalance of the exchange relations

was potentially exacerbated with the outbreak of the intifada and the consequences of what followed in further undermining the image of the military as failing again to provide security for the community of citizens. This all followed the collapse of the Oslo Accords, of which the military was one of the architects.

As the balance of the exchange had been violated, the military was pushed to defend its status. A perception that the political leadership was harming the military provided Chief of Staff Mofaz with the motivation to adopt contrarian behavior. This motivation intersected with the ability to stretch the boundaries of the permissible in the formal framework that institutionalizes the military's subordination to political authority. The chief of staff recognized that this was a situation where the political echelon was dependent on the military, and that the military and diplomatic moves conducted were guided by a government that had lost its parliamentary majority. This government would later become a transitional one.

Against this background, Mofaz and other military commanders criticized the government's policy of restraint and containment in dealing with the Palestinians' hostilities, stating that it would not calm the situation.[24] At the same time, the government attempted to promote the political track by holding a dialogue on President Clinton's parameters for an agreement with the Palestinians. The government accepted the parameters, but Chief of Staff Mofaz declared that they constituted an existential danger. Then-Foreign Minister Shlomo Ben-Ami viewed this comment as being almost tantamount to a military coup.[25]

The military's independence was demonstrated not only in words. Field commanders were given a great deal of freedom in conducting policy on aggressively suppressing Palestinian uprisings, which frequently deviated from governmental decisions. At times this created a sense that the government, and in particular, Prime Minister and Defense Minister Barak, had lost control of the military.[26] Former Chief of Staff Amnon Lipkin Shahak, who served as a minister in the Barak government, gave voice to Barak's weakness in restraining the military: "Barak knew it could be publicized in the media that he gives the military guidelines that were not to the military's liking. He was very concerned about that. I have no doubt that he feared that such leaks could undermine legitimacy."[27] In this case of violated exchange relations, the politicians avoided punishing the military for its deviations in exchange for the military's partial restraint

and its refraining from mobilizing even more massive support against the politicians, a move that Barak feared from most.

The exchange relations became much more balanced in 2001, when the government of Major General (ret.) Ariel Sharon replaced the Barak government. The transition to a more aggressive policy toward the Palestinian Authority, which reached its peak in Operation Defensive Shield (2002) during which Israel partly re-occupied the West Bank, allowed the military to rehabilitate its status. Sharon's approach was that the military should be allowed victory[28] so its motivation to behave in a contrarian fashion toward the government would be reduced. Furthermore, a right wing government, and in particular, one led by a renowned military figure like Ariel Sharon, was less exposed to pressures of using military force than a left-center government, and had more of an ability to deal with such pressures. The politicians' need for the military's support was, therefore, reduced, and so too, the military's ability to contrarianism. These factors led the military command to experience less friction with the prime minister and minister of defense.

When tensions were present, the Sharon government had more effective tools than its predecessor for disciplining the chief of staff. In October 2001, for example, around the time the cabinet discussed easing the conditions for the Palestinians, the IDF spokesman announced that Chief of Staff Mofaz opposed a military withdrawal from the Hebron region neighborhoods and easing of conditions for the Palestinians, as he believed this would create a security risk. In the cabinet's discussion, the ministers who opposed these moves relied on the opposition of the chief of staff. Prime Minister Sharon, however, did not find it difficult to put an end to these objections by criticizing the chief of staff's statement, which, in Sharon's opinion, spilled over into the realm of politics. Later, the chief of staff was reprimanded by Defense Minister Binyamin Ben Eliezer, and issued a clarification, coordinated with Ben Eliezer, that "he did not object to the cabinet decision...but only advised against it."[29]

But the relatively balanced exchange was again undermined in the following years. During the first few years of the intifada, the military's operations had a broad public support, which rehabilitated its status. Cracks, however, began to develop later, mainly from 2003, as conscientious objection grew, the organization of released conscripts (Breaking the Silence) formed and exposed abuse of Palestinians, and criticism was

voiced regarding the harm caused to Palestinian noncombatants as a result of targeted killings and regarding the IDF presence on the Philadelphi Corridor, which led to many casualties. The erosion of legitimacy at home, along with the fear of the erosion of international legitimacy for IDF operations, gave rise to the disengagement plan, which, according to Dov Weissglass, head of the prime minister's bureau and one of the plan's architects, was greatly influenced by the domestic process.[30]

Chief of Staff Moshe Yaalon viewed the disengagement plan as a security threat. Along with this basic view, he objected to the fact that the political decision was, as he believed, decided on without the military.[31] Having the military take part in decision making processes was one of the assets the government granted it in exchange for its subordination to political authority, which Yoram Peri called the "partnership model" between the military and the politicians.[32] From the perspective of the military, a political move that involves risk like the disengagement has the potential to expose the military to criticism for its inability to provide security, if the risk is realized in the future. From another standpoint, appointing Shaul Mofaz to be the defense minister only a few months after he retired from serving as the chief of staff had the potential to create tension in the relations between the military and the politicians. Minister Mofaz's intervention in allocating troops for the disengagement plan,[33] along with allegations about direct contacts between the prime minister's bureau and military officers, exacerbated the tension between the sides, to the point that Yaalon considered resignation.[34] In this case, the violation of the exchange by means of undermining the military's status, restricting its autonomy, and not considering its professional outlook, paved the way for contrarian conduct by the chief of staff. In this instance, the contrarian conduct took the form of a public statement made by Yaalon against the plan in March 2004, which he said "would give a tail-wind to terrorism."[35] Right wing politicians used this opinion to counter the disengagement.

But the room for opposition by the chief of staff was limited: the move was led by a right wing government headed by military authorities, such as Prime Minister Sharon and Defense Minister and former Chief of Staff Mofaz, and had relatively broad public support. As mentioned previously, the politicians' dependency on the military is generally weaker when a political process has broad legitimacy (even though in this case the dependency increased slightly the more the government moved from

conventional fighting against the Palestinians to a withdrawal). The chief of staff's restraint, therefore, was effective: in the first stage, Yaalon prepared the military for the move, and in the second stage, a year later, the defense minister decided not to extend Yaalon's term for a fourth year. In a certain sense, this was a dismissal of the chief of staff, and the task of leading the disengagement was given to Yaalon's successor, Dan Haloutz.

In circumstances such as these, the military can be restrained, even without an exchange in the form of partnership in decision making. Similarly, the right wing Menachem Begin government that led the peace process with Egypt during the years 1977-1978, backed by a broad consensus even though it involved many concessions but did not include the military in the political management of the process. In this case, even if the military had reservations about the process, they remained silenced.[36] It is reasonable to assume that had the center-left Labor government led this process, the politicians' dependency on the military would have been greater, given the powerful opposition of the right, which the military could have leveraged to strengthen its position in the decision making process.

***Indirect Contrarianism***

When the politicians' dependency on the military weakens, the military personnel's ability to adopt contrarian behavior toward the politicians is reduced. In these situations, military officials, and the chief of staff in particular, are restrained, and the ability of the prime minister and the defense minister to discipline the military grows stronger, even at the price of harming what military officials perceive as the military's organizational interests. In such situations, contrarianism is channeled into more indirect means of opposition that may bypass the area of the direct dispute between the military and the politicians.

The years Lieutenant General Moshe Levy was chief of staff under Defense Minister Yitzhak Rabin were characterized by a great deal of restraint by the military. Rabin and Prime Minister Shimon Peres needed the military's support to lead the unilateral withdrawal from Lebanon in 1985, which gave rise to opposition from the right. This opposition was relatively muted, given the inclusion of the right in the national unity government established after the 1984 elections. But following the withdrawal, the dependency of the politicians on the military decreased, especially because the security situation was quiet for several years.

These years were exploited for one of the more significant cuts made to the defense budget, which gradually reshaped the military's economic behavior as it absorbed the cuts. Under these circumstances, the political echelon could only be challenged by indirect contrarianism.

When in late 1986 Defense Minister Rabin decided to appoint Major General Dan Shomron, who was viewed as Levy's adversary in the General Staff, as Levy's successor, Levy was indirectly contrarian. Levy attempted to thwart the appointment, but could not directly challenge the defense minister's decision, since Shomron's appointment was legitimate and opposition to it included only a few senior military officials. Nevertheless, in discussing the appointment with Prime Minister Yitzhak Shamir, Levy argued that Shomron was a homosexual, which in those years could have thwarted an appointment in the IDF as it was still limiting the promotion of homosexuals to sensitive positions. An inquiry even revealed that the chief of staff had allegedly persuaded senior officers to testify on Shomron's sexual orientation.[37] This was a move to foil the politicians' selection of the chief of staff. The response by Deputy Chief of Staff Major General Amir Drori was even harsher: he told the media that the decision to appoint Shomron would cause more damage to the State of Israel than was caused by terrorist organizations. Defense Minister Rabin ordered the chief of staff to dismiss Drori but the latter objected by using legal arguments. Ultimately Drori apologized and the crisis passed.[38]

Chief of Staff Amnon Lipkin Shahak's conduct toward the first Netanyahu government between 1996 and 1998 was also characterized by indirect contrarianism. During this period, relations between the government and the military were particularly tense. Netanyahu, as a right wing politician, perceived the military as part of the old elite he sought to undermine, especially in light of the military's support for the Oslo Accords, with which Lipkin Shahak was identified more than his predecessor, Barak. Beyond the disputes over policy, which to a large extent were mitigated with the mediation of Defense Minister Major General (ret.) Yitzhak Mordechai, criticism of the military was voiced by members of Netanyahu's party and close circle, while military criticism of the prime minister leaked out. The hostility of the government increased the challenge that the Oslo period posed to the military's identity, as noted above.

But beyond these conflicts, relations of mutual dependency developed: the military leveraged the politicians' dependency on it to maintain the

Oslo Accords. IDF commanders thereby provided legitimacy to the government to curtail the left wing opposition, which was backed by the US administration, and objected to Netanyahu's hawkish approach to the Palestinians. In this case, the military successfully restrained Netanyahu so that he was unable to translate political rigidity into military aggression (particularly after the bitter experience of Western Wall Tunnel crisis that generated clashes with Palestinian militias in 1996),[39] and security cooperation with the Palestinian Authority flourished. Still, however, the military was more dependent on a right wing government that was at times hostile to it. This government maintained the political agreement with the Palestinians without advancing it, and was therefore less dependent on the military to legitimize peace moves. In the context of this balance of power, the chief of staff mainly showed restraint after receiving freedom of action in the realm of security relations with the Palestinians. Contrarianism here was reflected in what Yoram Peri called "the democratic putsch"—reserve military officers, including Lipkin Shahak and Mordechai, joining together to establish a centrist party in order to oust Netanyahu. This move led to Barak's election as a prime minister in the 1999 elections.[40]

In similar circumstances, Chief of Staff Gabi Ashkenazi engaged in indirect contrarianism in the Harpaz Affair. Ashkenazi served as chief of staff under the Ehud Olmert government with Ehud Barak serving as Defense Minister. During that time, the centrist government was relatively dependent on the military and needed its legitimization services for its attempts to promote a political process with the Palestinians. At the same time, the government also contended with pressures from the right to react firmly to the firing of rockets and missiles at Israeli civilian communities from Hamas-controlled Gaza. Especially crucial was the cooperation between the sides to contain intense pressure for a deep ground operation in Gaza, which the government was not in a hurry to perform and which Chief of Staff Ashkenazi opposed. Ashkenazi supported the December 2008 Cast Lead operation against Gaza only in circumstances in which it was possible to mobilize domestic and foreign legitimacy for the operation that required significant harm to civilians in Gaza in order to reduce the risk to IDF soldiers.[41]

But the balance of power changed again when the Netanyahu government was formed in 2009. The military's dependence on the politicians increased as the politicians became less dependent on the

military. The right-center government improved its position vis-à-vis the military as its ability to fend off political pressures for a military action exceeded that of the Olmert government and did not need the military to lead the peace process, which was deadlocked at the time. Ehud Barak received the defense portfolio again, and the prime minister's dependency on him for maintaining the government and its international legitimacy gave Barak broad power in conducting military affairs, similar to Rabin's status in the Shamir government between 1986 and 1988. Barak did not have this status in the Olmert government.

At a later point, the government needed the reluctant military to support an Israeli attack on Iran's nuclear facilities, but the military once again blocked military moves, as it had done during Netanyahu's first term. This legitimization service became especially relevant after former security figures, headed by former Mossad Director Meir Dagan, set off a public debate on the matter. This, however, only occurred in 2011, after the retirement of Ashkenazi and the appointment of his successor, Benny Gantz, both of whom are among the proponents of military moderation. In fact, it is possible that in the future (as has been the case in the United States since the 1990s), politicians will need the military in order to give legitimacy to military moves in the face of left-center opposition, and not only for military restraint or territorial concessions in the face of right wing opposition.

Given the new balance of power, Barak had the ability to restrict Chief of Staff Gabi Ashkenazi—along with the motivation to prevent Ashkenazi from leveraging his public popularity into political power. This popularity was achieved by Ashkenazi through his image of the military's rebuilder, particularly after Operation Cast Lead, which improved the military's prestige after the perceived fiasco of the Second Lebanon War (2006). The restraints on the chief of staff then began with the formation of the Netanyahu government in 2009, following two years of good relations between Barak and Ashkenazi.

Whether these moves by the defense minister were legitimate as he acted to impose his authority over the chief of staff, or were a show of force (such as the minister's public attack on IDF Spokesman in February 2012 for his alleged role in publicizing information about the possibility that Ashkenazi's term would be extended for a fifth year), they were interpreted in the chief of staff's bureau as an attempt to harm him and his ability to

function. Colonel Erez Weiner, an aide to Chief of Staff Ashkenazi, stated in a testimony before thestate comptroller that he was determined to "protect the chief of staff and his ability to command the IDF appropriately."[42]

The chief of staff's bureau then acceded to the proposal by Boaz Harpaz, a reserve intelligence officer known to be well-connected in the defense establishment, to collect information on the defense minister's bureau. In May 2010, Harpaz provided Ashkenazi with a document allegedly written by strategic advisers to Major General Yoav Galant presenting a plan to promote Galant's candidacy for chief of staff upon Ashkenazi's retirement while damaging Ashkenazi's image. The chief of staff refrained from undertaking a thorough inquiry or relaying the document to authorized powers, as in his assessment it was prepared by someone close to the defense minister. Several weeks later, the document leaked to the press.[43]

If the balance of power had tilted in favor of the military as in the past, Ashkenazi could have involved the prime minister, but he believed that Netanyahu would give full backing to Barak. As noted, the greater the division in the political system, the greater the ability of the military to maneuver between different parties or branches. In Israel, the division is not only between coalition and opposition, but also between the prime minister and the defense minister, particularly when they are from different parties or rival wings of the ruling party. With a moderate political division however, the military's ability to maneuver was weakened in the Harpaz Affair.

With a different balance of power, Ashkenazi could have also done what his predecessors sometimes did and come out openly against the minister under whom he served, but the chief of staff's weakness pushed him to remain silent. Furthermore, in contrast to Netanyahu's first term, and in spite of the shaky relations between the minister and the chief of staff, the military's status was not damaged. As part of the budgetary framework established after the Second Lebanon War the military's budgets actually increased, the government treated it respectfully, and its public standing improved, as is evident from the increased public confidence in the military. Thus, there was no basis for expanding the interpersonal conflict into an inter-institutional conflict. The chief of staff's aide entered the vacuum that was created, and with mainly passive backing of the chief of staff or at least the latter's knowledge (recorded in the state comptroller's report), worked in indirect ways.

During the time this article was written, Israel's Attorney General ordered a criminal police investigation of Ashkenazi and his aides who are suspected of breach of trust and alleged to have taken actions against their superiors. But the fact that the Former Chief of Staff and his aides turned to actions hidden from the public eye (the investigation is based on the documents and recordings suggesting that Ashkenazi may have been much more involved in the affair than previously thought) indicates that the chief of staff internalized the limits of his power. This was very far from the public shows of strength by former chiefs of staff.

## Conclusion

Even if the principle that the military is subordinated to civilian control is not questioned, in democracies in general and in Israel in particular, tensions between generals and politicians have the potential to weaken political authority. This could be the case when officers demonstrate opposition to politicians in various ways when they feel that the politicians are harming or could harm the military. From their point of view, this is a violation of the exchange relationship that establishes civilian control over the military.

Military commanders have a repertoire of means to challenge the decisions of politicians without risking a flagrant violation of the principle of political authority over the military. The choice of means is derived from the intersection between two factors. The first is the perceived intensity of the violation: the greater the violation, the greater the motivation to demonstrate contrarianism. The second factor is the balance of power between the military and the politicians—the military's ability to demonstrate independence toward the politicians or even to attempt to thwart their will increases as the politicians' need for the military's legitimization services grows. This rule also works in the opposite direction, and the civilian independence, or alternatively, the dependence of military officials on politicians, increases the military's restraint.

This article has presented the repertoire of contrarian methods and their use in recent decades: from chiefs of staff who spoke out publicly against moves by politicians in direct contrarianism (such as Mofaz and Yaalon) to more indirect contrarian behavior (Levy, Lipkin Shahak, and Ashkenazi), and in contrast to situations involving relatively great restraint, which sometimes characterized the same chiefs of staff when there was

a different balance of power vis-à-vis the politicians. Figure 1 illustrates the argument by charting the various cases (the location for each case is in relation to the other and does not necessarily indicate absolute values).

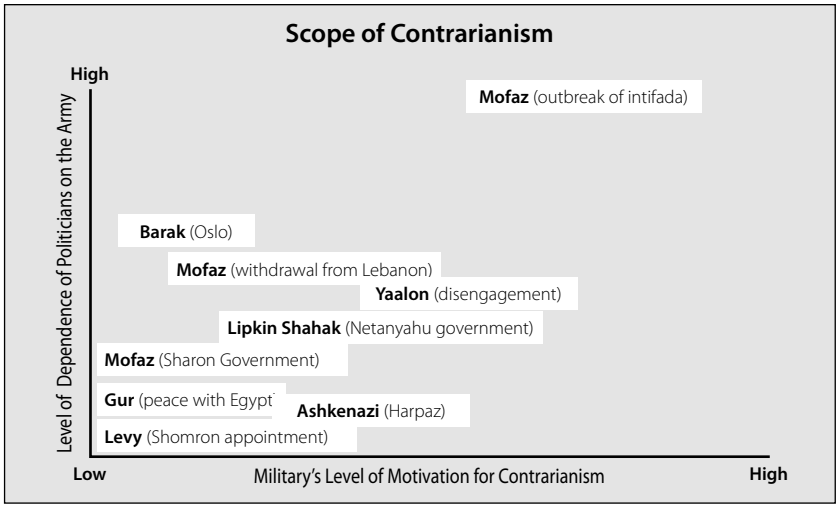


**Figure 1: Instances of Contrarianism**

As shown by the analysis of the above cases, the key for analyzing civilian control is not the "black box" of relations between the military and the politicians in general, or the personal relationships between the actors in particular. Even the formal rules do not exclusively shape the relationship and instead delineate it with coordinates that have been narrowed over the years, but still leave room for conflicts between the military and the politicians. The key to understanding the relationship is the degree of the politicians' ability to mobilize legitimacy for political and military moves. The greater this ability, the less dependent the politicians are on the military's legitimization services and the greater their ability to discipline the military, even if the military feels that its interests are being harmed. This is an important conclusion for anyone who is worried about the excessive power of the military in Israel but is counting on the ability of formal arrangements to regulate this power.

## Notes

1 State Comptroller, *Report on the Harpaz Document Affair*, State Comptroller's Office, Jerusalem, 2013.
2 Editorial in *Haaretz*, "A Criminal Investigation is Needed," *Haaretz*, January 8, 2013, http://www.haaretz.co.il/opinions/editorial-articles/1.1902505.
3 State Comptroller, "Report on the Harpaz Document Affair," p. 32.
4 See in particular Charles Tilly, *Coercion, Capital, and European States, AD 990–1992* (Cambridge, MA: Basil Blackwell, 1992).
5 Yagil Levy, *Who Governs the Military? Between Control of the Military and Control of Militarism* (Jerusalem: Magnes Press, 2010).
6 On this type of exchange see Uri Ben-Eliezer, "Rethinking the Civil-Military Relations Paradigm: The Inverse Relation between Militarism and Praetorianism through the Example of Israel," *Comparative Political Studies* 30, no. 3 (1997): 356-74.
7 For a summary of this approach see Yagil Levy, "A Revised Model of Civilian Control of the Military: The Interaction between the Republican Exchange and the Control Exchange," *Armed Forces and Society* 38, no. 4 (2012): 529-56.
8 See, for example, Martin L. Cook, "Revolt of the Generals: A Case Study in Professional Ethics," *Parameters* No. 38 (2008): 4-5.
9 Wright C. Mills, *The Power Elite* (New York: Oxford University Press, 1956), p. 200.
10 Richard D. Hooker, "Soldiers of the State: Reconsidering American Civil-Military Relations," *Parameters* 33, no. 4 (2003-4): 4-18.
11 Peter D. Feaver, *Armed Servants: Agency, Oversight, and Civil-Military Relations* (Cambridge, MA: Harvard University Press, 2003).
12 Deborah D. Avant, "Are the Reluctant Warriors out of Control? Why the U.S. Military is Averse to Responding to Post-Cold War Low-Level Threats," *Security Studies* 6, no. 2 (1996): 51-90.
13 Samuel P. Huntington, *The Soldier and the State: The Theory and Politics of Civil-Military Relations* (New York: Vintage Books, 1957).
14 Peter D. Feaver, "The Right to Be Right: Civil-Military Relations and the Iraq Surge Decision," *International Security* 35, no. 4 (2011): 87-125.
15 Peter D. Feaver and Christopher Gelpi, *Choosing Your Battles* (Princeton, NJ: Princeton University Press, 2003).
16 Yagil Levy and Kobi Michael, "Conceptualizing Extra-Institutional Control of the Military: Israel as a Case Study," *Res Militaris- European Journal of Military Service* 1, no. 2 (2012, electronic journal).
17 Stuart A. Cohen, "Changing Civil-Military Relations in Israel: Towards an Over-subordinate IDF?" *Israel Affairs* 12, no. 4 (2006): 769-88.
18 Levy, *Who Governs the Military?*
19 Yagil Levy, "Militarizing Peace: Why Did the Israeli Military Spearhead the Oslo Accords?" *Contemporary Politics* 14, no. 2 (2008): 145-59.
20 Ibid.
21 Yoram Peri, *Generals in the Cabinet Room: How the Military Shapes Israeli Policy* (Washington, DC: United States Institute of Peace Press, 2006), pp. 94-5.

22 Uzi Dayan, "The Reality and What is Desirable in Civilian-Military Relations," in *Civil-Military Relations in Israel: Influences and Restraints*, ed. Ram Erez, Memorandum No. 68 (Tel Aviv: Tel Aviv University, Jaffee Center for Strategic Studies, 2003), p. 26.
23 Peri, *Generals in the Cabinet Room*, pp. 103-4.
24 Ibid., pp. 104-5.
25 Shlomo Ben-Ami, *Scars of War, Wounds of Peace: The Israeli-Arab Tragedy* (New York: Oxford University Press, 2006), p. 272.
26 Ben Caspit, "Rosh Hashanah 5763: Two Years of Intifada," *Maariv NRG*, September 5, 2002, http://www.nrg.co.il/online/archive/ART/344/233.html; Peri, *Generals in the Cabinet Room*, pp. 104-7.
27 Interview conducted by Kobi Michael (personal communication with Kobi Michael, 2007).
28 Dov Weissglass, *Arik Sharon: A Personal View* (Tel Aviv: Yediot Books, 2012), pp. 126-28.
29 Linoy Bar Geffen and Attila Somfalvi, "Mofaz: Won't Resign, Sorry about the Crisis," *Ynet*, October 15, 2001, http://www.ynet.co.il/articles/0,7340,L-1197630,00.html.
30 Ari Shavit, "The Big Freeze," *Haaretz.com*, October 8, 2004, http://www.haaretz.com/the-big-freeze-1.136713.
31 Knesset State Comptroller Committee, Protocol No. 195, June 28, 2005.
32 Yoram Peri, *Between Battles and Ballots: Israeli Military in Politics* (New York: Cambridge University Press, 1983).
33 Weissglass, *Arik Sharon*, pp. 223-25.
34 Moshe (Bogie) Yaalon, *The Long Short Road* (Tel Aviv: Yediot Books, 2008), pp. 186-87.
35 Erez Halfon, "Chief of Staff: Evacuation under Fire Won't Solve the Problem," *Ynet*, March 8, 2004, http://www.ynet.co.il/articles/1,7340,L-2885606,00.html.
36 Kobi Michael, *Between Militarism and Statesmanship in Israel: Military Influence on the Transition Processes from War to Peace* (Tel Aviv: Tel Aviv University, The University Institute for Diplomacy and Regional Cooperation, 2008).
37 Amir Oren, "It Could Happen to Anyone," *Haaretz.com*, February 28, 2008, http://www.haaretz.com/general/it-could-happen-to-anyone-1.240317.
38 Amnon Strashnov, "Control of the IDF Judicial System," in *Civil-Military Relations in Israel: Influences and Restraints*, p. 42.
39 Yossi Werter, "His Nightmare Returns," *Haaretz.com*, June 10, 2012, http://www.haaretz.com/weekend/week-s-end/his-nightmare-returns-1.366931.
40 On relations between Lipkin Shahak and the Netanyahu government see Yoram Peri, *Generals in the Cabinet Room*, pp. 77-90.
41 Levy, *Who Governs the Military*? pp. 144-74.
42 State Comptroller, "Report on the Harpaz Document Affair," p. 32.
43 State Comptroller, "Report on the Harpaz Document Affair."

# Who Will Stop the Robots?

## Liran Antebi

Unmanned tools and systems play an increasingly large role in the modern battlefields, as these tools have significant advantages that encourage many countries and violent non-state actors to develop and use them. At the same time, this advanced technology raises moral, ethical, legal, and social concerns and questions. This article explains basic terms in the area of unmanned warfare, examines the developments made in the past twenty years, and presents the United States' future plans in the field. It raises various challenges facing the field, including technological, while making the claim that limiting the field's development will be difficult if not impossible due to the investments made by many countries, the large role unmanned tools and systems already play in today's battlefield, and the field's potential in the context of non-military uses, such as in science, medicine, services, and industry.

**Keywords:** robots; unmanned tools; unmanned airborne vehicles; autonomy; United States; Israel; battlefield; asymmetrical conflict

## Introduction

Unmanned tools and systems play an increasingly large role in the modern battlefields. The United States and Israel, two of the leading countries in the development and usage of these tools, enjoy the reduction of risks to their soldiers' lives and the ability to carry out tasks that cannot be performed by human beings due to physical limitations. Alongside the pursuit of military power, these tools have significant advantages that encourage many countries and violent non-state actors to develop and use them.

This advanced technology also raises moral, ethical, legal, and social concerns and questions. The developing autonomy of these tools and their

Liran Antebi is a Neubauer research fellow at INSS and a PhD student in the Department of Political Science at Tel Aviv University.

ability to act independently without human intervention also raises acute opposition, and has received media coverage, reactions from human rights groups, and governmental responses like the November 2012 US Defense Department directive on autonomous weapons. These reactions indicate that the field is becoming more central in the modern battlefields and is worthy of an in-depth discussion.

This article will review the field of unmanned tools and systems and its development, and examine factors such as the opposition of human rights organizations, or specific decisions taken by governments that could limit the development of the field more so than the technological difficulties it may encounter. The article will explain basic terms in the area of unmanned warfare, examine the developments made in the past twenty years, and present the United States' future plans. It will later raise various challenges facing the field, including technological, while making the claim that in light of the developments and investments made by many countries, limiting the field's development will be difficult if not impossible, both generally and in terms of autonomy. Limitation will also be difficult due to the large role unmanned tools and systems already play in today's battlefield, and also due to the field's potential in the context of non-military uses, such as in science, medicine, services, and industry.

## Unmanned Military Systems

It is difficult to find one accepted definition for unmanned tools. There is also a tendency to confuse unmanned systems or tools with robots and various other types of autonomous tools. A review of current definitions shows an agreement on the idea that unmanned systems are manmade platforms that do not have a human operator but have the ability to carry out repeated tasks, be they mobile or stationary, guided or autonomous.[1] The most up-to-date document from the US Department of Defense, published in November 2012, defines an unmanned platform as "an air, land, surface, subsurface, or space platform that does not have the human operator physically onboard the platform."[2] This is a broad definition that allows for the inclusion of different levels of autonomy.

The platforms are usually capable of transporting a load of materials that were dedicated to the execution of the attack mission such as a camera, bombs, or missiles. However, some of the tools are intended for carrying out missions without a dedicated load, such as an unmanned

ground vehicle with a guided arm for bomb disposal. Missiles, rockets, and artillery are not included in the category of unmanned tools, nor are cyber combat systems.

The field of unmanned systems is highly developed today, and it includes a variety of tools used for executing many missions in different areas of warfare. Especially common in the ground dimension are bomb disposal tools and unmanned vehicles, which are used for patrolling specific areas and transporting loads. The tools in existence today, however, are still limited in their ability to carry out many of the tasks performed by manned combat tools.

Between fifty and eighty countries around the world are developing robots or have already been making operational use of robots in the battlefield. The United States leads in unmanned ground tools' development and usage. In 2010, the ratio of robots to soldiers in the battlefield of Afghanistan was 1:50 (a figure that is expected to increase to 1:30 within a few years),[3] with the total number of unmanned ground tools in America's possession at that time being 12,000.[4] The large majority of such tools are run by a human operator through various control mechanisms. In spite of the fact that their numbers are larger than those of aerial tools, unmanned ground tools are less well-developed than aerial tools. This is mainly because of the technological difficulties, or the difficulties in establishing cooperation between the tools and the soldiers or civilians who move in the same territory. Nevertheless, such tools operate in Israel during fence patrols on the southern border, for example, or by US troops for bomb disposal missions and for relaying images from within buildings.[5]

In the maritime dimension, unmanned tools are used mainly in policing missions. These tools are usually equipped with a camera and various means of navigation, as well as with controlled weapons that can also be installed. Subsurface tools are also operational and carry out diving missions like intercepting enemy ships, sweeping for naval mines, and performing underwater searches. The maritime dimension has its own limitations and difficulties, which its operators and developers try to contend with, such as waves, poor visibility, and loss of contact. Nevertheless, the great potential these tools hold in terms of execution of various maritime tasks that were hitherto the preserve of manned tools (such as maritime policing and patrolling) is close to being fulfilled.[6]

The aerial dimension of unmanned tools is by far the most developed one, being used both in the air and in space. Although US forces had already used them in 1919 to attack a German warship, these aerial tools only became widely operational by the US during the Vietnam War.[7] These tools had excellent intelligence-gathering capabilities thanks to their ability to fly over targets in a low altitude, photograph them, and return to their bases without risking the lives of the crew necessary for flying manned planes. The arming of unmanned aerial tools has gained momentum in the past two decades, as the appropriate technologies matured through the 1990s Revolution in Military Affairs (RMA), and is based on the use of information technologies. American forces are the leaders in the use of unmanned tools, which they employed in operations in Iraq and the currently ongoing operations in Afghanistan, Pakistan, and Yemen.

In Israel, unmanned aerial vehicles (UAVs) entered into operational use in the 1970s, carrying out tasks such as deception, observation, photography, and espionage.[8] The increasing Israeli use of UAVs was clearly demonstrated in the Second Lebanon War, when UAVs logged 15,000 flight hours versus 12,000 flight hours of manned combat aircraft.[9] The missions carried out by UAVs are controlled by human operators, and only some of them have certain autonomous capabilities.

## Autonomous Tools

The word "autonomous" defines the operational independence of the tool or the system. An unmanned platform can be completely non-autonomous. Autonomy is commonly divided into four categories:

- *Platforms controlled by human operators:* The human operator makes all the decisions. The system has no independent control over its environment (for example, a toy car operated by remote control).
- *Platform authorized by human operators:* The platform performs actions independently when it is authorized to execute them by a human operator (for example, robotic vacuum cleaners that by being turned on, receive authorization to wander around the house and clean without outside intervention).
- *Platforms supervised by human operators:* The system can carry out a wide range of actions independently when it receives the approval or instructions from a human operator. Both the human operator and the system can begin an action based on information received from

sensors, but the system can do so only within the range of tasks that it is planned to carry out.

- *Full autonomy:* The system receives targets from human operators and translates them into tasks that will be performed without any human intervention, including the stage of planning and choosing the means of implementation. The human operator can still intervene and influence events when necessary.[10]

The majority of tools used today in the service of modern armies have only a limited degree of autonomy and belong to one of the first three categories mentioned above. American Predator UAVs, for example, are used to attack targets on the ground (as of 2012, particularly in Afghanistan) and to control and supervise the landing, takeoff, and time spent in the air with a high level of autonomy. However, the planning of the mission, identification of the target, and the attack itself are guided and controlled by a human operator in a control room on the ground (usually within the borders of the United States, even when the UAV is in Afghanistan).

Tools that are fully controlled by a human operator have existed and been in use on low levels since the beginning of the twentieth century. Dramatic changes will take place if the technological forecasts come true and the tools themselves will operate in full autonomy, requiring fewer operators than are necessary today. Such a technological change would also lead to a dramatic change in the battlefield.

Another term often heard in the context of unmanned combat is "robot." In order for a tool to be defined as a robot, it must enjoy a level of autonomy that would allow it to operate according to the basic principles of "feel-think-act" and include the following elements that enable it to operate:

- Sensors that monitor the environment and detect changes in it.
- Processors ("artificial intelligence"), which determine the robot's response.
- "Effectors" that operate in a manner representing the decision and create a change in the world surrounding the robot.

When these three parts work together, the robot has the functionality of an artificial organism. A tool that lacks one of these components is not a robot.[11] Even unmanned tools that are composed of simple sensors, processors, and effectors but have a human operating the tool's thought processes do not fit the definition of a robot.

## Tools for Civilian Purposes

This article focuses on the military sphere, but one cannot ignore the civilian dimension, especially because these realms influence one another and their developments are being implemented and are relevant. Unmanned tools, beginning with industrial robots with various levels of autonomy, are becoming more and more common in civilian factories and manufacturing sites. These tools developed from machines, which are associated with the industrial and technological revolution.

Industry, however, is not the sole factor in the revolution of unmanned tools and systems. In recent decades, robots have been adopted in medicine, services, and housework. Medicine is the most prominent of these fields, and even today, many robots are being used in surgeries, wandering independently within the patient's body for medical purposes.

## Advantages of Unmanned Tools

There are three prominent advantages to the usage of unmanned tools. The first advantage is unmanned tools' reduction of risk to soldiers' lives on the battlefield, as their use allows for an increase in the distance between soldiers and the dangers to which they were previously exposed. In such instances, the tools even allow the operator to be removed from the battlefield as in the case of a Predator UAV operator. In the liberal democratic countries that lead the development and usage of unmanned tools, human life is sanctified, and the reduction of risk to soldiers' lives becomes the foremost advantage.

Another advantage of these tools is their miniature size and precision. The multiple yet limited conflicts of the past two decades have been categorized as severely asymmetrical and as creating numerous situations of urban warfare. Current unmanned tools emphasize the asymmetry between modern countries, which make use of advanced technology for combat, and their adversaries, violent non-state actors, which sometimes fight using primitive means against states. The majority of today's unmanned tools are more suitable for achieving the goals of current conflicts as they are more precise and accurate, and are miniature in their size in contrast to tools developed at a time where all-out wars erupted between states. Their usage is helpful in confronting some of the challenges posed by the current type of warfare, and in particular, in reducing collateral damage and harm to non-combatants.

The third advantage of unmanned tools is economic. Though in this point development and procurement are expensive, in the future, the usage of these tools could significantly lower the modern army's maintenance costs. The current savings are reflected in the low cost of some of the tools, which results from the trend toward miniaturization and the availability of technologies. The savings are expected to grow, especially when the technology will allow a large number of tools to be operated by one person, or to become autonomous, saving money on a large number of operators' salaries. Elements of savings in such tools can also be found in cases where the unmanned tool is damaged, for example, as unlike human soldiers, these tools do not have a family that would be supported financially by the state. The trends toward future cost reduction are among those tipping the balance in the direction of a preference for unmanned tools due to the realization that in the long term, this solution will be cheaper than the existing situation.

## Unmanned Tools in the United States: Development and Future Plans

The advantages presented above—among many others—have not escaped the US government, which, in 1999, announced the Future Combat System (FCS) program. The program was due to begin in 2015 and entailed far-reaching reforms to its ground divisions' structure, operation, training, and the replacement of manned tools with unmanned ones. Under it, both manned and unmanned tools were scheduled to operate in the air and on land and communicate among themselves through a unified information system.[12] The program ran into budgetary and deadline difficulties, and, in 2009, it was decided to reduce its scope, specifically in the area of unmanned tools. FCS was then replaced with Brigade Team Combat Management (BTCM), a program that also included a large number of unmanned tools, scheduled to be added to the forces, or to replace manned tools that are scheduled to be removed from use.[13]

The new program is in the implementation stages, but even before its full implementation, unmanned tools are already playing a major role in the battlefield. As noted previously, US forces that are operating in the air and on the ground in conflicts such as in the Middle East are making extensive use of such tools.[14] The mixture of soldiers and robots indicates a dramatic change within a relatively short period of time. Given its future

plans and the existing numbers, there is no doubt that the United States is the leading power in the realm of unmanned tools. In 2001, for example, when the United States entered Afghanistan for the first time, it had a small number of unarmed UAVs, and did not possess unmanned tools for terrestrial use. Approximately ten years later, the United States is making use of more than 8,000 unmanned aerial vehicles.[15]

The change in the United States applies not only to purchasing trends, but also to the mixture in the use of force. Until 2009, the Predator UAVs had racked up 295,000 flight hours, but in 2010, it had already crossed the million flight-hour line.[16] This increase in the Predators flight hours reflects a dramatic change in the use of unmanned tools. Considering that the number of clashes the United States was involved in between 2009 and 2010 did not increase this change, becomes even more significant. Reports written by the Obama administration prior to the November 2012 elections state the government's desire to establish regulations on the killings of terrorists using UAVs. It then becomes evident that this change was not coincidental but rather a result of decision[17] and indicates the importance the administration attributes to these tools and their usage in the war on terrorism.

The preference for unmanned tools is reflected in budgetary terms as well. According to the American roadmap for unmanned systems, a budget of more than 6 billion dollars per annum was allocated for the development of unmanned tools between 2011 and 2015.[18] This is almost 10 percent of about the total US defense annual budget of 70 billion dollar, allocated to research, development, testing, and evaluation.[19]

## Unmanned Tools around the World

The development, production, and assimilation of new technologies require a significant monetary investment, and the United States is surely not working alone in this field. Israel is also a superpower in the area of unmanned systems, which is relatively surprising, given its size and economy. A number of Israeli companies are active in this field, exporting unmanned systems and related services to various countries around the world. In terms of purchasing and procurement, however, a number of other countries are equipped with larger numbers of medium or heavy UAVs, some of which are used in attack missions. Among the countries in possession of dozens of unmanned tools are Great Britain, France, Egypt,

Turkey, and Singapore, as well as other countries that operate an unknown number of such tools.[20]

It is troubling yet not surprising that the development of unmanned tools is also affecting the behavior and efforts of violent non-state organizations, such as Hizbollah and Hamas, which attempt to develop, purchase, and operate unmanned tools. They have had some successes, such as the Hizbollah-operated unmanned aerial vehicle that penetrated the Israeli airspace in October 2012,[21] or attempts made by Hamas, foiled in Operation "Pillar of Defense" in November 2012, to operate UAVs.[22]

Given the availability and accessibility of such technologies, alongside the reduction in price, these first attempts made by non-state organizations are not surprising. Tools and their parts can be easily purchased for a few hundred dollars on various websites or in electronic stores. They are controlled by smartphones, remote controls, or embedded sensors, and are sometimes produced by the same companies that manufacture military robots (such as the American company IRobot). These off-the-shelf technologies can be used by terrorist organizations for violent operations after the appropriate conversion and customization is performed.

From developments in a variety of fields, through budget allocation, to change in operating trends, the change in the field of unmanned tools that has taken place in the past twenty years is significant. Much more development is necessary, however, and the future of the unmanned industry today is equal, according to some researchers, to that of the automobile industry of 1910 or the computer industry of the 1980s.[23]

## The Technological Challenges

The field of unmanned tools is relatively new and therefore still limited technologically in a number of ways. Although a great amount of resources are being allocated to its development, it still faces a number of technological challenges, which make it impossible for unmanned tools to execute the entire range of tasks that are performed by manned tools and soldiers today. This hurts the credibility of unmanned tools and the ability to depend on them, even for the tasks they are qualified to perform. The following are some limitations that create technological challenges for the developers of unmanned tools:

- *Limited visual range:* Unmanned tools are capable of reaching places soldiers cannot due to physical and physiological limitations. The

limitations of their sensors, however, do not allow the range and level of vision and identification that would be possible if a human being was present.

- *Difficulties in ground tasks:* There are two particularly conspicuous problems in ground tasks. The first is the difficulty unmanned tools have in coping with obstacles, particularly negative ones like sharp drops or cliffs, adapting their operation to the environment, identifying and coping with unfamiliar territories, and moving on them. Another problem is the difficulty in cooperation and operating interfaces (communication) between soldiers and unmanned tools and the difficulty in working side by side.
- *Difficulties in subsurface tasks:* Unmanned tools that work underwater are affected by problems such as pressure, and also by turbulence. Problems of communication and poor visibility are also common in maritime tasks.
- *Cyber threats:* A group of students from Texas succeeded in taking over US army UAVs with the minimal investment of less than a thousand dollars.[24] The report on this, alongside reports on other tools that have been taken over, and on information transmission that was intercepted, exemplifies problems of information security. An operational example of this issue can be seen in the claim by Hizbollah that its successful attack on IDF soldiers in the 1997 naval commando disaster (Shayetet 13 Disaster) was made possible by its success in intercepting information transmitted from an unmanned aerial vehicle belonging to the IDF.[25] Beyond the spillover of information to the enemy, the great fear of using unmanned tools is of a hostile takeover by various elements, which would remove the unmanned tools from use, or even turn them against their operators.

In addition to the challenges described above, the ability to invest in development is also influenced by budgetary constraints and the global economy. In addition, the duration of technological development is problematic, as it is sometimes drawn out, making it difficult to meet deadlines. This presents a difficulty, particularly when the tools are intended to replace outdated manned tools that are being removed from use. It would appear that technological challenges can be more easily solved than non-technological challenges.

## Non-Technological Challenges and Lessons from the Past

In addition to technological challenges, other factors affect the development of unmanned tools. As noted above, the countries leading in the development of this field are liberal democracies, and a public discussion about these tools' nature and usage is present. After about ten years in which the United States and Israel have used unmanned tools intensely, particularly aerial tools, we cannot ignore the impact that the partial or full removal of the human factor from the battlefield will make on the nature of the fighting, and, even more so, on the definition of war.

These changes of definitions are evident already. Peter Singer, an expert on military robots argues that the 118 American unmanned attacks carried out in Pakistan until 2010 are not defined as a war. This is particularly interesting as the number of unmanned attacks in Pakistan doubles that of manned bombs carried out in the beginning of the 1990s military operation in Kosovo, which was defined as the start of a war. Singer wonders if this approach is based in the fact that the American operations were conducted by the CIA and not by the military, or perhaps because the American Congress was never asked to vote on them. This could also be the case due to public opinion that does not consider unmanned attacks as events with a cost, or because of the changing definition of war.[26]

The situation indicates that the removal of the human factor from the battlefield could change the conventional terms of war. The reduction in costs and the change in methods of operation could perhaps even indicate that we are on the verge of a paradigm shift, one that will revolutionize military affairs. The main challenge is in adjusting to the new terms and approaches, as well as in acquiring a profound understanding of the advantages and disadvantages of unmanned tools.

In spite of the challenge, various players from both in and out of the United States already understand the change that is taking place. Their arguments concern several aspects such as the slow pace in which international law adjusts to or addresses technological changes as treaties limiting the usage of this new technology have yet to be produced. This results in the possibility various international players such as states and non-state actors have to exploit legal loopholes and operate unmanned tools in ways they are not allowed to do with other tools. Human rights organizations are expressing concern over irresponsible use of unmanned tools as well as regarding future use of completely autonomous tools,

which could harm civilians without there being a human on the battlefield preventing this or held accountable. Various political figures and human rights organizations are calling for the establishment of a treaty that would monitor armed robots.[27] Fears stemming from science fiction speak of an autonomous system that slips out of control and harms its creators or operators, just like in *The Terminator* movies, where an autonomous computer system built for the purpose of protecting the United States goes out of control and attempts to exterminate the human race. The first movie, released in 1984, reflected the fear of computer technology, which was starting to become widespread at that time, but also sparked and inspired current fears of autonomous unmanned tools.

A moral question that is discussed and is also relevant to tools that operate through a remove control is whether robots make killing too easy. The operators of these tools are not physically present on the battlefield risking their lives, but still have the ability to end their enemy's life at the touch of a button, as if playing a computer game. This fear is supported by the large number of attacks and killings in Afghanistan, which also took hundreds of civilians' lives.[28]

The trend of self-defense and distance from the battlefield is not new. A historical review indicates there is a constant trend to develop tools that enable the protection of human beings by their removal from the battlefield while still providing them with the possibility of striking the enemy. As part of this trend, the ranges of weapons increased and the physical strength required for their operations has decreased. In current times, we are moving towards a new level—wars that are carried out by brain power as opposed to brute strength. The previous level of distance and self-defense, took place at the start of the 1990s with the revolution in military affairs, which allowed the use of counter munitions, like precision-guided munitions that could be shot from outside the threat range of surface-to-air missiles.

The US administration has attempted to answer the general public's reservations and concerns. The first, unofficial action of the Obama administration—which, since the 2008 inauguration, approved some 300 UAV attacks, resulting in 2,500 dead, including 153 citizens[29]—was intended to prevent the reservations from affecting the use of unmanned tools. The administration attempted to establish procedures for targeted UAV attacks even before the 2012 presidential elections due to concerns that Obama

would not be reelected. When Obama won the election, the initiative was postponed.[30]

The second action taken by the US administration came in response to the growing public fear of autonomous tools and to actions taken by human rights organizations on this issue. In November 2012, the Department of Defense published a directive declaring that it would not purchase or use manned or unmanned weapons systems that were fully autonomous in any attack mission and that there would always be a human operator involved.[31]

The fact that the administration voluntarily limited itself raises questions. Is this an action that stems from true fears and the desire to avoid unnecessary loss of life, or is it an attempt to silent the media and the public in order to allow for continued development of this field without interference? And is this limitation imposed on autonomous tools by the Department of Defense sufficient? It is difficult to provide unequivocal answers to these questions, but inspiration for this discussion can be drawn from previous restrictions imposed on other types of weapons.

Weapons of mass destruction, which include biological and atomic weapons, were previously limited internationally in their use through the Nuclear Non-Proliferation Treaty (NPT), on which most countries in our world are signed.[32] Nuclear weapons can be compared to unmanned tools as they can both serve for military and civilian purposes (Dual-Use). For example, nuclear technologies also run nuclear power stations, supplying most of the electricity in certain countries.

Autonomous unmanned tools have many possible applications in a range of civilian areas as well. In spite of the restrictions and the supervision on weapons of mass destruction, it has become clear over the last decade that it is very difficult—if not impossible—to prevent a state from developing these types of capabilities if it insists on doing so. We can conclude from this that even if there would be treaties and restrictions on the development and use of autonomous weapons, it would be difficult to stop a country from developing such technologies, especially if the development was done in non-military areas (and later converted into deadly weapons, or alternatively, slipped out of control and became deadly by mistake).

Even today, autonomous unmanned technologies are developed and researched not only for military purposes, but also for various civilian purpose like improvement of transportation, industry, medicine, home appliances, and so on. If the United States or any other country truly aspires

to restrict autonomous unmanned tools, it must first restrict the research and development of these tools in both academic and civilian companies, just as other sensitive scientific fields are restricted, such as genetic engineering. Restrictions are specifically important in the autonomous tools' field as a situation can occur where a fully autonomous humanoid robot with learning capabilities in research or services could turn deadly as a result of error or malicious intent. If this occurs, a robot, unlike a human, is unstoppable. If development of autonomous unmanned tools continued or increased without thought, supervision, control, the risks science fiction presents could become a real and firm reality.

Review of the history of the arming of states shows us that restriction of weapons is not an easy process—when one state achieves capabilities in a ground-breaking field, other countries usually aspire to acquire the same capabilities. In cases of existing conflicts and tensions, it even leads to arms races (such as the nuclear arms race). Lowered cost and availability of unmanned tools have made it easier for violent non-state actors to acquire them, which strengthen the hypothesis that stopping development would be difficult. Eventually, even countries that do not wish to participate in the unmanned arms race will be forced to do so for deterrence and self-defense purposes.

Alongside the fears mentioned above, there is an ethical dilemma as well: the people who operate unmanned tools will be required to make responsible and moral decisions on dilemmas connected to the machine's ability of taking human life with various levels of autonomy. Similar dilemmas will arise regarding any unmanned or autonomous tools that have the ability to make these decisions regarding human life, like the tools currently used in transportation and medicine. These dilemmas, along with legal dilemmas in the political and international realm, are worthy of an in-depth discussion in a separate article.

## Conclusions

Unmanned weapons play a significant role in the twenty-first century battlefield. They have already proven themselves operationally, which leads to increased development attempts and purchasing of tools, particularly among fighting forces of democratic states. This modern trend raises questions in various areas, and the most conspicuous ones are that of moral and legal nature. In recent years, there have been calls demanding

to restrict the development and use of unmanned tools, but despite these moral concerns, the use of unmanned tools has grown considerably.

President Obama led the trend of increased unmanned tools' usage mainly to allow for aerial attacks in the asymmetric conflict between the US and violent non-state actors in Afghanistan, Pakistan, and Yemen. American declarations on restricting the use and purchasing of full autonomous weapons are a response to the calls asking to restrict these weapons. These declarations do not stop the US and other countries from developing this technology for both military and civilian usage.

One can conclude that under the current circumstances it is difficult to restrict unmanned tools, and perhaps there is a lack of desire to do so. Development of these tools will not cease even if some steps are taking to delay it. Though there is certainly a need to supervise and restrict this field, the anticipated difficulty of doing so is great as these weapons are inexpensive, available, and have current and future civilian uses. It is important for decision makers and for the public to be aware of the advantages and the potential inherent in unmanned tools, but also of the risks this field brings with it, which should be addressed in a serious manner.

## Notes

1 U.S. Department of Defense, *Unmanned Systems Integrated Roadmap FY2011-2036*, http://www.defenseinnovationmarketplace.mil/resources/UnmannedSystemsIntegratedRoadmapFY2011.pdf; U.S. Department of Defense, *Unmanned Aircraft Systems Roadmap 2005-2030*, https://www.fas.org/irp/program/collect/uav_roadmap2005.pdf.

2 U.S. Department of Defense, "Directive Number 3000.09," November 21, 2012, http://www.dtic.mil/whs/directives/corres/pdf/300009p.pdf.

3 David Axe, "One in 50 Troops in Afghanistan is a Robot," *WIRED.COM*, July 2, 2011, http://www.wired.com/dangerroom/2011/02/1-in-50-troops-robots.

4 Charles Levinson, "Israeli Robots Remake Battlefield," *The Wall Street Journal*, January 13, 2010, http://online.wsj.com/article/SB126325146524725387.html.

5 Inbal Orpaz, "When Border Fence Is Touched, Robots Can Respond instead of Soldiers," *Ha'aretz*, September 4, 2012, http://technation.themarker.com/hitech/1.1816281.

6 Peter Warren Singer, *Wired for War: The Robotics Revolution and Conflict in the Twenty-First Century* (New York: Penguin Press, 2009), pp. 114-15.

7 Gerald Mies, "Military Robots of the Present and the Future," *AARMS*, vol. 9, no. 1 (2010): 131.

8 On aircraft used by the IDF in recent decades, see the Israel Air Force website, http://www.iaf.org.il/Templates/Aircraft/Aircraft.aspx?lang=HE&lobbyID=69&folderID=83.
9 Yitzhak Ben Israel, *The First Missile War*, position paper, Harold Hartog School of Government and Policy, Tel Aviv University, May 2007, pp. 46-47.
10 US Department of Defense, *Unmanned Systems Integrated Roadmap FY2011-2036*, p. 46.
11 Peter W. Singer, *Wired for War*, p. 67.
12 Hans Ulrich Kaeser, *The Future Combat System: What Future Can the Army Afford?,* CSIS, February 5, 2009, pp. 4-10, http://csis.org/files/media/csis/pubs/090205_fcsarmy.pdf.
13 U.S. Department of Defense, *New Release: Future Combat System (FCS), Program Transitions to Army Brigade Combat Team Modernization*, June 23, 2009, http://www.defense.gov/releases/release.aspx?releaseid=12763.
14 David Axe, "One in 50 Troops in Afghanistan is a Robot."
15 Peter W. Singer, "The Robotics Revolution," *Brookings,* December 11, 2012, http://www.brookings.edu/research/opinions/2012/12/11-robotics-military-singer.
16 "UAV Market: Predator-Series UAVs Reach One Million Flight Hours," *Defense Market*, April 10, 2010, http://www.defensemarket.com/?p=238.
17 Scott Shane, "Election Spurred a Move to Codify U.S. Drone Policy," *New York Times*, November 24, 2012, http://www.nytimes.com/2012/11/25/world/white-house-presses-for-drone-rule-book.html?pagewanted=all.
18 US Department of Defense, *Unmanned Systems Integrated Roadmap FY2011-2036*, p. 13.
19 US Department of Defense, *The Budget for Fiscal Year 2013*, p. 83, *http://www.whitehouse.gov/sites/default/files/omb/budget/fy2013/assets/defense.pdf.*
20 *The Military Balance 2011*, Institute for Strategic Studies, vol. 111, issue 1: The War in Afghanistan; Unmanned Aerial Vehicles: Emerging Lessons and Technologies; Cyberspace: Assessing the Military Dimension, pp. 24-26, http://www.tandfonline.com/doi/abs/10.1080/04597222.2011.559831.
21 Paul Rogers, "Remote Control – A New Way of War," *ISN ETH Zurich*, December 12, 2012, http://isn.ethz.ch/isn/Digital-Library/Special-Feature/Detail?lng=en&id=156055&contextid774=156055&contextid775=156053&tabid=145343154.
22 IDF Spokesman, "UAV Infrastructure Developed by Hamas in Gaza Strip Destroyed," November 16, 2012, http://www.idf.il/1133-17623-he/Dover.aspx.
23 Peter W. Singer, "Unmanned Systems and Robotic Warfare," *Brookings*, March 23, 2010, http://www.brookings.edu/research/testimony/2010/03/23-unmanned-systems-singer.
24 Snejana Farberov, "How a Team of Students HIJACKED a Drone in Midair – All for a $1,000 Bet with U.S. Government," *Daily Mail Online*, June 29, 2012,

http://www.dailymail.co.uk/news/article-2166796/How-team-students-HIJACKED-drone-midair--1-000-bet-U-S-government.html#ixzz2Fzx6ZsD1.

25 Avi Issacharoff and Jacky Khoury, "Nasrallah: We Ambushed Shayetet Soldiers in 1997 Using Drone Photos We Intercepted," *Ha'aretz*, August 10, 2010, http://www.haaretz.co.il/misc/1.1216000.

26 Peter W. Singer, *Unmanned Systems and Robotic Warfare*.

27 International Committee for Robot Arms Control, "Who We Are," http://icrac.net/who/.

28 "March of the Robots," *Economist*, June 2, 2012, http://www.economist.com/node/21556103.

29 Bill Roggio and Alexander Mayer, "Charting the Data for US Airstrikes in Pakistan, 2004- 2013," *The Long War Journal*, http://www.longwarjournal.org/pakistan-strikes.php.

30 Scott Shane, "Election Spurred a Move to Codify U.S. Drone Policy."

31 US Department of Defense, Directive Number 3000.09.

32 United Nations Office for Disarmament Affairs, "Treaty on the Non-Proliferation of Nuclear Weapons (NPT)," http://www.un.org/disarmament/WMD/Nuclear/NPT.shtml.

# The Military Secretary at the Junction of Israel's Security Decisions

**Shmuel Even**

The prime minister's military secretary is an officer with the rank of major general whose official role is to serve as a liaison between the prime minister and the IDF and other security agencies. In practice, his duties are more extensive, and thus his position is one of the most influential ones in the decision making process on security issues in Israel. Nevertheless, the military secretary does not have formal responsibility in the realm of national security, nor does he have a professional staff at his disposal. On certain issues, there is even overlap and a lack of clarity in the division of powers between him and the National Security Staff. In addition, the fact that the military secretary is a major general in the IDF who is subordinate to the prime minister and not to the chief of staff is not self-evident in the structure of government in Israel. This article will analyze the responsibilities of the military secretary, examine differences of opinion regarding the military secretary's realms of activity and his rank, and present recommendations for resolving outstanding issues relevant to the position. It is proposed that the military secretary's activities be limited to the formal description of the position, that the interfaces with the NSS be defined, and that a civilian with extensive security experience be appointed to the position and called the security secretary to the prime minister.

**Keywords:** military secretary; decision making; prime minister; intelligence; security; IDF; National Security Staff; Lipkin Shahak Commission; chief of staff; defense minister; state comptroller; GSS; Mossad

## Introduction

The prime minister's military secretary is an officer with the rank of major general whose job is in part to act as a liaison between the prime minister

Dr. Shmuel Even is a senior research associate at INSS.

and the IDF and other security agencies.[1] By nature, the job of military secretary has relatively little exposure, but there are a number of reasons that it should be in the public eye.

The first reason concerns the weight of the position and its place in the decision making system. According to Prime Minister Benjamin Netanyahu, the military secretary's work lies at the most sensitive decision making point for Israel's security.[2] While there is some overlap between his work and that of the National Security Staff (NSS), the military secretary does not have formal responsibility in the area of national security, and unlike the heads of the defense establishment and the NSS, he has no professional staff. Nonetheless, the military secretary wields much influence over critical decisions on state security that reach the prime minister because of his control of sensitive information, his involvement in preparing the agenda for the prime minister and the cabinet, his direct access to the prime minister, and his senior rank.

The second reason concerns changes that have taken place over time. In recent decades, the complexity of the political-security issues confronting the prime minister, the amount of information received by the prime minister's bureau from various sources, and the challenges of state intelligence organizations, two of which are directly under the auspices of the prime minister, have all increased significantly. The prime minister's small bureau and his advisers, including the military secretary, are not built to handle national security challenges and oversee intelligence organizations. The National Security Staff was established for that purpose, and the NSS has grown much stronger since passage of the National Security Staff Law of 2008. In addition, the Ministry of Intelligence Affairs, which was established in 2009, assists the prime minister on these issues. These agencies are supposed to perform a considerable number of tasks that were the domain of the military secretary and advisers in the prime minister's bureau, while the position of military secretary is supposed to be modified to meet the new situation.

The permanent presence of a major general in uniform in the prime minister's bureau is not a given. This is especially true since the *Basic Law: The Military* of 1976 does not grant the prime minister supreme command authority over the army. The law states that the chief of staff is the "senior command echelon in the army," and it does not recognize a situation in which a major general in the IDF is neither subordinate to the chief of

staff nor required to report to him. Furthermore, the position of military secretary has created a track for promotion of an officer to the rank of major general outside of the IDF though he will likely return to the army's top echelons. While he is selected by the prime minister, he is not always the first choice of the chief of staff and the defense minister, who are responsible for appointments in the army.

There is a disagreement on the definition of the position and its seniority. The conclusion of the Lipkin Shahak Commission[3] and former heads of the defense establishment (including Defense Minister Ehud Barak and Chief of Staff Gabi Ashkenazi)[4] is that there is no place for a military secretary with the rank of major general in the prime minister's bureau. They believe that the position of military secretary is suited to the rank of colonel or brigadier general, whose functions and influence are more limited, as was the accepted practice until 1993. Nevertheless, Prime Minister Netanyahu has made it clear that an officer with the rank of major general is required for the position.[5]

From 2006 to 2012, at least three reports published by the state comptroller on a variety of issues revealed systemic shortcomings connected to the role of military secretary; two were published after the National Security Staff Law was passed. In addition, the Winograd Commission and the Lipkin Shahak Commission reports address the need to resolve the issues related to the position of military secretary.

This article examines the position of military secretary and the source of its power. Among the questions raised: What are the differences of opinion regarding the position? Why have the recommendations of the Lipkin Shahak Commission from 2007 to downgrade the position of military secretary and limit the areas dealt with by the office not been implemented? What is the prime minister's view? The article concludes with recommendations to improve the situation.

## The Role of the Prime Minister in Areas of National Security

The roles filled by the military secretary are derived to a large extent from the prime minister's work on national security. The prime minister is in direct charge of the General Security Services (GSS), the Mossad, the Atomic Energy Commission, the National Security Staff, the National Cyber Staff, and more. However, the prime minister is not officially in charge of the IDF, which is the pillar of the defense establishment. According to the *Basic*

*Law: The Military* of 1976, "the military is subject to the authority of the government," and "the minister in charge of the military on behalf of the government is the defense minister." Unlike the president of the United States, who is defined as the commander in chief of the armed forces, in Israel the government is collectively the commander of the army.

In practice, the prime minister's influence over the military is greater than what the Basic Law stipulates, in part because over the years, norms have been established whereby the prime minister approves important military actions. The situation is also a result of the prime minister's major influence on the agenda and staff work of the Foreign Affairs and Defense Committee[6] and the entire government, where issues relating to security and the IDF frequently come up for discussion. In addition—and this is perhaps the main reason—the prime minister has taken it upon himself to direct some of the main efforts in foreign affairs and defense, including Iran's nuclear program, the political process with the Palestinians, and strategic relations with the United States. All of these require constant strategic and operational staff work.

In January 2007, Prime Minister Netanyahu made some observations about the daily aspects of his job, asserting that decisions about the numerous security-political issues in the State of Israel command the greatest urgency. It is impossible to compare the amount of time and resources that an Israeli prime minister devotes to these issues to the time and resources spent by any other country or politician in the world—in part because in Israel there is no minimal centralized structure or orderly capacity for this. The prime minister spends an enormous amount of time in security briefings that deal with both very important matters and less important matters. In practice, dealing with a low level terrorist translates into something akin to dealing with the Iranian problem. The flow of intelligence is naturally something that one does not want to limit, and if it is not limited, the result is a tremendous cascade of intelligence, which demands an hour or two a day just to review. While both tactical and strategic intelligence is overflowing, the items are actually forwarded to the prime minister without distinction and with very little triage done beforehand, with the final triage done by the military secretary. While he is bombarded with intelligence, the prime minister does not have the benefit of an orderly structure for staff work, which should outline for him the main topics that he must address or on which he and the cabinet must

give their opinion. In addition, he has no tools to determine which issues should be the focus of the government systems.[7]

## The Military Secretary in the Hierarchy

The military secretary is subordinate to the prime minister alone. According to the explanation given by Prime Minister Netanyahu to the state comptroller, "the military secretary's loyalty must be to the prime minister, and therefore, he is chosen by him personally, is subordinate to him, and works according to his instructions." However, he is appointed "in consultation with the minister of defense and the chief of staff as well."[8] Formally, the chief of staff is the person who appoints the military secretary (who has been chosen by the prime minister) and gives him his military rank, but he has no influence over the military secretary.

### *Tasks Performed by the Military Secretary*

a. Contact person for relaying the prime minister's instructions. "The secretary, on behalf of the prime minister, gives directives to the heads of the defense establishment and government offices and holds an ongoing and continuous dialogue with them and monitors the implementation of the directives," as Prime Minister Netanyahu explained to the state comptroller.[9] However, the prime minister and the heads of the defense establishment hold working meetings and direct discussions, and at least some believe that it is not appropriate for their relationship with the prime minister to go through the military secretary, and feel they should have direct contact with the prime minister. In addition, there are those who believe that the military secretary serves as "the super-coordinator for the defense establishment," while he should actually serve "strictly as the military secretary."[10]

b. Sorting information and transmitting it to the prime minister. The information includes intelligence, reports, assessments, recommendations for action, and other material in the political security realm. It comes mainly from the security agencies and the Foreign Ministry, mostly at their initiative, and sometimes at the request of the military secretary. A significant part of the information is sensitive intelligence that requires tremendous capital to obtain, including sometimes a risk to life. In addition, the military secretary conveys

to the prime minister information from meetings he has attended. According to Eitan Haber, who served as the head of the prime minister's bureau under Prime Minister Yitzhak Rabin in the 1990s: "The military secretary to the prime minister is the State of Israel's number one confidant." The military secretary participates in all discussions between the prime minister and the chief of staff, the head of the Mossad, the head of the GSS, the director general of the Atomic Energy Commission, and representatives from the defense industry, and therefore "only the military secretary knows all."[11] Azriel Nevo, who served as military secretary to Prime Ministers Menachem Begin, Yitzhak Shamir, Shimon Peres, and Yitzhak Rabin, noted that "one of the problems of the military secretary is the need not to overburden the prime minister with too much information. He must select material from the large pile and decide what is important and what is not."[12] In other words, the considerations of the military secretary and his deputy in sorting and understanding the information—what is important and what is peripheral—have a great impact on the picture the prime minister sees, and hence also on his decisions.

c. Coordinating the discussions of the prime minister and the cabinet on defense and political issues. This position gives the military secretary tremendous influence through his involvement in setting the agenda and preparing the discussions. The head of the NSS also serves this function, yet according to the state comptroller's report, "most of the prime minister's discussions on issues of foreign affairs and defense were coordinated by the military secretary and not the NSS, which is in accordance with the prime minister's directives."[13] The report also notes that "the military secretary coordinated discussions on subjects important to state security, including discussions of the forum of seven, the Nuclear Non-Proliferation Treaty, and the map of Israel's security interests." The state comptroller explained that the military secretary has no professional staff[14] whose job is to perform ongoing, integrative staff work on issues of foreign affairs and defense and examine the recommendations of the respective institutions, as the NSS is required to do in the discussions it coordinates. This could interfere with a comprehensive view of foreign affairs and defense, the decision making processes in the discussions coordinated by the military secretary, and the organizational memory.[15] Dr. Uzi Arad,

who from 2009 to 2011 served as head of the NSS, has noted that the lack of clarity in the division of tasks between the military secretary and the head of the NSS caused "glitches and conflicts," and it was not always clear, even to institutions in the system, whom to approach on issues relating to discussions underway or proposed deliberations. It thus happened that the NSS and the military secretary scheduled discussions in the prime minister's bureau on the same subject for the same week.[16]

d. In a meeting in July 2011, the prime minister made clear to the state comptroller that the NSS should first of all coordinate cabinet meetings and ministerial meetings on security issues. He noted that the military secretary handles ongoing intelligence and operations and that it is very difficult to define in advance when the operation becomes something that spills over into an issue that must be handled on the level of the NSS. The prime minister also explained that he decides to divide the topics between the military secretary and the NSS, "partly in accordance with 'its [the NSS's] competence in certain areas.'"[17]

e. Consulting for the prime minister on security issues. There is a dispute, or at least a substantial lack of clarity, concerning the status of the military secretary as an adviser to the prime minister.[18] Major General (ret.) Danny Yatom, who served as the military secretary for Prime Ministers Rabin and Peres from 1993 to 1996, thinks that "it is your duty to express your opinion and your position, and we should remember that the military secretary is with the prime minister more than any other aide. There are almost endless opportunities to influence the decision maker in the discussions. In this job, you have a tremendous ability to have an impact."[19] According to the Lipkin Shahak Commission report, it is not the job of the military secretary to advise the prime minister on defense issues, but "over the years, the position has grown, and there were those who saw him as the prime minister's adviser on security."[20] In 2011, the Prime Minister's Office told the state comptroller that "the military secretary does not serve as an adviser to the prime minister."[21] However, among the military secretary's roles noted in the job description is in fact the task of "providing a recommendation to the prime minister on operational issues that require his personal involvement."[22]

f. Representing the prime minister in defense forums. The military secretary participates in General Staff discussions, serves as an observer in the committee of heads of intelligence services,[23] appears before Knesset committees as the prime minister's representative, and more. The military secretary is not obligated to report to state institutions, e.g., Knesset committees, with his security assessments, unlike other office holders, such as the chief of staff and the head of the NSS, who present their surveys and situation assessments.

g. Performing special tasks on behalf of the prime minister. For example, in May 2010, in connection with efforts to persuade the Turkish government to block the flotilla from the area, "the military secretary worked with political and informational officials himself, which included direct interaction with the Foreign Ministry and foreign ambassadors."[24] Uzi Arad, who was head of the NSS at that time and worked on the political aspect of this task, noted that he did not know in real time about this irregular activity by the military secretary on the issue of the flotilla.[25]

## Three Types of Military Secretaries

The job of the military secretary is a one-man show, and therefore his personality and experience and the prime minister's trust in him have a great impact on his powers and contribution. This article does not discuss the contribution of a particular military secretary, but only the nature of the position. In this vein, then, from the time of Israel's establishment until today, there have been three different types of military secretary: an officer with the rank of colonel-brigadier general (a senior staff officer), a major general in his first job (an entry-level major general), and a major general who comes to the position of military secretary after performing other functions as a general in the IDF (a seasoned major general). This typology is supposedly based on the military hierarchy, but in practice, it has ramifications for the nature of the job—how the military secretary is perceived by the prime minister and the defense establishment, and even by the holder of the office himself.

### *The Senior Staff Officer*

This type of military secretary is a staff officer with the rank of brigadier general whose main job is to act as a liaison between the prime minister

and the IDF and other security agencies. The first military secretary was Brigadier General Nehemia Argov. He was first called the prime minister's military adjutant, and in 1950 he was appointed to the position of military secretary to the prime minister.[26] From 1950 to 1993, the officers who served in this position ranged from colonels to brigadier generals, and most were not promoted to command positions in the IDF after serving as military secretary.[27] The prime minister could see such a military secretary as a professional aide, a trusted person who for the most part had no agenda of his own in the army's top leadership. The best known of these was Brigadier General (ret.) Azriel Nevo, who served as military secretary for four prime ministers (1981-1993).

***The Entry-Level Major General***

This is the model of the twenty-first century military secretary, which began during the tenure of Prime Minister Ariel Sharon. Since 2001, six of the seven IDF officers appointed to the position of military secretary have been promoted from the rank of brigadier general to the rank of major general while serving in this position. Most returned to the IDF and continued to perform other duties of a major general.[28] The rank of major general gives the military secretary an elevated status in the military and political system. The choice of an entry-level major general over a seasoned major general could have advantages in terms of his relationship with the Defense Ministry and the IDF, to which he will likely return, and because of his distance from the political system, where the seasoned major general is liable to find himself at the next stage.

Nevertheless, a beginning major general may be at a disadvantage compared to a seasoned major general in terms of prior knowledge and experience regarding the strategic-political level and familiarity with the intelligence community. The gap between the traditional tasks of the military secretary (as described in the senior staff officer model) and the strategic thinking ability and command skills expected of a major general in the IDF could lead the beginning major general to give security-political advice to the prime minister and exert his influence during coordination of complex security-political discussions, even though he does not have a professional staff like that of the defense minister and the head of the NSS. Furthermore, at least in the first part of his term, his knowledge and experience are limited to areas he has dealt with previously, since he has

not had special training for the position. This is significant, since the terms of military secretaries are relatively short (on average about 2.5 years in the past decade), and thus, the time for learning is a significant portion of the period of service of the beginning major general who serves as military secretary.

Because he is in the prime minister's bureau, the entry-level major general could find himself with a conflict of interests: on the one hand, he is an officer who is scheduled to return to the army, and on the other hand, he is a loyal adviser to the prime minister, discreet and professional, who is sometimes required to make difficult decisions, even at the expense of the interests of the army or in opposition to the position of the army. And indeed, there is resistance in the defense establishment to appointing a major general as military secretary, particularly a beginning major general, as will be discussed below.[29]

***Seasoned Major General***

Prime Minister Yitzhak Rabin, who also served as defense minister, was the first to appoint a major general as military secretary. His choice was Major General Danny Yatom, an experienced officer who served from 1993 to 1996. Prior to that, Yatom had served as OC Central Command and as head of the IDF Planning Branch. Experienced major general Zeev Livneh succeeded Yatom, serving from 1996 to 1997 under Prime Minister Netanyahu. Both military secretaries were with the prime minister at the height of the peace process and were privy to sensitive diplomatic information that even the heads of the defense establishment did not know. Their tenure preceded the establishment of the NSS.

The seasoned major general can be characterized as an officer with much experience, knowledge, and well thought out opinions, who is deeply involved in the politics of the defense establishment and even the political system. The prime minister may see him as an authority on defense issues and rely on his judgment, more than with a senior staff officer or beginning major general. He may offer the prime minister alternative positions to those of the defense establishment, which he knows well, while he enjoys priority over the heads of the defense establishment in familiarity with sensitive political information, access to the prime minister, and the ability to influence the cabinet's agenda. As noted, he does not have the responsibility that they have.

## The Preferred Model

The best model for a military secretary is to a large extent dependent on the challenges facing the prime minister and his advisers. Already at the time of Israel's establishment, it was clear that the prime minister could not fill his role properly without appropriate mechanisms for advice on national security and intelligence, even though the military secretary was always at his disposal. During periods when prime ministers also functioned as defense ministers, they positioned themselves to a decisive extent on the apparatuses of the IDF and the Ministry of Defense, so that the gap was less conspicuous. However, the surprise of the Yom Kippur War in 1973 undermined this model.

The amendment to the *Basic Law: The Government* from March 1992 states that "the government will have a team, set up and operated by the prime minister, for ongoing professional advice in the area of national security." In fact, this team was not established, and seasoned major generals (Danny Yatom and Zeev Livneh) were appointed to the position of military secretary and closed the gap partially, since they were not head of a professional staff. Only in 1999 was a decision made by the government, headed by Netanyahu, to establish the National Security Council (NSC) as "the staff institution of the prime minister and the entire government on matters of national security," and Major General (ret.) David Ivry was appointed head of the first NSC. The military secretary at that time was a brigadier general. In 2001, Prime Minister Sharon began to promote officers of the rank of brigadier general to major general during their term as military secretary. The model of the entry-level major general apparently suited Sharon, known for his deep involvement in the IDF. The NSC had already been established, but it was not included in decision making processes, which were coordinated by the military secretary and holders of other offices in the prime minister's bureau.[30]

The gap was even more prominent in both the state comptroller's report on the NSS[31] and in the conclusions of the committee to examine the events of the Second Lebanon War (the Winograd Commission of 2006), which pointed out serious flaws in staff work and in the decision making process of the prime minister's office. In 2007, the steering committee to implement the recommendations of the Winograd Commission interim report (the Lipkin Shahak Commission) suggested limiting the role of the military secretary to the realm of the prime minister's connection with the

security agencies and giving the military secretary the rank of colonel.[32] This suggestion was intended to pave the way for the development of the NSS in order to improve government decision making.

The bill to establish the National Security Staff, which was discussed in the Knesset in 2007 and preceded the National Security Staff Law of 2008, is in keeping with the conclusions of the Lipkin Shahak Commission (to recommend the model of a senior staff officer), and for similar reasons. In addressing the role of the military secretary, the commission wrote that the prime minister, in consultation with the minister of defense, should appoint an officer of the rank of colonel to the position of military secretary, and that the role of the military secretary would be to serve as a liaison between the prime minister and the IDF, the GSS, and the Mossad.[33]

Nevertheless, the National Security Staff Law, passed in the Knesset on July 29, 2008, did not define the role of the military secretary. The law left it to the prime minister to arrange through (internal) regulations the relationship between the head of the NSS and other officials in the Prime Minister's Office (including the military secretary).[34] While such a regulation was approved by the prime minister in 2011, it became clear that it allows him to delegate staff work connected to foreign affairs and defense to officials outside the NSS, including the military secretary. This means that the role of the military secretary has remained quite extensive and its delineation in regard to the NSS has remained vague. As a result, in spite of the NSS Law, the inherent tension between the head of the NSS and the military secretary has not disappeared. In 2012 Uzi Arad noted that "the military secretary does not obey the NSS Law and attempts to keep as much power for himself as possible, at the expense of the head of the NSS."[35] This claim matches the state comptroller's report from June 2012 on implementation of the NSS Law, which noted that the two documents received by the Prime Minister's Office that are supposed to resolve the issues regarding the role of the military secretary (the procedure for implementing the NSS Law and the job description for the military secretary) "include clauses that are opposed to the NSS Law and its intent. Therefore, it would be advisable to correct these documents so that they are compatible with the provision of the law. A situation in which there is overlap and a lack of clarity in the division of powers could perpetuate power struggles between the NSS and [the office of] the military secretary, and impair the ability of each to fulfill its role optimally."[36]

The prime minister needs assistance on issues connected to management of the intelligence community, with an emphasis on the Mossad and the GSS, which are directly under him. He also needs advice on the use of intelligence and intelligence assessments for decision making purposes. In previous decades, various elements pointed out the gaps in the prime minister's ability to cope with these issues on his own. Thus, for example, commissions that examined the issue of intelligence, such as the Yadin-Saraf Commission in 1963 and the Agranat Commission in 1975, recommended the appointment of an intelligence adviser to the prime minister.[37] Since then, the intelligence community has grown much larger, as have the intelligence challenges. The vacuum was eventually filled by the military secretary, with the assistance of a colonel appointed as deputy military secretary for intelligence. Efraim Halevy, former head of the NSS and the Mossad, has noted that since generally the military secretary is an officer from operations, his understanding of intelligence is lacking.[38] In 2006 the Winograd Commission recommended eliminating the military secretary's "intelligence division" and establishing a team in the NSS to deal with intelligence assessments that would integrate the information and assessments coming from intelligence agencies. This recommendation was not accepted by the prime minister. However, in May 2009 the Ministry of Intelligence Affairs was established, headed by Dan Meridor, to assist the prime minister (the Mossad and the GSS remained under the prime minister). In March 2013, Dr. Yuval Steinitz was appointed minister of strategy, intelligence, and international relations.

From the above, it is evident that a number of officials who examined the issue found that the desired model for a military secretary is a senior staff officer. All of them ruled out the models in which a major general serves in this position. Their reasons were as follows:

a. It is an important position that is appropriate for a colonel or brigadier general.
b. The power and the broad activities of a military secretary of the rank of major general are not desirable and could even be harmful. They are liable to limit the influence of offices with responsibility and actual and legal authority, such as the NSS and the Defense Ministry, on issues of weighty significance for national security, for example, a strategic attack on an enemy country, a decision to launch or postpone a military operation, a change in the size of the defense budget, IDF buildup,

division of operational responsibility among security agencies, and security aspects of political issues (such as withdrawal from the Golan Heights, the fate of the Jordan Valley in a political agreement, and the like). In addition, a high ranking military secretary could create an undesirable barrier between the prime minister and the heads of the defense establishment; this was pointed out, for example, by former defense minister Major General (ret.) Yitzhak Mordechai[39] and former Mossad head Efraim Halevy.[40]

c. The military secretary is at a relative disadvantage. The ability of the military secretary to coordinate security discussions and advise the prime minister could be inferior to that of the head of the NSS and the Defense Ministry, partly because the military secretary does not serve as the head of a professional staff suited to this. Furthermore, the military secretary's working in parallel to the NSS without coordination is likely to cause problems.

d. Negative impact on the IDF: As defense minister, Ehud Barak noted that the appointment of an officer of the rank of major general from the command track as military secretary "has a negative impact on the officers themselves and is damaging to the IDF." Then-Chief of Staff Gabi Ashkenazi also had principled reservations about such an appointment.[41]

## The Prime Minister's Position

Since Netanyahu's election as prime minister in 1996, it has generally been evident that he considers orderly, in-depth staff work on the national level to be very important, and his contribution to the establishment of the NSS is noteworthy. However, in recent years since the passage of the NSS Law in 2008, which he supported, Netanyahu has given the impression of having retreated significantly from his concept of the NSS as a dominant institution in preparing staff work for the prime minister. This can be seen in his prior high expectations of the NSS,[42] compared with his current support for the position of the military secretary and his powers even at the expense of the NSS.

A letter from Prime Minister Netanyahu to the state comptroller in July 2010 reflects his position.[43] According to Netanyahu, the military secretary operates at the most sensitive junction for decisions on Israel's security. His work requires an officer with the rank of major general, who

is greatly recognized by the defense establishment and the prime minister, the prime minister's bureau, and the entire government. The officer must have experience in the use of operational force and force buildup, including strategic thinking and assessment. "All of these leave no room for discussion about the rank of the military secretary." And, "the military secretary gives directives to the heads of the defense establishment and government ministries on behalf of the prime minister, holds an ongoing dialogue with them, and monitors their implementation of directives. Since the prime minister and his bureau's work interfaces with the heads of the defense establishment, if the interests of the defense establishment are represented in the prime minister's bureau by an officer with a rank lower than major general, they could be significantly harmed." The prime minister added that "ultimately, the military secretary, like other staff in the prime minister's bureau . . . must be representative and have official status. Therefore, the military secretary cannot have a rank other than major general." In closing, the prime minister wrote that "in light of all of this, I agree with the position of previous prime ministers in stating that the status and the rank of the military secretary should be major general."

In a meeting with the state comptroller in June 2011, the prime minister noted: "I have never thought, although this is the law, that one institution [or] person should give you the recommendations, because this is a recipe for trouble . . . in other words, it [the NSS] is a major institution but not the only one. I really think that it is dangerous for a prime minister to be in a situation in which he accepts, on almost all the issues I mentioned, one opinion or [person] that coordinates all opinions for him."[44] And indeed, the state comptroller's investigation showed that the prime minister gives the military secretary the task of coordinating discussions on foreign affairs and defense, even more than the head of the NSS.[45]

The above shows two reasons for the prime minister's rejection of recommendations on lowering the status of the military secretary. One is that the rank of major general gives the military secretary authority as the representative of the prime minister, especially in contacts with the IDF, and it makes the prime minister's retinue more representative. For this purpose, it is possible to make do with a beginning major general as military secretary, since if his professional experience on strategic issues was the decisive factor, a seasoned major general should have been chosen.

A second reason is that Prime Minister Netanyahu is not prepared to give the NSS exclusivity over coordination of staff work on national security, in spite of the NSS Law. He leaves a considerable portion of this work in his hands, through the military secretary. It would appear that Netanyahu has learned from experience about the capabilities of the NSS, but also about its limitations, and he divides the issues between the military secretary and the NSS, "partly in accordance with the NSS's capability in certain areas," as the state comptroller put it.[46] Aside from the need for pluralism, noted by the prime minister, he apparently sees the military secretary as a senior personal and professional aide, and a member of his staff, who is loyal exclusively to him. The NSS, in contrast, is a governmental institution that is required to fulfill its functions under the law and is liable to have a conflict of interests with him. For example, the head of the NSS could present to the prime minister and later to the cabinet a political-security situation assessment formulated by a professional staff without considering political sensitivities. Such a result could be avoided by using the military secretary or a personal adviser. In addition, holding discussions that include a small number of people in the prime minister's bureau reduces the risk that sensitive information will be leaked. In other words, compartmentalization and the duty of loyalty give an advantage to the military secretary.[47] The position of the prime minister, that the NSS "should first of all coordinate cabinet meetings and ministerial meetings on security issues"[48]—and by implication, the military secretary will coordinate more limited discussions—tends to support this distinction.

Prime Minister Netanyahu appears to find advantages in the position of military secretary on a number of other issues, such as those requiring short response times. For example, it is possible that in many cases, the Prime Minister would prefer to receive staff work quickly, all of which was coordinated by the Ministry of Defense with the mediation of the military secretary, and not to delay them with further staff work by the NSS. In addition, he relies on the military secretary for ongoing operational matters and for conveying intelligence and reports on security incidents. In the meantime, it appears that Netanyahu ultimately has left to the military secretary the task of "regulating and conveying intelligence" to the prime minister, which in the past, he considered to be clearly the job of the NSS.[49] To be sure, establishing the NSS has not yet solved the problems in operational coordination between all security agencies in Israel, which

are in various government ministries. This is a function carried out to a certain extent by the military secretary as he coordinates between them and the prime minister. There are also the difficulties the NSS has encountered in cooperation with the defense establishment, even after passage of the NSS Law. The heads of the defense establishment are not enthusiastic about the division the military secretary creates between them and the prime minister, but the head of the NSS, who has a staff and can check their outcomes, could be a greater obstacle than the military secretary.

## Conclusion and Recommendations

Some of the problems that have become evident in the role of the military secretary are only symptoms of deeper problems in the management of defense and foreign affairs in Israel. These concern, inter alia, the need to define the role of the prime minister vis-à-vis the IDF[50] and the need to define the control, division of responsibility, and joint action of all institutions in Israel that deal with foreign affairs and defense matters, which are in different government ministries. This article has not discussed these matters but has instead examined the role of the military secretary within this matrix.

In the past five years, there has been evident improvement in staff work on national security in the Prime Minister's Office, especially because the NSS has grown stronger, and there are periods of coordination and cooperation between the military secretary and the NSS, in spite of the structural flaws. Nevertheless, the potential for glitches has remained, and the issues with the position must be resolved by the prime minister, who determines the nature of the position and its powers.

What follows are some recommendations to improve the situation:

a. Define clearly and formally the role of the military secretary as a component in the overall staff work of national security. The current ambiguity concerning the functions of the military secretary could prevent the closing of the circle of authority and responsibility for issues of national security and leave an opening for failures in the future. Such a correction is necessary for the proper functioning of the entire security-political complex in Israel. In the meantime, the clash between the NSS Law and the regulations defining the role of the military secretary should be resolved. Either the arrangement should be amended or the NSS Law changed. In addition, it would

be preferable for the responsibilities of the military secretary to be anchored in a government directive or in a law (appended to the NSS Law) and for them to be mainly on non-classified issues.

b. Limit the work of the military secretary to the traditional role of liaison between the prime minister and the security agencies. This role is highly influential in any case, and it suits the position of the military secretary in the system. This would also allow the NSS and the Ministry of Intelligence Affairs to perform their functions and realize their relative advantages. For example, Intelligence Affairs could have an advantage in coordinating staff work (work plans, budgets, and the like) with intelligence organizations, with ongoing operational activity remaining at this stage with the military secretary. The NSS has an advantage in comprehensive staff work and organizational memory, and therefore, it would be better if the NSS also coordinated broad staff work on foreign affairs and defense that the prime minister assigns to others (outside the NSS), mainly the Defense Ministry.

c. Appoint a civilian to the position. It is not necessary for the military secretary to be a military figure, and in any case, a considerable part of his work concerns liaison between the prime minister and civilian security organizations that are subordinate to the prime minister. Appointing a civilian would make it possible to shape the role of the military secretary in accordance with its original purpose and would resolve the need to appoint an officer with the rank of major general out of considerations of representation. This would end the permanent presence of a senior officer in uniform in the prime minister's bureau, which is rife with political tensions, and would remove the incongruousness of a major general in the IDF being subordinate to the prime minister and not to the chief of staff. The civilian should be someone with broad professional knowledge and experience in security (such as a former high ranking official in the IDF, the GSS, or the Mossad) who is familiar the defense establishment and the intelligence community, is experienced in staff work, and has strong personal skills in communication and coordination. This appointment should be based on trust and not a political appointment, and the position be called "security secretary to the prime minister."

d. Have a personal adviser. On security-political issues that are very sensitive politically or personally and on which the prime minister is

not interested in consulting with statutory office holders, such as the head of the NSS, it would be desirable for him to appoint a personal adviser who is not involved in staff work himself.

e. Reexamine the need for a "cascade" of reports and intelligence reaching to the prime minister through the military secretary. It is clear that this is a result of a decision not by the military secretary, but by the prime minister himself and the organizations that provide the information to his bureau. Although it is hard to cut oneself off from the flow of intelligence, this resource places an enormous burden on the prime minister and it is doubtful that it is justified in terms of costs and benefits to his valuable time, which is supposed to be dedicated to a large extent to economic and social issues as well. Therefore, the procedures for disseminating security information to the prime minister should be reexamined with an eye toward focusing it and reducing the quantity, and having the reporting organizations take responsibility.

## Appendix. Military Secretaries to the Prime Minister

| Military Secretary | Term of Office | Prime Minister | Positions prior to and following military secretary position |
|---|---|---|---|
| Colonel Nehemia Argov | 1948-1953<br>1955-1957 | David Ben Gurion | Before the establishment of the state, served as adjutant to the Haganah.<br>Between the establishment of the state and 1950, served as adjutant to the prime minister.<br>In January 1950, appointed first military secretary. Died in November 1957. |
| Colonel Haim Ben-David | 1958-1963 | David Ben Gurion | Before military secretary position: chief of staff for Northern Command and head of officers' personnel administration in IDF Manpower Branch.<br>After military secretary position: head of Manpower Branch. |
| Colonel Yitzhak Nessyahu | 1963-1966 | Levi Eshkol | |
| Brigadier General Yisrael Lior | 1966-1974 | Levi Eshkol, Golda Meir | Before military secretary position: head of Manpower/Individuals Department in Manpower Branch.<br>After military secretary position: left the IDF, served as director general of national oil company. |

| Military Secretary | Term of Office | Prime Minister | Positions prior to and following military secretary position |
|---|---|---|---|
| Brigadier General Ephraim Poran | 1974-1981 | Yitzhak Rabin, Menachem Begin | Before military secretary position: IDF spokesman (brigadier general). After military secretary position: left the IDF. |
| Brigadier General Azriel Nevo | 1981-1993 | Menachem Begin, Yitzhak Shamir, Shimon Peres, and Yitzhak Rabin | Before military secretary position: deputy military secretary. As military secretary, was promoted from the rank of lieutenant colonel, to colonel, and to brigadier general. After military secretary position: military attaché in Great Britain and Ireland. |
| Major General Danny Yatom | 1993-1996 | Yitzhak Rabin, Shimon Peres | Before military secretary position: OC Central Command, head of Planning Branch. After military secretary position: head of Mossad, head of Ehud Barak's political-security staff. |
| Major General Zeev Livneh | 1996-1997 | Benjamin Netanyahu | Before military secretary position: head of Combat Corps headquarters (Ground Forces); commander, Home Front Command. After military secretary position: IDF attaché in Washington. |
| Brigadier General Dr. Shimon Shapira | 1997-1999 | Benjamin Netanyahu | Before military secretary position: deputy military secretary for intelligence. Promoted to rank of brigadier general during term as military secretary. After military secretary position: left the IDF. |
| Brigadier General Gadi Eizenkot | 1999-2001 | Ehud Barak, Ariel Sharon | Before military secretary position: Golani Brigade commander. Promoted to rank of brigadier general while serving as military secretary. After military secretary position: commander of reserve Armored Division, Judea and Samaria Division commander, head of Operations Branch (major general), OC Northern Command, and today, deputy chief of staff. |

| Military Secretary | Term of Office | Prime Minister | Positions prior to and following military secretary position |
|---|---|---|---|
| Major General Moshe Kaplinsky | 2001-2002 | Ariel Sharon | Before military secretary position: commander of the Galilee Division. Promoted to rank of major general while serving as military secretary. After military secretary position: OC Central Command and deputy chief of staff. |
| Major General Yoav Galant | 2002-2005 | Ariel Sharon | Before military secretary position: chief of staff, Ground Forces. Promoted to rank of major general while serving as military secretary. After military secretary position: OC Southern Command. |
| Major General Gadi Shamni | 2005-2007 | Ariel Sharon, Ehud Olmert | Before military secretary position: head of Operations Branch in the General Staff (brigadier general). Promoted to rank of major general while serving as military secretary. After military secretary position: OC Central Command, military attaché in Washington. |
| Major General Meir Kalifi | 2007-2010 | Ehud Olmert, Benjamin Netanyahu | Before military secretary position: deputy commander of Ground Forces with rank of major general. After military secretary position: left the IDF. |
| Major General Yohanan Locker | 2010-2012 | Benjamin Netanyahu | Before military secretary position: chief of staff of the IAF. Promoted to rank of major general while serving as military secretary. After military secretary position: left the IDF. |
| Major General Eyal Zamir | 2012- | Benjamin Netanyahu | Before military secretary position: chief of staff of Ground Forces. Promoted to rank of major general while serving as military secretary. |

## Notes

1 State Comptroller, "Audit Report, Implementation of the NSS Law and Handling of the Turkish Flotilla," June 2012. The report deals with 2009 through 2011.

2 According to a letter from Prime Minister Netanyahu to the state comptroller in June 2010, as noted in the state comptroller's report "Procedures for the Appointment of Senior Officers in the IDF," August 2010.

3 "Recommendations of the Steering Committee on Implementing the Recommendations of the Winograd Commission Interim Report" (Lipkin Shahak Commission), June 26, 2007.

4 State Comptroller, "Audit Report, Procedures for the Appointment of Senior Officers in the IDF."

5 Ibid.

6 In March 1992, there was an amendment to the Basic Law: The Government, which stated, inter alia, that "there will be a ministerial committee on security issues in the government that will be headed by the prime minister."

7 Minutes No. 46, Meeting of the Knesset Committee for State Audit Affairs, January 17, 2007, Knesset website. The committee discussed the state comptroller's report on the National Security Council from September 2006. The prime minister's comments were apparently intended to support resolution of the issues with the functions of the NSS.

8 State Comptroller, "Audit Report, Procedures for the Appointment of Senior Officers in the IDF."

9 Ibid.

10 For example, the opinion of former Mossad head and NSS head Efraim Halevy. See State Comptroller, "Audit Report on the National Security Council," September 2006.

11 Rinat Avigur, "Man in the Shadows," *Bamahaneh*, No. 6, February 3, 2010, IDF Spokesman's website.

12 Azriel Nevo in an interview with Tom Segev, Channel 10, June 26, 2012.

13 State Comptroller, "Audit Report, Implementation of the NSS Law and Handling of the Turkish Flotilla."

14 According to the state comptroller's report of June 2012, the office of the military secretary incudes the deputy military secretary for intelligence (colonel), the bureau head (major), bureau manager (captain), and a number of soldiers doing regular army service. The fact that the size of the military secretary's office has remained limited over the years could indicate that there is broad agreement that the position does not require a large staff.

15 State Comptroller, "Audit Report, Implementation of the NSS Law and Handling of the Turkish Flotilla."

16 From a draft of Uzi Arad and Limor Ben-Har, *The National Security Council: The Struggle to Regulate Decision Making at the Top*, June 2013.

17 State Comptroller, "Audit Report, Implementation of the NSS Law and Handling of the Turkish Flotilla."
18 By "consulting" the intention is direction for activities in which the military secretary himself formulates a professional, well-grounded position, sometimes while gathering data and assessments from various institutions, and the prime minister feels confident in relying on it in his decisions by virtue of his assumption that the military secretary is an authority and a senior figure in the defense establishment. This does not mean expressing a non-binding opinion in a conversation taking place with close colleagues, which could also have a considerable impact.
19 Avigur, "Man in the Shadows."
20 "Recommendations of the Steering Committee on Implementing the Recommendations of the Winograd Commission Interim Report."
21 State Comptroller, "Audit Report, Implementation of the NSS Law and Handling of the Turkish Flotilla."
22 Ibid. According to the law, the description is an internal document written by Military Secretary Major General Meir Kalifi in 2009, which was also adopted by the military secretary who succeeded him.
23 In 1986, the military secretary was included as an observer and a representative of the prime minister on the committee. See State Comptroller, "Audit Report on Implementation of the NSS Law and Handling of the Turkish Flotilla."
24 Arad and Ben-Har, *The National Security Council: The Struggle to Regulate Decision Making at the Top*.
25 Ibid.
26 In a book in memory of Nehemia Argov, Yigael Yadin writes about the role of the first military secretary: "Sometimes, Nehemia had to convey orders and commands on delicate issues that had not been clearly defined and to coordinate the position of subordinates who were not comfortable with the orders given. It was his job to mediate between the prime minister and the defense minister and the military leaders." See Yigal Yadin, *Nehemia Argov* (Yedidim, 1959).
27 Brigadier General Gadi Eizenkot was the exception in this group. In 2001, he returned to the IDF chain of command as a brigadier general, and today he serves as deputy chief of staff.
28 Major General Moshe Kaplinsky, who was the first to be promoted to the rank of major general while serving as military secretary, later served as OC Central Command and as deputy chief of staff.
29 The defense establishment is not a strong supporter of improving the standing of the NSS, which was among the reasons for the NSS Law.
30 NSC head Giora Eiland stated in 2005 that while the prime minister has the National Security Council, which is an institution with capabilities and depth, although it is at least partially distanced from the circle of decision makers. In addition, there is a group of very close advisers near the prime

minister, a military secretary, a political adviser, and others, who have no ability to do serious work. See "Audit Report on the National Security Council."

31 Ibid.

32 "Recommendations of the Steering Committee on Implementing the Recommendations of the Winograd Commission Interim Report."

33 The Government Law bill (National Security Staff Amendment), 2007. The draft law was proposed by twenty-seven MKs, headed by Amira Dotan and Tzahi Hanegbi.

34 National Security Staff Law, 2008.

35 Barak Ravid, "Lindenstrauss: I'll Check Arad's Claims that Prime Minister's Bureau Lied in Audit," *Haaretz*, March 13, 2012. Nimrod Busso, "It's a Shame the Prime Minister's Office is Not an Elite Unit," *The Marker*, December 19, 2012.

36 State Comptroller, "Audit Report, Implementation of the NSS Law and Handling of the Turkish Flotilla."

37 The Yadin-Saraf Commission focused on the adviser's providing the prime minister a picture of activity by the services (including work plans, plans for action, and the like) and assisting him with intelligence assessments, while the Agranat Commission focused only on the need for assessment.

38 State Comptroller, "Audit Report, The National Security Council."

39 State Comptroller, "Audit Report, Procedures for the Appointment of Senior Officers in the IDF."

40 State Comptroller, "Audit Report, The National Security Council."

41 State Comptroller, "Audit Report, Procedures for the Appointment of Senior Officers in the IDF."

42 The following are comments made by Prime Minister Netanyahu to the Knesset Committee for State Audit Affairs, January 2007: "The (national security) adviser must meet with the prime minister every day, not in a staff meeting, but in a separate meeting. He is not part of the political team; he is in the national security team, every day. The council must be not only the regulator and provider of intelligence; it must be directed by the prime minister to do and to follow up and to lead the staff work for him on issues of national security. An example: Today, this council was supposed to convene daily with the relevant functionaries, whether the head of the Mossad or the head of the Atomic Energy Commission or the chief of staff or the heads of the intelligence agencies. It must convene daily on a master plan to remove the Iranian threat. Removing the Iranian threat is a classic case in which you need a National Security Council because you also need a very large international effort, a political effort, an informational effort, a legal effort, like that which we have begun to initiate."

43 State Comptroller, "Audit Report, Procedures for the Appointment of Senior Officers in the IDF."

44 State Comptroller, "Audit Report, Implementation of the NSS Law and Handling of the Turkish Flotilla."
45 Ibid.
46 Ibid.
47 Some believe that it is precisely the compartmentalization and the discussions in a small forum that increase the risk of making staff work superficial because "they take away from prime ministers the possibility of relying on high-quality, skillful, and thorough action and enjoying the fruits of orderly and systematic staff work." See Government Law bill [National Security Staff Amendment], 2007, explanatory remarks).
48 State Comptroller, "Audit Report, Implementation of the NSS Law and Handling of the Turkish Flotilla."
49 See note 7.
50 See Shmuel Even and Zvia Gross, *Proposed Legislation on the IDF: Regulating Civil-Military Relations in the Wake of the Second Lebanon War*, Memorandum No. 93 (Tel Aviv: Institute for National Security Studies, April 2008).

# The Revolutionary Guards and the International Drug Trade

**Sami Kronenfeld and Yoel Guzansky**

The Revolutionary Guards are significantly involved in the international drug trade, both directly and through proxies. This involvement provides the organization with access to sources of financing that bypass international sanctions, as well as to sophisticated operational platforms that support its subversive efforts aimed at the West. For Iran's enemies, and especially to Israel, the link between a global, sophisticated, and determined organization as the Revolutionary Guards and the world of organized crime is a phenomenon that is, in the absence of appropriate attention and response, liable to have significant strategic ramifications. This essay seeks to demonstrate the link between the Iranian Revolutionary Guards and the international drug trade as one development within the growing terrorism-crime spectrum. The Western discussion on security has not given a great deal of attention to this connection as it relates to the Iranian threat, but evidence and developments of recent years invite an in-depth analysis of the phenomenon and its ramifications. This essay suggests that the link between the Revolutionary Guards and the international drug trade contains not only challenges but also opportunities for Western countries and their allies.

**Keywords:** Revolutionary Guards; Iran; drug trade; terrorism; Hizbollah

The 2013 annual Worldwide Threat Assessment Report produced by the Office of the Director of National Intelligence (ODNI) rated terrorism and transnational organized crime as the second most severe threat to the United States security. Second to cyber threats, terrorism and transnational

Sami Kronenfeld is an intern in the Cyber Warfare Program at INSS. Yoel Guzansky is a research fellow at INSS.

organized crime bypassed the unconventional weapons proliferation threat.[1]

ODNI's decision to link terrorism and organized crime together indicates that Western decision makers realize these two worlds are colliding, and present Western interests with a profoundly dangerous challenge.[2] This essay seeks to demonstrate the link between the Iranian Revolutionary Guards and the international drug trade as one development within the growing terrorism-crime spectrum. The Western discussion on security has not given a great deal of attention to this connection as it relates to the Iranian threat, but evidence and developments of recent years invite an in-depth analysis of the phenomenon and its ramifications. This essay suggests that the link between the Revolutionary Guards and the international drug trade contains not only challenges but also opportunities for Western countries and their allies.

## Terrorism and Organized Crime

Extensive, systematic interactions between terrorist organizations and organized crime began in the 1980s, when organizations with political agendas forced their patronage on the drug industry and imposed "taxes" on producers and smugglers of the growing Afghani drug industry. In other locations, such as Latin America, terrorist and criminal organizations joined forces to achieve common goals. Still, despite the friction between political terrorist organizations and criminal organizations, a clear separation between the two was maintained until the early 1990s. While terrorist organizations participated in organized crime solely to finance their political and ideological activities, crime organizations were motivated by the possibility of economic gain, using violence and terrorism as a tactic to ensure the flow of income and the neutralization of both competition and law enforcement.[3]

This dichotomy grew less distinct after the dissolution of the Soviet bloc, which fundamentally changed the international system. New pressures and opportunities for the different players were created through the formation of an open, global economic system, the increase of freedom of travel and trade, the great access to advanced technologies, the expansion of immigrant communities, the weakening of many states, and the many civil wars that broke. Within this new environment, international crime syndicates flourished and built cross-border networks that produced

vast amounts of money and created an extensive global black market, which replaced the funding many terrorist organizations received from sponsoring states during the Cold War. In the 1990s, some of these terrorist organizations started assimilating into the thriving international criminal system by participating in criminal activities, such as the drug trade, smuggling, and credit fraud. This trend led the worlds of terrorism and crime to adopt one another's behavioral patterns and organizational characteristics, blurring the lines between the players.[4]

The events of 9/11 and the war on terrorism gave significant impetus to the involvement of terrorist organizations in organized crime. As sources of funding that were previously available (like supporting nations, "charity" funds, and private donations) were now the main target for international intelligence and law enforcement agencies, terrorist organizations were forced to increase their reliance on the black capital generated by international crime, which escalated the global battle on terrorism. Similarly, the growing international pressure on the operational and logistical infrastructures of terrorist organizations made many of them resort to tactics that were traditionally associated with organized crime[5] and allowed for covert cross-border activity.[6]

These developments have made many researchers in recent years reject the dichotomous view of terrorism and organized crime as separate spheres, and instead opt to view the two as part of a large spectrum of interactions, organizational structures, and methods. Makarenko describes the link between political terrorism and organized crime as a single axis comprises the various players that progress according to developments in their goals and operational tactics. This axis includes phenomena such as alliances between terrorist and criminal organizations that further specific interests, the appropriation of criminal tactics by terrorist organizations and the creation of organic criminal mechanisms within them, the founding of hybrid entities that unify terrorism and organized crime tactics to advance political goals and to maximize profits (coalescence), and the transition of some organizations from one type of activity to another (transformation).[7]

Terrorist organizations are deeply involved in a wide gamut of criminal activities, such as blood diamonds and vehicle theft. Still, the international drug industry, the initial locus of the terrorism-crime connection, remains the most common crime of terrorist organizations.[8] The term "narco-terrorism" was coined by Peruvian president Fernando Belaúnde Terry

in 1993 to describe the drug cartels' usage of terrorist tactics, and has since served as a code name for the tight relationships between terrorist organizations and the global drug industry. According to the American Drug Enforcement Agency (DEA), 19 of the 49 organizations on the State Department's list of terrorist organizations and some 60 percent of terrorist organizations around the world are linked to the international drug market. Among the prominent organizations on this list are the Afghani Taliban, al Qaeda, the Colombian FARC,[9] and Hizbollah.[10]

A major motivating factor for terrorist organizations to take part in the drug industry is its tremendous potential for profit, which stems from the industry's enormous consumer base worldwide.[11] According to assessments made by the United Nations Office on Drugs and Crime (UNODC), the international drug market is worth some $320 billion annually.[12] The potential for such high profits, along with the relatively simple processes of drug production, commerce, and sales makes this industry an effective and accessible source of income for terrorist organizations.[13] In addition, working with organizations that control international smuggling allows for terrorist organizations to have easy access to operations that enhance their capacity to carry out complex, cross-border acts, such as document forgery, human trafficking, customs schemes, and money laundering.[14]

## The Revolutionary Guards and International Drug Trade Connection

Established in 1979 by Ayatollah Khomeini, the Revolutionary Guards have grown beyond their basic security function to become a political, social, and economic corporation with a foothold in every aspect of Iranian political and social life.[15] The organization is the most robust economic body in the country, possessing holdings in a wide range of industries, such as security, energy, construction, and communications,[16] and many of its former members currently hold senior political and bureaucratic positions. At the state security level, the institution is a major advocate of Iranian interests in the Middle East and around the world, focusing particularly on Iran's desire for regional hegemony and the ouster of Western influence from the Middle East. In this context, the Revolutionary Guards are active on two major complementary levels. First, the organization leads the efforts to export the Iranian Islamic Revolution, seeking to expand the republic's political, ideological, and religious influences in the Middle

East, Central Asia, Africa, and Latin America. Secondly, the Revolutionary Guards continuously exert efforts to undermine the influence of the United States in the Middle East by harming the superpower's regional interests and its allies. Given that Iran is militarily inferior to the United States, the Revolutionary Guards make extensive global use of asymmetrical strategies in their struggle against the West and its allies, preferring tactics of subversion and terrorism.[17]

Within the ranks of the Revolutionary Guards, the al-Quds Force is in charge of exporting the Islamic Revolution and organizing terrorist and subversive activity against Iran's enemies. Established in 1990, this elite unit uses terrorist methods, provides operational, logistical, and training support to revolutionary and anti-American groups, and penetrates Shiite and various other Muslim populations to create civilian and political infrastructures that support Iran's agenda. The Al-Quds Force utilizes proxies as a way to disguise Iran's involvement in acts of cross-border terrorism. The force's most prominent ally is the Lebanese Hizbollah, which was established with the assistance of the Revolutionary Guards.[18]

The Revolutionary Guards are a part of the Iranian establishment, as opposed to other players along the terrorism-crime axis that are considered non-state actors. Nevertheless, the organization's extensive direct and indirect involvement in international terrorism creates extensive similarity between its needs and methods and those of non-state terrorist organizations.[19] Similar to these non-state actors, the Revolutionary Guards, using the great wealth afforded by the international drug trade, try to gain operational and logistical capabilities that will enhance their ability for terror and subversion in enemy territory.[20] These factors have led the Revolutionary Guards to join the trend of the merging of terrorism and crime and take part in a variety of criminal acts around the world, including the international drug trade.

The Revolutionary Guards' involvement in the international drug trade is neither trivial nor natural. Drug addiction, and especially addictions to products of poppy, is responsible for tens of thousands of Iranian deaths per year[21] and has inflicted much damage on Iranian society, which has one of the world's highest rates of opium and heroin usage (2.26 percent of the population aged 15-64, the third highest rate after the United States and Afghanistan).[22] The vast scope of the Iranian drug problem has driven the government to heavily invest in the prevention of smuggling across

the eastern border of the country. Iran is traditionally considered one of the leading countries in the confiscation of heroin.[23] The Revolutionary Guards play a significant role in Iran's war on drug smugglers, and many members of the organization have been killed in battles with drug traders in the southeastern province of Sistan va Baluchistan and in other eastern provinces.[24] The Revolutionary Guards' participation in the war on drugs is prominently and proudly highlighted by the organization as a means of strengthening its domestic and international legitimacy.[25] Nonetheless, alongside their efforts to battle drugs, the Revolutionary Guards also wish to harness the strategic and tactical potential of the international drug trade in order to advance their goals.

The involvement of the Revolutionary Guards and the al-Quds Force in the international drug trade provides them with strong ties to global crime organizations. These ties create operational and logistical platforms that support and enhance the ability of the Revolutionary Guards and specifically the al-Quds Force to pose a threat to their enemies' territories and populations by forging documents, smuggling goods across borders, laundering money, supporting black banking, and so on.[26] Drugs are also used by the Revolutionary Guards as weapons against Western nations and their allies, as they are destructive to society, break the nuclear family, damage youth, strengthen organized crime, cause increased violence, decrease the sense of personal safety, and exert pressure on welfare and law enforcement agencies. The state is then forced to allocate a great deal of money and manpower to combat these phenomena. According to the testimony of an Iranian defector and a former member of the Revolutionary Guards, "We were told that the drugs will destroy the sons and daughters of the West, and that we must kill them. Their lives are worth less because they are not Muslims."[27]

Finally, the Revolutionary Guards' involvement in the drug market also provides the organization with cash. Due to the severe international sanctions imposed on Iran, the Revolutionary Guards' involvement in the country's smuggling industry has become a major factor in the country's economy and trade, as it allows the organization to make tremendous profits by controlling border crossings and "taxing" illegal smuggling activity.[28] In this context, the Revolutionary Guards' involvement in the international drug trade and the sponsorship of criminal organizations that are involved in it are a source of income of almost unlimited potential.

The Revolutionary Guards are involved in the international drug trade directly and through proxies. The direct involvement of the Revolutionary Guards is first and foremost exemplified by the Afghani heroin industry. Geographically, Iran is located between the poppy fields of Afghanistan and the West, which makes it the starting point of the world's major heroin trade routes, supplying the drug to Russia, Western Europe, and the United States. The UNODC estimates that some 140 tons of heroin—87 percent of the Afghani heroin trade—are transported through Iran annually.[29] These geostrategic conditions make the Revolutionary Guards a major player in the Afghani heroin industry and, according to American classified intelligence assessments, indicate the involvement of the al-Quds Force in several of the drug smuggling routes going to Western markets from Iran.[30] The Revolutionary Guards maintain close contact with leading figures from the Afghani drug trade and international crime organizations in order to facilitate drug deliveries to the West. The transport of drugs is then exchanged for monetary payment or operational assistance, such as the distribution of Iranian weapons to the Taliban or other terrorist organizations that fight against the Afghani government and the NATO forces that are stationed in Afghanistan.[31]

In addition to cooperation with crime organizations, the Revolutionary Guards also seem to run their own autonomous apparatus for the production and distribution of heroin. Members of the organization bring tremendous quantities of raw opium from Afghanistan to Iran, which are processed into heroin and other opiates in local labs. These drugs are then transported westwards through the extensive smuggling network established by the Revolutionary Guards, which consists of large fleets of ships and planes, straw companies, and secret bank accounts.[32] A report produced by the US Embassy in Azerbaijan cites senior Azeri government personnel as saying that the Revolutionary Guards are a major player in the country's heroin market. According to the report, investigations by the Azeri government discovered that members of the Revolutionary Guards are directly involved in the transportation of heroin from Afghanistan to Azerbaijan and that the production of these drugs take place in labs in Tabriz and in other Iranian cities. In Azerbaijan, this activity is seen as part of the Iranian attempt to destabilize the pro-Western Azeri government.[33] Evidence submitted by Revolutionary Guards deserters reveals that

involvement in the heroin trade is a widespread phenomenon among various units of the organization.[34]

The Revolutionary Guards also seek to advance their goals by teaming up with international drug traders from Latin America, which is an important strategic arena for Iran. A major player in this Iranian effort is the al-Quds Force. With great determination and the investment of large resources, Iran is trying to expand its web of relations with dominant regional players like Venezuela, Bolivia, and Cuba in order to create operational platforms that could cause harm to US targets and hurt US interests in case the conflict over Iran's nuclear arms program escalates.[35]

In accordance with its traditional operational methods, much of the al-Quds Force activity in Latin America is carried out by proxies that provide it with high levels of operational capabilities while maintaining distance and the ability to deny their involvement. The main Iranian proxy has been identified by American intelligence and administration sources as Hizbollah, which maintains close links with the al-Quds Force and is the executioner of various terrorist and organized criminal activities in Latin America, such as money laundering, member recruitment and training, weapons and drug trade, document forgery, and even the acquisition of minerals and other raw materials likely to serve the Iranian nuclear arms program. It is natural that al-Quds Force relies on Hizbollah for its activities, largely due to the organizations' close relationship and shared interests, and also due to Hizbollah's operational capabilities and power in that part of the world.[36] American authorities point to Hizbollah as a major element in the Iranian threat to American national security and interests in Latin America. A central component of this assessment is Hizbollah's connection to the South American drug cartels.[37]

Hizbollah is a richly experienced player in every aspect of the international drug trade. Since its founding, the organization has been a key player in the Lebanese drug industry, its involvement spanning to everything from growing the raw materials, through producing the drugs, to smuggling and distributing them.[38] Over the years, Hizbollah has expanded its involvement in the international drug trade and became active throughout the Middle East, Europe, Africa, and South America.[39] The organization's extensive involvement with the South American cocaine market has been exposed in recent years.[40] Hizbollah is active in operations such as the initiation and development of contacts and joint ventures with

large drug cartels in countries like Mexico and Colombia, the transporting of drugs to the United States and to other global destinations, laundering of vast amounts of money, and participation in smuggling and organized crime.

The connection between Hizbollah and the Mexican drug cartels has provided the al-Quds Force with an effective operational and logistical platform for conducting subversive activity along the American border and on US territory, as well as in carrying out strategic acts of terrorism. The Mexican drug cartels operate a smuggling apparatus along the 3,000-kilometer-long Mexican-US border. They maintain organizational infrastructures and very loyal manpower from 250 American towns and cities, and their economic means and political influence are almost unlimited.[41] These capabilities allow the cartels to bypass the security features along the border and move vast amounts of drugs, weapons, people, counterfeit goods, explosives, and the like into the United States. It is not inconceivable that, if asked to do so, the cartels would allow the drug smuggling infrastructures to serve Hizbollah agents at carrying out terrorist acts on behalf of al-Quds Force.[42] According to US law enforcement and drug agencies, Hizbollah is already using the cartels' smuggling apparatus to introduce weapons, agents, and money into the United States.[43]

Nevertheless, the al-Quds Force also wants to develop direct working relationships with major players in the Mexican drug market. An attempt to do precisely that was exposed in October 2011 when a plot to assassinate the Saudi Arabian ambassador to Washington came to light. Mansour Arbabsiar, an American citizen of Iranian extraction, was arrested by the FBI. The investigation revealed an attempt by al-Quds operatives to recruit the Mexican drug cartel Los Zetas[44] to carry out strategic terrorist attacks against the United States[45] and the Israeli and Saudi Arabian embassies, and to establish transportation routes to North America for Afghani heroin.[46] According to senior American sources, these attempts were made at the bidding of the highest al-Quds echelons. As a result, Gen. Qasem Soleimani, the commanding officer of al-Quds Force, was placed on the American administration's list of terrorists.[47] James Clapper, the current Director of National Intelligence of the United States, concluded that the affair is evidence of Iran's capacity to carry out an attack on American soil.[48]

It is clear that the Revolutionary Guards and al-Quds Force are deeply involved in the international drug trade, which according to Michael Braun,

the former head of the DEA's operations department, provides them with a vast range of operational and tactical opportunities to advance their strategic goals around the world.[49]

## Implications

The Revolutionary Guards' involvement in the international drug trade should be examined in a broader context and as a part of the changing nature of asymmetrical warfare of the 21st century. In the past, the activity of the weaker side in asymmetrical confrontations was limited to relatively small territories and relied on military tactics and tools aimed primarily against the fighting forces in those territories. Current processes of globalization and technological development, however, give relatively low intensity players the ability to conduct global campaigns and the tools to harm civilian fronts and security interests of nations and powers that are much stronger than they are. The Revolutionary Guards, at the forefront of these developments, systematically and determinedly exploit globalization processes to expand its store of operational capabilities in the asymmetrical conflict against the West and its allies in the Middle East. An example is the Revolutionary Guards' large investment in developing advanced cyberwar capabilities that exploit global information and communications networks to damage the economic and strategic front of powers like the United States.[50] Similar to cyberwar, involvement in the international drug market is also a tool in the asymmetrical battle the Revolutionary Guards are fighting against the West. The organization uses globalization processes, such as the blurring of international borders, the development of global transportation and communications systems, and the growth of international crime syndicates to turn the international drug market into a platform for damaging the strategic interests of the West and its allies.

For Iran's enemies, the connection between a sophisticated and determined global organization like the Revolutionary Guards and the operational capabilities and vast capital represented by the international drug market is rife with security and strategic threats. First, the Revolutionary Guards' involvement in the international drug trade and their deepening relationship with organized crime and drug cartels have improved the organization's operational capabilities, making it more effective at threatening Western interests in many arenas and perpetrating terrorist attacks throughout the world. Second, the Revolutionary Guards'

drug activity could undermine the internal stability of pro-Western regimes in strategic nations, as is happening in Azerbaijan. Third, the financial gain from the drug trade is helping to counter the effectiveness of the international sanctions against the Revolutionary Guards, strengthening its ability to continue to engage in global terrorism.[51]

Still, the Revolutionary Guards' involvement in the international drug trade provides an opportunity to incriminate the organization in illegal activity. While the organization's core activities are subjected to political interpretation and its links to terrorism and cyber attacks leave room for deniability, their involvement in the drug trade is one activity whose traces are harder to hide. This involvement also forces the Revolutionary Guards to forge closer working relationships with criminal organizations that, unlike ideologically motivated terrorists, would not hesitate to sell out their Iranian partners in exchange for lighter sentences and monetary rewards. In addition, the drug trade leaves money tracks that can be followed and used to incriminate the organization. Exposing the links between the Revolutionary Guards and the international drug trade may serve as an effective tool in legal steps and sanctions against Iran and the organization.

All members of the international community are obligated to enforce laws and punish individuals, organizations, and states that take part in the international trade of banned substances and in laundering drug proceeds.[52] Given this, exposing the evidence of the Revolutionary Guards' involvement in the international drug trade would allow the international community to define the organization as one that operate in violation to international law, thereby legally obligating all members of the international community (including Iran itself) to impose sanctions that would limit its activity (apprehension of its members, confiscation of its assets, extradition of wanted individuals, seizures of ships and planes, limits on movement, etc.).[53] This could bypass some of the political and legal obstacles standing in the way of further strengthening the sanctions currently in place against Iran.

Beyond the legal aspect, emphasizing the connections between the Revolutionary Guards and the Iranian regime on the one hand, and the trade in dangerous substances, such as heroin and cocaine on the other, could represent a serious blow to the moral stance to which the Islamic Republic lays claim. Drugs seriously damage the social fabric of many nations throughout the world, including pro-Iranian countries like Russia

and China. Exposing the involvement of the Revolutionary Guards in the international distribution of dangerous drugs to international public opinion could delegitimize the Iranian regime and create public pressure against cooperating with it and supporting it. In addition, Iranian society itself has a very severe problem with heroin addiction, which has destroyed many Iranian families. Stressing the ties between the regime and the drug market could damage the regime's religious and moral authority and even undermine its credibility in the conservative Islamic circles that have traditionally been its powerbase.

In light of all of the above, a concerted effort on the part of the United States, Israel, and other countries to direct intelligence and operational resources into investigating and exposing the ties between the Revolutionary Guards and the international drug trade could result in the creation of legal and political platforms for tightening the sanctions against the organization and furthering the international isolation of the Islamic Republic.

Clearly, the Revolutionary Guards are significantly involved in the international drug trade, both directly and through proxies. This involvement provides the organization with access to sources of financing that bypass international sanctions, as well as to sophisticated operational platforms, that support its subversive efforts aimed at the West. For Iran's enemies, including Israel, the link between a global, sophisticated, and determined organization as the Revolutionary Guards and the world of organized crime is a phenomenon that is, in the absence of appropriate attention and response, liable to have significant strategic ramifications.

## Notes

1 James R. Clapper, *Worldwide Threat Assessment of the US Intelligence Community* (Washington, DC: Office of the Director of National Intelligence, 2013), http://www.dni.gov/files/documents/Intelligence%20Reports/2013%20ATA%20SFR%20for%20SSCI%2012%20Mar%202013.pdf.

2 In previous reports, organized crime appeared only as a subset within the broader category of economic threats.

3 Louise I. Shelley, John T. Picare et al., *Methods and Motives: Exploring Links between Transnational Organized Crime & International Terrorism*, 2005.

4 Tamara Makarenko, "The Crime–Terror Continuum: Tracing the Interplay between Transnational Organised Crime and Terrorism," *Global Crime* 6, no. 1 (February 2004): 128-29.

5 Tactics such as relying on safe havens and diaspora communities, using intelligence and counter-intelligence systems, using forged documents and cross-border smuggling schemes, etc.
6 Thomas M. Sanderson, "Transnational Terror and Organized Crime: Blurring the Lines," *SAIS Review* (Winter–Spring 2004).
7 Tamara Makarenko, "Terrorist Use of Organized Crime: Operational Tool or Exacerbating the Threat?" in *Defining and Defying Organized Crime: Discourse, Perceptions, and Reality*, ed. Felia Allum (London: Routledge, 2009).
8 Sanderson, "Transnational Terror and Organized Crime: Blurring the Lines," p. 52.
9 The Revolutionary Armed Forces of Colombia
10 Michael Jacobson and Matthew Levitt, "Tracking Narco-Terrorist Networks: The Money Trail," *The Fletcher Forum of World Affairs* 34, no. 1 (2010): 118-19, http://www.washingtoninstitute.org/uploads/Documents/opeds/4bbcba42e5c8a.pdf. See also Derek S. Maltz, *Narcoterrorism and the Long Reach of US Law Enforcement,* testimony in US Congress, House Committee on Foreign Affairs, Subcommittee on Terrorism, Nonproliferation and Trade, November 17, 2011.
11 The most recent report by UNODC, published in 2012, estimates that between 150 million and 300 million people in the 15-64 age bracket around the world (i.e., 3.4-6.6 percent of the global population in that age bracket) have used illegal psychoactive drugs at least once. Of these, between 15.5 million and 38.6 million are addicts who use drugs on a regular basis. UNODC, *World Drug Report 2012*, 2012, p. 7.
12 Matthew Levitt, *Hizbullah Narco-Terrorism: A Growing Cross-Border Threat*, IHS Defense Risk and Security Consulting, September 2012, p. 34.
13 James A. Piazza, "The Opium Trade and Patterns of Terrorism in the Provinces of Afghanistan: An Empirical Analysis," *Terrorism and Political Violence* 24, no. 2 (2012): 216.
14 Tamara Makarenko, "Europe's Crime-Terror Nexus: Links between Terrorist and Organised Crime Groups in the European Union," *European Parliament's Committee on Civil Liberties Justice and Home Affairs*, 2012.
15 Frederic Wehrey, Jerrold D. Green et al., "The Rise of the Pasdaran: Assessing the Domestic Roles of Iran's Islamic Revolutionary Guards Corp," *RAND*, 2009, p. xi.
16 Ali Alfoneh, "How Intertwined are the Revolutionary Guards in Iran's Economy?" *American Enterprise Institute*, October 22, 2007.
17 "The Quds Force: The Revolutionary Guards Elite Unit Spearheads Iranian Terrorism," *The Meir Amit Intelligence and Terrorism Information Center-Israeli Intelligence and Heritage Commemoration Center* (2012), pp. 5-6.
18 Ibid, pp. 8-9.
19 United States Department of State, *Country Reports on Terrorism 2012*, May 2013, http://www.state.gov/documents/organization/210204.pdf.
20 Alfoneh, *How Intertwined are the Revolutionary Guards in Iran's Economy?*

21 Bill Samii, "Iran: Domestic Drug Abuse, Smuggling on the Rise," *Radio Free Europe-Radio Liberty*, July 3, 2013, http://www.rferl.org/content/article/1063489.html.

22 UNODC, *World Drug Report 2011*, 2011, http://www.unodc.org/documents/data-and-analysis/WDR2011/StatAnnex-consumption.pdf.

23 In 2010, Iranian authorities caught 33 percent of all heroin intercepted that year. UNODC, 2011, p. 29.

24 John Calabrese, "Iran's War on Drugs Holding the Line?" *Middle East Institute*, 2007.

25 Wehrey, Green et al., "The Rise of the Pasdaran: Assessing the Domestic Roles of Iran's Islamic Revolutionary Guards Corp," p. 65.

26 Piazza, "The Opium Trade and Patterns of Terrorism in the Provinces of Afghanistan: An Empirical Analysis," p. 217.

27 David Cohen, "Iranian Drug Ring Funding Terror?" *Ynet*, November 18, 2011, http://www.ynetnews.com/articles/0,7340,L-4149990,00.html.

28 Jonathan Spyer, "Inside Iran: War by Other Means," The Global Research in International Affairs Center *(GLORIA)*, July 13, 2012.

29 UNODC, *World Drug Report 2010*, 2010 pp. 54-55, http://www.unodc.org/documents/wdr/WDR_2010/World_Drug_Report_2010_lo-res.pdf.

30 Joby Warrick, "In Iran, Drug Trafficking Soars as Sanctions Take Bigger Bite," *The Washington Post*, November 1, 2012, http://articles.washingtonpost.com/2012-11-01/world/35504357_1_global-drug-drug-dealers-drug-trade.

31 In March 2012, the American Treasury Department declared Brig. Gen. Gholamreza Baghbani, the commanding offer of the al-Quds Forces in the city of Zahedan on the Iranian-Afghani border, to be a kingpin of heroin exports to the West. Similar accusation were also leveled against Brig. Gen. Abdullah Araqi, the deputy commander of the Revolutionary Guards' ground forces and the former commander of Tehran Province, who was suspected of maintaining contact with Albanian, Bulgarian and Romanian crime organizations involved in transporting Afghani heroin to the West. US Department of the Treasury, "Treasury Designates Iranian Quds Force General Overseeing Afghan Heroin Trafficking Through Iran," March 7, 2012, http://www.treasury.gov/press-center/press-releases/Pages/tg1444.aspx; Hugh Tomlinson, "Iran's Elite Guard Runs Global Crime Network Pushing Heroin to West," *The Times*, November 17, 2011.

32 Tomlinson, "Iran's Elite Guard Runs Global Crime Network Pushing Heroin to West."

33 "Tehran-Baku Tensions Heat Up," *Aftenposten*, October 15, 2009, http://www.aftenposten.no/spesial/wikileaksdokumenter/article3999424.ece.

34 Tomlinson, "Iran's Elite Guard Runs Global Crime Network Pushing Heroin to West."

35 Jaime Daremblum, "Iran and Latin America," *Hudson Institute*, 2011, http://www.hudson.org/files/publications/Iran_Latin_America_Daremblum_Jan2011.pdf; Norman A. Bailey, "Ahmadinejad's Tour of Tyrants and

Iran's Agenda in the Western Hemisphere," *Hearing Before the House of Representatives Committee on Foreign Affairs*, February 2, 2012, http://www.gpo.gov/fdsys/pkg/CHRG-112hhrg72653/pdf/CHRG-112hhrg72653.pdf.

36 Hizbollah started operating in Latin America in its early years, in the mid-1980s, when its operatives penetrated the Lebanese and Shiite communities in the border triangle where Argentina, Brazil, and Paraguay meet (an area that, even now, is considered to be a type of a Wild West, where government influence is relatively weak). Over the years, Hizbollah agents built extensive infrastructures in Central and South America for training operatives, laundering money, and carrying out acts of terrorism. Western espionage agencies have concluded that in the last decade, some 450 Hizbollah agents have been active in Latin America, managing a widespread network of terrorist and criminal cells. John Rollins & Liana Sun Wyler, "Terrorism and Transnational Crime: Foreign Policy Issues for Congress," *Congressional Research Service*, October 19, 2012, pp. 19-20.

37 US House of Representatives, *House Resolution 429,* October 11, 2011, http://www.gpo.gov/fdsys/pkg/BILLS-112hres429ih/pdf/BILLS-112hres429ih.pdf; US 112th Congress, ''Countering Iran in the Western Hemisphere Act of 2012," December 28, 2012, http://www.gpo.gov/fdsys/pkg/PLAW-112publ220/pdf/PLAW-112publ220.pdf; Roger F. Noriega & José R. Cárdenas, "The Mounting Hezbollah Threat in Latin America," *American Enterprise Institute*, October 6, 2011, http://www.aei.org/article/foreign-and-defense-policy/regional/latin-america/the-mounting-hezbollah-threat-in-latin-america.

38 Gilad Natan, *Drug Smuggling and Interdiction: The Knesset Information and Research Center*, 2010, http://www.knesset.gov.il/mmm/data/pdf/m02424.pdf.

39 Levitt, *Hizbullah Narco-Terrorism*.

40 Roger F. Noriega, "Hezbollah's Strategic Shift: A Global Terrorist Threat," *Hearing Before the House of Representatives Committee on Foreign Affairs*, March 20, 2012, pp. 3-4, http://www.aei.org/files/2013/03/20/-hezbollahs-strategic-shift-a-global-terrorist-threat_134945797264.pdf; US Department of the Treasury, "Treasury Targets Major Money Laundering Network Linked to Drug Trafficker Ayman Joumaa and a Key Hizballah Supporter in South America," June 27, 2012, http://www.treasury.gov/press-center/press-releases/Pages/tg1624.aspx.

41 Bailey, "Ahmadinejad's Tour of Tyrants and Iran's Agenda in the Western Hemisphere," p. 25.

42 Frank J. Cilluffo & Joseph R. Clark, "Thinking About Strategic Hybrid Threats in Theory and in Practice," *Prism* 4, no. 1 (2012), pp. 52-54, http://www.ndu.edu/press/lib/pdf/prism4-1/prism46-63_cilluffo-clark.pdf.

43 "Hezbollah Uses Mexican Drug Routes into US," *The Washington Times*, March 27, 2009, http://www.washingtontimes.com/news/2009/mar/27/hezbollah-uses-mexican-drug-routes-into-us/print; Noriega & Cárdenas, 2011; Levitt, *Hizbullah Narco Terrorism*, p. 41; CIA, " Expanding Links

between Alien Smugglers and Extremist: Threats to the United State," p. 2, http://www.documentcloud.org/documents/369169-2001-07-06-expanding-links-between-alien.html.

44 One of the largest and strongest drug cartels in Mexico, Los Zetas is a violent and vicious organization established by former members of elite units of the Mexican army. The organization maintains widespread and proven links with Hizbollah.

45 US Department of Justice, "Man Pleads Guilty in New York to Conspiring with Iranian Military Officials to Assassinate Saudi Arabian Ambassador to the United States," October 17, 2012, http://www.fbi.gov/newyork/press-releases/2012/man-pleads-guilty-in-new-york-to-conspiring-with-iranian-military-officials-to-assassinate-saudi-arabian-ambassador-to-the-united-states; US Department of Justice, "USA Vs. Mansour Arbabsiar & Gholam Shakuri," October 11, 2011, http://www.justice.gov/opa/documents/us-v-arbabsiar-shakuri-complaint.pdf.

46 Charlie Savage and Scott Shane, "Iranians Accused of a Plot to Kill Saudis` US Envoy," *The New York Times*, October 11, 2011, http://www.nytimes.com/2011/10/12/us/us-accuses-iranians-of-plotting-to-kill-saudi-envoy.html?ref=mansourjarbabsiar&_r=0; US Department of the Treasury, "Treasury Sanctions Five Individuals Tied to Iranian Plot to Assassinate the Saudi Arabian Ambassador to the United States," October 11, 2011, http://www.treasury.gov/press-center/press-releases/pages/tg1320.aspx.

47 US Department of Treasury, "Treasury Sanctions Five Individuals Tied to Iranian Plot to Assassinate the Saudi Arabian Ambassador to the United States," October 11, 2011, http://www.treasury.gov/press-center/press-releases/pages/tg1320.aspx.

48 James R. Clapper, *Worldwide Threat Assessment of the US Intelligence Community*, Office of the Director of National Intelligence, 2012, p. 5, http://www.intelligence.senate.gov/120131/clapper.pdf.

49 Michael A. Braun, "Iran, Hezbollah and the Threat to the Homeland," *Hearing Before the House of Representatives Committee on Homeland Security*, March 21, 2012, p. 2.

50 Gabi Siboni and Sami Kronenfeld, "Iran and Cyberspace Warfare," *Military and Strategic Affairs* 4, no. 3 (2012): http://www.inss.org.il.cdn.reblaze.com/upload/(FILE)1362314938.pdf.

51 Cohen, "Iranian Drug Ring Funding Terror?"

52 The prohibition on participating in the trade of banned substances is based on three binding treaties: The Single Convention on Narcotic Drugs (1961), The Convention on Psychotropic Substances (1971), and The United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (1988).

53 UN, *The United Nations Conference for the Adoption of a Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances*, 1988, http://www.unodc.org/pdf/convention_1988_en.pdf.

# Cyber Weapons and International Stability:
## New Destabilization Threats Require New Security Doctrines

**Guy-Philippe Goldstein**

Though cyberspace is a domain of strategic importance, cyber weapons have not yet been associated with publicly well-enunciated doctrines of use comparable to that of the nuclear age. Taking two very different approaches from the strategic literature—Jervis' security dilemma and Zagare & Kilgoure's perfect deterrence model—cyber weapons are demonstrated in both cases to induce a higher level of international instability. In particular, instability is favored by the attribution issue and the lack of clear thresholds. The outline of a cyber defense doctrine, focusing on the two mentioned informational issues, is then suggested.

**Keywords:** cyber weapons, deterrence, doctrine, security dilemma, perfect deterrence, attribution, thresholds, escalation

In 2013 cyberspace is a domain of strategic importance.[1] The threat of cyber attacks has been placed at the top of the list of national security risks in the "Intelligence Community Worldwide Threat Assessment of 2013,"[2] and computer network warfare is one of the only military areas in both the US and in NATO countries that is expected to grow.[3] Beginning in 2009, the United States Cyber Command, for example, was established as a unified command under the United States Strategic Command. As was stated quasi-officially by the *Wall Street Journal* in June 2011, computer sabotage that is generated in another country is sometimes considered

Guy-Philippe Goldstein MBA, HEC (France), is the author of *Babel Minute Zero*, a bestseller about international cyber warfare.

by the Pentagon as an act of war. In that sense, since the effects of cyber weaponry could be substantially vast, key decisions require direct approval from the US President, as they "should be unleashed only on the direct orders of the commander in chief."[4]

There is, however, no doctrine of use that is as clearly communicated as the doctrine of nuclear deterrence. First, many rules remain secretive and strictly in the realm of the highest echelon of the executive powers. Second, the domain itself is not clearly defined: it may be a in the war fighting domain,[5] or not.[6] Is cyberspace critical only because it is conducive to military assurance?[7] Or is it critical in its own right due to the increasing value of the data stored and protected in cyberspace? Finally, the development of a doctrine takes time and historical precedents. Though concepts of nuclear deterrence began emerging in 1946 following the works of Brodie,[8] Mutually Assured Destruction (MAD) did not come to the forefront before the late 1950s.[9] In the USSR, the nuclear strategy's "learning curve" was even less advanced.[10] Certainly, the field of cyber studies is still relatively young, and cyber weaponry in itself is constantly evolving in scale and scope.

The lack of a doctrine poses a significant problem because without the proper management framework—or doctrine of use in international relations—the introduction of any untested and disruptive technologies has the potential to yield unexpected consequences. This is particularly true in the business of war. To rely solely on technological solutions without the context of a doctrine does not guarantee the preservation of the status quo. Stability during the Cold War was not assured by defensive techniques, such as efficient anti-ballistic missiles systems. Not only were these technological solutions elusive, but they were also not desirable in the preservation of the balance of terror at the heart of the MAD doctrine. Both conclusions led to the signing of the Anti Ballistic Missile (ABM) Treaty of 1972.[11]

That does not preclude the necessity of developing specific technologies, such as Submarine-Launched Ballistic Missiles (SLBM) that guarantee a capable and survivable second strike force, but they should espouse the logic of a doctrine in order to reinforce it. This is particularly true for cyberspace, whose nature and risks should indicate the necessity of such an effort. Although the topic is still relatively new, it is not an emerging issue anymore. More than 15 years have passed since the 1997 US Eligible

Receiver exercise, which triggered the first real concerns at the federal level with regard to cyber warfare.[12] In addition, the past five years were marked by several "cyber" episodes in international relations, from the Russian-Estonian cyber guerilla wars of 2007[13] to the 2012 foreign attacks against Saudi Arabia's Aramco, possibly originating from Iran.[14] Sufficient examples of recent years can supply the first guidelines on these issues and doctrines. Moreover, the field can be approached by some of the more classical legal and political frameworks. Though attention must be paid to the specificities of the domain, there are many examples that could be a baseline for the establishment of such doctrine. A recent study that could be used for the writing of such doctrine is the *Tallinn Manual on International Law Applicable to Cyber Warfare*, which managed to apply legal precedents to cyber warfare situations.[15] Following this example, the article will apply frameworks from the "classical" strategic literature in a more formal way to assess the risks cyber weapons pose to international stability and also identify the very core issues of cyber defense that must be addressed by future doctrines.

## The Nature and Current Risks of Cyberspace

### *The Nature of Cyberspace*

The definition of cyberspace has been debated extensively. The focus was usually given to the technological components (e.g., electromagnetic spectrum, information-communication technologies, and so on).[16] In this article I suggest a complementary view that asserts cyberspace is currently the name for all information systems that are based on digital data. An analog electro-magnetic radio, for example, is not considered a part of cyberspace as it does not know how to "speak digitally." A DNA computer, however, is conversant in digital data and is therefore a part of cyberspace, as is an electro-magnetic tape, which is encoded in digital data even though it is played in an analog tape recorder.

Digital information is the language humans have created to communicate with machines, which dates back to the Industrial Revolution and the invention of the Jacquard loom (1801), when the rising complexity of new machines required the creation of such a language. It took nearly two centuries for the language to spread among other machines, especially after the inventions of Turing machine computers and the internet protocol. By nature, this language consists of three components: hardware (including

telecommunication equipment), software (including data exchange protocols), and "brainware," the human component that takes part of the data transmission by constituting very vulnerable interception points[17] and by writing code. Some of the most dangerous weapons in cyberspace today are, in fact, the codes produced by talented hackers. Functionally, cyberspace can be split into two: the physical support that materially affects communication and calculation, and the semantic domain that transforms physical support actions into data or instructions, providing them with meaning and controlling its own physical support.

This simplified description of cyberspace explains the current urgency to define the conditions for cyber defense and sheds light on the most critical pain points in cyberspace.

First, the distinction between digital and analog data makes clear why cyber warfare has become a strategic topic only in recent years. Although computers have been in use since the end of World War II, in 1986, digital data comprised only 0.6 percent of global data for storage, communications, and broadcasting, increasing to 24 percent in 2000. It exploded in 2007, however, reaching 93 percent, while "old" analog information capabilities became noncritical.[18] By the second half of the 2000s, information systems—what is usually most critical to any institution or organism—was fully transferred into the digital format. This may explain why the number of cyber attack episodes increased in frequency and gravity over the last few years. Civilization, including warfare, has turned digital. To use the words of Marc Andreessen, "Software has eaten the world."[19]

Second, the semantic dimension highlights and reflects the heart of networked information systems. The objective of ARPAnet, the ancestor of the internet, was to "emphasize robustness and survivability, including the capability to withstand losses of large portions of the underlying networks."[20] Packet switching networks are designed to withstand material hardware degradation. In cyberspace, the most severe damages are obtained when data are corrupted and their meaning manipulated, as was evident in "Operation Orchard"[21] and Stuxnet. In both cases, a maximum effect was obtained because human controllers were manipulated by corrupted command and control systems. In addition, the corruption of the industrial controllers that set the speed of rotors in P-1 centrifuges increased the level of sabotage.[22]

***Characteristics of Cyber Attacks in Brief***

In ancient Greece, the term *logos* equally signified the uttered word, the sentence, the direct meaning, and the higher level of ideas expressed.[23] It was a confused but rich definition, which also led to the development of the first hackers, the sophists, who manipulated words and syntax in order to corrupt meaning. What we call cyberspace today is, essentially, a digitalized *logos*, i.e., the language designed to communicate with machines on anything from physical support through immediate semantic translation of ordering machines or humans, and to Gibson's "consensual hallucination."[24] In this digital form of *logos*, modern sophists act like *The Sorcerer's Apprentice* of Paul Dukas: the code alters the man-made environment of machines, which causes the machines to alter the physical world by believing wrong arguments or instructions. In that sense, the quality of the attack depends first and foremost on the talent of the wizards.

The flaws used by offensive cyber weapons were developed either mistakenly or purposefully during the production stage of the equipment[25] or code or during their human handling, and were then exploited for further actions. To more precisely assess the attack's impact in the physical world, cyber warriors created models to test attacks.[26] Cyber weapons can also be designed to hide their signature and origin.[27] These characteristics give an asymmetrical advantage to the attacker once a flaw (or "exploit") has been found: only the attacker knows what the exploit is and the identity of the attacker. Since cyberspace is continuously updated by software upgrades, however, the cyber physical environment changes constantly as well, which makes the potency of exploits limited and transient: searching or manufacturing exploits requires permanent efforts.

The effects of these attacks occur as soon as the machines receive the message—the code strikes at "zero day," and their range is extremely large due to the wide use of digital-speaking machines: from espionage (penetration of machines that store information) and economic sabotage (penetration or corruption of machines storing financial values or IP addresses) to physical sabotage (attacks against machines that control and command all sorts of civilian industrial processes or weapon systems ranging from the tactical to the strategic). Because "software has eaten the world" and continues to do so, there are no potential limits to what can be attacked, and these effects have a psychological component as well. While equipment that was damaged by a kinetic attack must be replaced,

equipment that was harmed by a cyber attack might appear to operate properly but doubts regarding its capabilities will remain permanently.

## Geopolitical Instability Induced by Cyber Weaponry

### *Pro-Offense and Speed*

The pro-offense, rapid, and possibly large extent of the effects mentioned above and their potential characteristics creates a military technological environment that is tilting toward the rupture of the status quo. Rober Jervis' seminal analysis on the offense-defense theory stresses that the terms of the security dilemma rely on two crucial variables: "whether defensive weapons and policies can be distinguished from offensive ones, and whether the defense or the offense has the advantage."[28] Combining these two variables to create four possible worlds, Jervis states that world powers will have the greatest difficulties in maintaining the status quo in a reality where "offensive posture is not distinguishable from [the defensive] one" and where "the offense has the advantage." Here, beliefs are as powerful as technology. For example, World War I was the product of such a world, which was termed "doubly dangerous": the technologies of machine guns and railroads gave the defense an advantage,[29] but because of Bismarck's quick victories in the preceding decades, great powers believed that military technologies were still yielding an advantage to offense.[30]

The parallelism with a military environment shaped and dominated by cyber weaponry should be obvious. First, there is a widespread belief that cyber weapons give an advantage to the offense,[31] which may lie in the perceived asymmetry of information between offense and defense. By definition, the defense ignores the existence of the flaw before it materializes, but when it does, correcting it may be too late. This argument may need to be refined and further examined, as the advantage given to the offense could be limited and transient in reality, but it is immaterial to the application of Jervis' model. As with Europe following Bismarck's victories, what matters is the belief expressed by the general consensus. Second, cyber weapons cannot be monitored, as one can hardly distinguish between offensive and defensive capabilities. Dual doctrines of use, including those of defensive and offensive uses, have been drafted in China and in major Western countries.[32] Core capabilities include assets that when examined from afar can be construed for defensive or offensive use, like IT infrastructure or code writers. Currently in cyber weaponry,

there are no equivalents to Salt II's "observable differences" used to single out bombers carrying long-range Air-launched Cruise Missiles (ALCMs).[33] Defensive capability development itself is hardly distinguishable from offensive capability development since it stems in large parts from Red-Team exercises.[34]

The "doubly dangerous" risks could also be exacerbated by a rapid offense, used in a first strike. Such a "bolt from the blue" attack would be so decisive it would preempt any reactions from the defender. In an initial analysis of mutual deterrence games, Zagare showed that the fewer moves there are in a game, the more harm would be made to the status quo.[35] The incentive to strike first is shared by peer powers that are at about the same level of technological development. In that case, the perception that the attack is of equal risk to both sides would lead to Schelling's "reciprocal fear of surprise attack."[36] As Schelling writes, "Military technology that puts a premium on haste in a crisis puts a premium on war itself... If the weapons can act instantaneously by the flip of a switch, a 'go' signal, and can arrive virtually without warning to do decisive damage, the outcome of the crisis depends simply on who first finds the suspense unbearable."[37]

These lines were written a few years before ARPAnet was even established. They are echoed in the writing of US Air Force officers on war in the Information Age, stating that "preemptive employment of force may become a prerequisite for success."[38]

The dynamics leading to a conflict are also exacerbated by the ongoing technological investment in R&D cyber weaponry. The impetus for further investment is fed by the branching out of cyberspace into additional domains of civilian and military life and the need to protect these new realms of cyberspace. Since defense and offense R&D capabilities are hard to distinguish, this naturally triggers an arms race. Cyberspace's internal rate of the conversion of offline processes conversion into online ones is not always controlled by the military. Different from other revolutions in military affairs that were driven by actual contests, the thrust for digitalization of the US military continued at a high pace after the collapse of the USSR.[39] This may have been the result of the manifestation of the autonomous dynamics of digital data and software as they continue to "eat" the military. In this case, it is the qualitative evolution of technology itself that can also disrupt the status quo stability. As noted by Kissinger, countries that are opposing one another live in fear that their "survival

may be jeopardized by a technological breakthrough on the part of [their] opponent[s]."[40] As stated by Joynt & Corbett, the rate of change creates an "intrinsic uncertainty about advancing technologies…{as they] cannot supply the sufficient conditions for stable deterrence."[41] Indeed, as a regional example, Horowitz notes that the cyber arms race in East Asia fuels instability.[42] Finally, beyond the growing scope of cyberspace's reach, the dynamic internal competition and constant upheaval of the IT industry generates an ongoing upgrade of cyberspace itself. These enhancements also constitute the sources of new alterations in the fabric of cyberspace and, thus, can generate new flaws. Independent from the political or military competition, this factor mechanically exacerbates the arms race.

### *Attribution and Thresholds*

In addition to the perception that the cyberspace environment is pro-offense and prone to haste and to the field's technological domain that is constantly changing, cyberspace is also characterized by the ability to wage attacks without a clear attribution or a clear identification of the thresholds at stake following the initial impact. These factors constitute additional triggers for instability.

The lack of signature (the attribution issue) gives an advantage to the offense. If attacked, the defender does not know against whom to retaliate. This impedes the defense because the defender is not able to strike a counter-blow that could stop or deter the attacker. Without a clear aggressor, the defender will also encounter difficulties in mobilizing diplomatic relations in order to organize counter-pressure. If the defender retaliates or elevates defense against the wrong party, it may actually isolate itself more or trigger international escalation.

Attribution is therefore not a trivial issue: in war games one of the very first questions asked by the player acting as the defending head of state concerns the attacker's identity.[43] To gain weight diplomatically, attribution needs to reach a high level of certainty. This is technically hard to obtain in a limited amount of time.[44] Potential aggressors can claim "plausible deniability" and neutralize the international audience, reducing the margins of maneuver for the defender. Attribution can be inferred from the international context,[45] but this would not equate producing an incontrovertible "smoking gun," which would be required for securing diplomatic and external military support, especially in the

context of the intelligence failures leading to the invasion of Iraq in 2003. Similarly, the international context could be muddied. Since the 1986 "BrainVirus" infection of digitally encoded floppy disks across the world prior to the web's existence,[46] most malware infections have been global in nature. All machines that speak the digital language are vulnerable to digital infections. Though Stuxnet is said to have targeted specific nuclear enrichment installations in Iran, it was also found in India, China, Russia, and the US.[47] That makes "plausible deniability" even easier for the attacker, which can portray itself as a victim among others.

Non-recognition of thresholds also clearly undermines stability. Schelling posits the importance of thresholds to articulate the "idiom of war."[48] For thresholds to efficiently structure the dialogue in the violent atmosphere of war, they need to possess "simplicity, reconcilability and conspicuousness,"[49] for example, the crossing of a river or a mountain, or the general mobilization of an army.

The question is all the more critical because each player's calculus depends on other players' "curve of credibility"[50]—i.e., the stakes that a country has invested in a conflict from its own volition or which was forced on it by its opponent. These stakes are delimited by the above mentioned thresholds. They are positioned within a hierarchical disposition that credibly organizes the perceived modus operandi of a government. The underlying sense of proportionality is related to the above-mentioned hierarchical disposition and is also the key to credibility. This, in turn, allows the violent dialogue to be controlled. If an error was created in understanding the opponent's curve of credibility, there is de facto a perceived "imbalance of resolve"[51]—potentially leading to the conflict's spiraling. The massive retaliation policy defined in the NSC-162/2 document, for example, was noted by William Kaufman as lacking credibility, as it was "out of character for the US" to implement it.[52] On the other hand, as identified by Frank Zagare and Marc Kilgour in their work on Perfect Deterrence Theory, the credibility of nuclear deterrence lies on the preference for retaliation over backing down.[53] This preference is assured by a capable threat (especially a survivable second strike force), but also on a rational calculus of retaliation, as this rational preference establishes credibility. If a nation's core population centers were hit, and the nation can retaliate and inflict a major cost to the aggressor, there is a high probability it will do so. Higher stakes change the pay-back calculus.

In this situation, if population centers were indeed destroyed, the state can more easily mobilize internal resources by way of national cohesion and consensus around revenge response. The option of a more forceful reaction becomes credible. Early in the nuclear age, Liddell Hart noted that "victims of aggression are driven by an uncontrollable impulse to hit back regardless of the consequences" and therefore an "aggressor may hesitate to employ atomic bombs" because of the likelihood of retaliation.[54]

Herein lies another difficulty with cyber attacks: they do not easily offer simple, recognizable, and conspicuous characterization in terms of thresholds. Would difficulties in online banking lead to financial panic or an economic disaster, and at what point would this occur? If the capital state of an attacked country had suffered a blackout, how many people would die after one day? When the Northeastern region of the US was struck by the blackout of 2003 that lasted more than 52 hours, the effects were surely not negligible but were also relatively minimal.[55] The evolution of the impact does not develop in a linear model. Difficulties are compounded by lack of precedents in the use of constantly evolving weaponry. A foreign force invading another nation's airspace is considered a breach of sovereignty, but what about cyber attacks of foreign countries that repeatedly corrupt servers used by national companies? Finally, effects may be caused by indirect and psychological actions; for example, by instilling doubts on the safe use of military or industrial capabilities, cyber weapon may induce paralysis but not directly provoke it. Is it the same when the paralysis is the consequence of a direct kinetic hit?

The consequences of lack of attribution and clear thresholds on stability can be analyzed through Perfect Deterrence Theory,[56] which posits that for a threat to be deterrent, it must be capable of creating significant pain to the threatened party so that it would prefer not to suffer from it. The threat must also be credible, as the threatening party must be perceived as preferring to use the threat rather than backing down. Without signature, however, the deterrent threat is not viable anymore, as the defending party does not know against whom to retaliate, and the secret offender is not threatened. The defender may also not be credible if it threatens to hurt everything and everyone in response to attacks of unknown origins. Similarly, even if attribution is realized but the effects are hard to measure and the distinctive thresholds at risks cannot be identified, the retaliation will not be "in kind," rather either too hard or too weak.

At a macro level, it is coherent with strategic literature that asymmetry or gaps in the information available to each party would lead to conflict. Spiraling is being modeled as triggered by errors of appreciation, or as Zagare and Marc Kilgour put it, "strategic uncertainty and unanticipated response, and both may be broadly construed as mistakes traceable to an intelligence failure, bureaucratic bungling, miscalculation, or some other cognitive or information-gathering deficiency."[57] The risks of spiraling are higher if countries retaliate against attacks that aim to create false information in the opponent's system. War can also be seen as a process that resolves an information problem: how much harm can a nation do to its opponent?[58] Resolving this question establishes a hierarchy among nations, which serves as an ordered bargaining system that is understood by all. These explanations show why war is much more probable when the two countries facing each other are of the same strength rather than when they are not, in which case the outcome would be obvious.[59] Cyber warfare's modus operandi, however, is to create confusion in data. This mode of action threatens to corrupt strategic information, create uncertainty, and pose risks that would upset the status quo.

The absence of large scale demonstration of cyber attacks has been one of the factors limiting the risk of spiraling. The capability to damage this type of weaponry is not as clearly assured as that of a kinetic or a nuclear weapon. However, both the potency of the Stuxnet worm and the understanding that "software is eating the world" have left major global powers more prone to the risks of this new class of weapons. Perceptions are transforming following changes on the ground and public declarations. The psychological frames at play, according to Jervis and Perfect Deterrence Theory, become applicable to a geopolitical environment that is under stronger influence of cyber weaponry.

## Conclusion: The Need for "Escalation Control" Doctrines in Cyber Defense

There are no reasons to believe that "the diplomacy of violence"[60]—a term coined by Schelling to evoke the phenomenon of warfare—is going to vanish with the immersion of our civilization into cyberspace. Similarly, during the internet bubble of the 1990s, Michael Porter demonstrated that although the internet's "new economy" may emphasize types of cost advantages over others in the search for competitive differentiation,[61] it would still

not suspend the old rules of strategy. Instead, the winners would be the ones who are able to "view the Internet as a complement to, not a cannibal of, traditional ways of competing."[62] Furthermore, the "power to hurt" is fully embodied in cyberspace, but does not supersede the laws of strategy. Cyber power can be analyzed through the classical dimensions of strategy, as elucidated by John Sheldon, Michael Howard and Colin S. Gray.[63]

New technologies do not eliminate the risks of spiraling in warfare. Instead, this depends on the effects of any technology that triggers general warfare—effects such as the perception that strategic military capabilities lean towards the offense; the possibility that defensive military capabilities could also be used by the offense; the rapid mode of action that would shorten the length of the military "game"; or the perception that quick technological change has the potential to reshuffle the balance of military forces. The strength of these factors ends up affecting the threat capability and credibility of each player, and thus alters the underlying deterrence relationship between the players. Ultimately, the deterrence balance can be summed up as an informational problem: does the party accurately recognize its enemy's capabilities and those of itself? Does the party have a good sense of its intentions and red lines, and are they clear to its enemy?

On all these accounts, and especially because of the corruption of data and strategic information, cyber weapons increase the risk of informational errors whereby a crisis escalates into overall warfare. In particular, the above discussion on lack of attribution and clear thresholds explains why this risk is so well materialized with the use of cyber weapons. Furthermore, the solution for both issues is rendered even more pressing due to the nature of a game, which becomes shorter by an innately speed-of-light technology that is perceived as pro-offense. All this shows how pressing the need is for a doctrine to manage this informational crisis. Thus, a doctrine for cyber stability will not be based solely on the capabilities for reprisal, such as a demonstrable, survivable second strike force at the heart of nuclear deterrence, but just as importantly, it would also be based on the capabilities for elucidation at the strategic level. If the truth about attribution and damage assessment cannot be established, then the defending party is at risk of either conceding defeat to an unknown attacker, or of engaging in reprisals "in the dark" with a high risk of spiraling. On the other hand, if the truth is fully established in the "brainware" of the strategic decision makers—if not in the whole of the software and hardware

systems of the defending nation—then at least the defender can unlock all of its other traditional options from diplomatic to strategic threats in order to credibly force the offender to back down. The parallels with the truth-seeking objectives of intelligence services should not be surprising: if in cyber, as in intelligence, "the truth shall make you free,"[64] then it is partially due to the fact that both fields operate in information domains, with one based in the digital format and the other on "secrecy."[65]

The outline of such cyber defense doctrines could resemble that of elucidation actions like counter-intelligence or police investigations, but it must be strategically led by the head of state. These investigations would be supported by strong technical capabilities and operated by state-of-the-art methodologies aimed at truth-seeking from deductive testing for attribution to systems simulation for red-lines assessment. They would also have a strong diplomatic component, leveraging some circles of very close cooperation. The establishment of the truth cannot be dictated by one center. It consists of a social process based on either the sharing of the data supporting the conclusions, carefully taking into account the constraints posed by the intelligence context, or the ability to replicate experiments.[66] In that respect, military defense doctrines in cyberspace are somewhat parallel to the disciplined, scientific approach to problem solving that has been taken recently by the management of corporations from marketing[67] to human resources.[68] To attain the highest ground in an informational domain is to reach for the truth.

## Notes

1 This article explores the strategic risks of cyber weapons and the need to develop specific doctrines for cyber defense in order to offset the risk of out-of-control crisis escalation. To detail such doctrines would go beyond the scope of the current article. The author will explore some of the doctrinal solutions to the stability problems exposed here in an upcoming article.

2 Luis Martinez, "Intel Heads Now Fear Cyber Attack More than Terror," *ABCNews*, March 13, 2013, http://abcnews.go.com/Blotter/intel-heads-now-fear-cyber attack-terror/story?id=18719593.

3 Despite austerity cuts, the UK's cyber security budget has been expected to grow by some £650m ($1.07bn) over the 2012-2015 period. In James Blitz, "Country Profile: UK Defences are Boosted to Fight e-Crime," *Financial Times*, June 2, 2011.

4 David E. Sanger and Thom Shanker, "Broad Powers Seen for Obama in Cyberstrikes," *New York Times*, February 3, 2012.

5 Keith B. Alexander, "Warfighting in Cyberspace," *Joint Forces Quarterly* 46, no. 3 (2007): 58-61.
6 Martin C. Libicki, "Cyberspace is Not a Warfighting Domain," *I/S: A Journal of Law and Policy for the Information Society* 8, no. 2 (2012): 325-40.
7 Libicki, "Cyberspace is Not a Warfighting Domain."
8 Bernard Brodie, "The Development of Nuclear Strategy," *International Security* 2, no. 4 (1978): 65-83.
9 Lawrence Freedman, *The Evolution of Nuclear Strategy* (New York: Palgrave Macmillan, 2003), pp. 234-36.
10 Freedman, *The Evolution of Nuclear Strategy*, pp. 243-44.
11 See for example Freedman, *The Evolution of Nuclear Strategy*, p. 338.
12 See PBS interview with former Deputy Secretary of Defense John Hamre in Michael Kirk, "Cyberwar!" *PBS*, April 24, 2003, http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/interviews/hamre.html.
13 See BBC World Service, "Estonia Hit by 'Moscow Cyber War," *BBC News*, May 17, 2007, http://news.bbc.co.uk/2/hi/europe/6665145.stm.
14 See Nicole Perlroth, "In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back," *New York Times*, October 23, 2012.
15 Michael N. Schmitt, gen. ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare* (New York: Cambridge University Press, 2013).
16 See Daniel T. Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," in *Cyberpower and National Security*, eds. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, D.C.: National Defense University Press, 2009), pp. 26-28.
17 Human errors in security configurations have been also identified as "responsible for 80% of Air Force vulnerabilities," in James A. Lewis, ed., *Securing Cyberspace for the 44th Presidency* (Center for Strategic and International Studies, 2008), p. 55. The rise of social engineering and phishing attacks has accentuated the importance of the "human factor" in cyber security. - It's not a quote—it's an expression. Kevin Mandia notes, "While previous generations of attacks targeted technology such as networks and servers and exploited vulnerabilities in software, attackers have now evolved to target human inadequacies and weaknesses." Kevin Mandia, "Cyber Threats and Ongoing Efforts to Protect the Nation," *Permanent Select Committee on Intelligence, US House of Representatives*, October 4, 2011.
18 Martin Hilbert and Priscila Lopez, "The World's Technological Capacity to Store, Communicate and Compute Information," *Science* 332, no. 6025 (2011): 60-65.
19 Marc Andreessen, "Why Software is Eating the World,"*Wall Street Journal*, August 20, 2011.
20 Barry M. Leiner, Vinton G. Cerf, David D. Clark, Robert E. Kahn, Leonard Kleinrock, Daniel C. Lynch, Jon Postel, Larry G. Roberts, and Stephen

Wolff, *A Brief History of the Internet* (The Internet Society, 2012), http://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet.

21 See David A. Fulghum, "Why Syria's Air Defenses Failed to Detect Israelis," *Aviation Week & Space Technology*, October 3, 2007, and David A. Fulghum, "Israel Used Electronic Attack in Air Strike against Syrian Mystery Target," *Aviation Week & Space Technology*, October 8, 2007.

22 See Nicolas Falliere, Liam O Murchu ,and Eric Chien, *W32. Stuxnet Dossier* (Symantec, 2010).

23 Barbara Cassin, CNRS, "Logos et Polis: La Force du Discours," in Catherine Golliau ed., *La Sagesse Grecque* (Paris: Le Point Référence, 2011), pp. 41-43.

24 William Gibson, *Neuromancer* (New York: Ace Science Fiction, 1984).

25 See the issue of kill switch in chips in Sally Adlee, "The Hunt for the Kill Switch," *IEEE Spectrum*, May 1, 2008.

26 For example, according to David Sanger, when Israel and the US developed a "bug" to derail nuclear enrichment operations at the Natanz plant in Iran, research teams "began building replicas of Iran's P-1 centrifuges" since "the bug needed to be tested." See David E. Sanger, "Obama Order Sped Up Wave of Cyberattacks against Iran," *New York Times*, June 1, 2012. In particular, the Dimona complex in Israel may serve as a testing ground for cyber attacks of centrifuges—see William J. Broad, John Markoff, and David E. Sanger, "Israeli Test on Worm Called Crucial in Iran Nuclear Delay," *New York Times*, January 15, 2011.

27 The issue of cyber attacks attribution is a major difficulty explored in fiction—see for example, Guy-Philippe Goldstein, *Babel Minute Zero* (Paris: Denoel, 2007—and illustrated in real life episodes such as the cyber attacks against Estonia in 2007. See Mikko Hypponen,"9thof May," *F-Secure Weblog*, February 15, 2010, http://www.f-secure.com/weblog/archives/archive-052007.html.

28 Robert Jervis, "The Security Dilemma," *World Politics* 30, no. 2 (1978), p. 187.

29 See a detailed discussion in Charles L. Glaser and Chaim Kaufmann, "What is the Offense-Defense Balance and Can We Measure It?" *International Security* 22, no. 4 (1998): 44-82.

30 Robert Jervis, "The Security Dilemma," p. 190.

31 In 2009, Gregory J. Rattray highlights the "offense dominance" in Cyberspace - see Gregory J. Rattray, "An Environmental Approach to Understanding Cyberpower," in *Cyberpower and National Security*, eds. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, D.C.: National Defense University Press, 2009), pp. 253-74. Three years later, David T. Fahrenkrug from the Office of Net Assessment / Office of the Secretary of Defense, notes that "Current accepted wisdom in cyberspace is that the attacker has the decisive advantage" - in David T. Fahrenkrug, *Countering the Offensive Advantage in Cyberspace: An Integrated Defensive Strategy*, 4th International Conference on Cyber Conflict (Tallinn: NATO CCD COE Publications, 2012).

32 New military development programs announced in 2012 for both DARPA and the US Air Force indicate- a clear interest in offensive weaponry. See Tom Gjelten, "First Strike: US Cyber Warriors Seize the Offensive," *World Affairs*, January/February 2013; additionally, in March 2013, "General Keith Alexander, who heads the US National Security Agency and Cyber Command, told lawmakers Tuesday that the military is creating at least 13 units which would have offensive capabilities in cyberspace." in "Obama Calls China Cyber Attacks 'State Sponsored,'" *News Wires*, March 13, 2013. In France, the project for the 2013 "Livre Blanc" mentions the need for LIO, aka "Lutte Informatique Offensive" or Offensive Cyber Warfare—in Vincent Lamigeon, "Livre Blanc de la Defense: Les 5 Nouvelles Priorités Imposes à l'armée Francaise," *Challenges*, April 29, 2013.

33 See Thomas K. Longstreth and Richard A. Scribner, "Verifications of Limits on Air Launched Cruise Missiles," in Frank von Hippel and Roald Z. Sagdeev, eds., *Reversing the Arms Race: How to Achieve and Verify Deep Reductions in the Nuclear Arsenals* (New York: Gordon and Breach, 1990), p. 185

34 For a very short US overview, see Zachary Fryer-Biggs, "Building Better Cyber Red Teams," *Defense News*, June 14, 2012.

35 Frank C. Zagare, *The Dynamics of Deterrence* (Chicago: University of Chicago Press, 1987), pp. 48-56—see discussion on rules relaxation and lengthening the game.

36 See Chap. IX, "The Reciprocal Fear of Surprise Attack," in Thomas C. Schelling, *The Strategy of Conflict* (Harvard University Press, 1960).

37 Thomas C. Schelling, *Arms and Influence* (New Haven: Yale University Press, 1966), p. 225.

38 See David S. Fadok, Major, USAF, *John Boyd and John Warden: Air Power's Quest for Strategic Paralysis* (Maxwell Air Force Base: School of Advanced Air Power Studies, 1995), p. 49. One year earlier, John Warden stated already that "Capturing and exploiting the datasphere may well be the most important effort in many future wars." The conquest of "datasphere" is implicitly defined as a priority for military success. See Col. John A. Warden III, USAF, "Air Theory for the Twenty-first Century," in *Challenge and Response: Anticipating U.S. Military Security Concerns*, ed. Karl P. Magyar (Maxwell AFB, Ala.: Air University Press, 1994)

39 See Keith L. Shimko, *The Iraq Wars and America's Military Revolution* (New York: Cambridge University Press, 2010), p. 129.

40 Henry Kissinger, "Arms Control, Inspection and Surprise Attack," *Foreign Affairs* 38, no.4 (1960): 557-75.

41 Carey B. Joynt and Percy E. Corbett, *Theory and Reality in World Politics* (London: Macmillan Press, 1978), pp. 92-93.

42 Michael Horowitz, "Information Age Weaponry and the Future Shape of Security in East Asia," *Global Asia* 6, no. 2 (2011).

43 On the issue of US Defense officials publicly struggling with the issue of attribution, see John Markoff, David E. Sanger, and Thom Shanker, "In Digital Combat, U.S. Finds No Easy Deterrent," *New York Times*, January 26, 2010; David E. Sanger and Elisabeth Bumiller, "Pentagon to Consider Cyberattacks Acts of War," *New York Times*, May 31, 2011.

44 In a recent example, after facing a simultaneous shutdown of computer networks at several major broadcasters and banks on March 20, 2013, South Korea first said that cyber attacks came from China, in Warwick Ashford, "South Korea Says Cyber Attack Came from IP Address in China," *Computer Weekly*, March 21,2013. South Korea publicly admitted a mistake the next day. See Warwick Ashford, "South Korea Admits Mistake in Linking Cyber Attacks to China," *Computer Weekly*, March 22, 2013. Three weeks later, South Korea accused North Korea. See Warwick Ashford, "South Korea Accuses North Korea of Launching Cyber Attacks," *Computer Weekly*, April 11, 2013.

45 For a thesis minimizing the "attribution problem" by analysis of the international context, see Richard L. Kugler, "Deterrence of Cyber Attacks," in *Cyberpower and National Security*, eds. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington D.C.: National Defense University Press, 2009), pp. 309-42.

46 Rupert Goodwins, "Ten Computer Viruses that Changed the World," *ZDNet*, August 3, 2011.

47 Nicolas Falliere, Liam O. Murchu, and Eric Chien, *W32. Stuxnet Dossier* (Symantec, 2010), p. 6 and "Chinese infections in Stuxnet 'Cyber Superweapon' Moves to China," *AFP*, September 30, 2010.

48 Schelling, *Arms and Influence*, p. 135: "Finite steps in the enlargement of a war or a change in participation. They are conventional stopping places or dividing lines. They have a legalistic quality, and they depend on precedents or analogy. They have some quality that makes them recognizable, and they are somewhat arbitrary....We don't make them or invent them, but only recognize them....Apparently, any kind of restrained conflict needs a distinctive restraint that can be recognized by both sides, conspicuous stopping places, conventions and precedents to indicate what is within bounds and what is out of bounds, ways of distinguishing new initiatives from just more of the same activity."

49 Schelling, *Arms and Influence*, p. 137.

50 See Carey B. Joynt and Percey E. Corbett, *Theory and Reality in World Politics* (Pittsburgh: University of Pittsburgh Press, 1978), pp. 94-95.

51 See Frank C. Zagare and D. Marc Kilgour, *Perfect Deterrence* (Cambridge: Cambridge Studies in International Relations, 2000), p. 301.

52 See Freedman, *The Evolution of Nuclear Strategy*, pp. 96, citing William Kaufman, *Military Policy and National Security* (Princeton University Press, 1956), p.21, 24-25.

53 Frank C. Zagare and D. Marc Kilgour, *Perfect Deterrence*, chapter 3.

54 See Freedman, *The Evolution of Nuclear Strategy*, p. 40 citing B. M. Liddell Hart, *The Revolution in Warfare* (London: Faber and Faber, 1946) pp. 85-86.

55 In New York City, during the blackout, there were significant increases in respiratory, cardiac, and other EMS calls. See Gary Kalkut, MD, MPH, "Effects of the August 2003 Blackout on the New York City Healthcare Delivery System: A Lesson for Disaster Preparedness," *Critical Care Medicine* 33, no. 1 (2005), pp. S96-S101. Reports by the press, as cited on Wikipedia, accounts for 11 indirect fatalities (http://en.wikipedia.org/wiki/Northeast_Blackout_of_2003); however, a further study indicates that "there was minimal morbidity and mortality reported that could be attributed to the event." See J. Kile, S. Skowronski, M.D. Miller, S.G. Reissman, V. Balaban, R.W. Klomp, D.B. Reissman, H.M. Mainzer, A.L. Dannenberg, "Impact of 2003 Power Outages on Public Health and Emergency Response," *Pre-hospital and Disaster Medicine* 20, no. 2 (2005): 93-97. The estimates of total costs in the United States range between $4 billion and $10 billion US dollars, or less than 0.1% of US GDP. sSee U.S.-Canada Power System Outage Task Force, *Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations* (2004), p.1.

56 See Zagare, and Kilgour, *Perfect Deterrence*.

57 Zagare and Kilgour, *Perfect Deterrence*, p. 302.

58 Put differently, if states knew the outcome of a possible war and had perfect information on each other's capabilities and resolve, they would probably avoid war. See James D. Fearon, "Rationalist Explanations for War," *International Organization* 49, no. 3 (1995): 379-414 and Dan Reiter, "Exploring the Bargaining Model of War," *Perspective on Politics* 1, no.1 (2003): 27-43.

59 See empirical analysis in Stephen L. Quackenbush, "General Deterrence and International Conflict: Testing Perfect Deterrence Theory," *International Interactions* 36, no. 1 (2010): 1-26.

60 Schelling, *Arms and Influence*, chapter 1.

61 See Michael Porter, "Strategy and the Internet," *Harvard Business Review*, March 2001.

62 See Porter, "Strategy and the Internet."

63 John B. Sheldon, "The Dimensions of Strategy for Conceptualizing Cyberpower: Laying the Foundations for Sensible Cyber Security Policy and Doctrine," presented to the panel on "Comparative Cyber Security Strategies: Theory and Practice," International Studies Association Conference, San Diego, 2012.

64 Extract from the Gospel according to St. John, initially inscribed on the CIA building's facade. See https://www.cia.gov/news-information/featured-story-archive/ohb-50th-anniversary.html.

65 See for example Michael Warner, "Wanted: A Definition of Intelligence," *Studies in Intelligence* 46, no. 3 (2002), pp. 20-21.

66 Sharing of data is a core requirement for any submission to peer reviewed journals. See for example the recommendations for *Nature*: http://www.

nature.com/authors/policies/availability.html; Evidently, in intelligence matters, sharing must balance the gain from sharing with the risks of exposure for the source—what Director of National Intelligence (DNI) James R. Clapper has referred to the need to find the "sweet spot" between sharing and protecting information. See Remarks and Q & A by Director of National Intelligence, Mr. James Clapper, 2010 Geospatial Intelligence Symposium, New Orleans, Louisiana, November 2, 2010, quoted in Richard A. Best Jr., "Intelligence Information: Need-to-Know vs. Need-to-Share," *Congressional Research Services*, June 6, 2011.

67 See the impact of A/B Testing in management of Silicon Valley startup companies up to Google in Brian Christian, "The A/B Test: Inside the Technology That's Changing the Rules of Business," *Wired*, April 25, 2012.

68 See Steve Lohr, "Big Data, Trying to Build Better Workers," *New York Times*, April 20, 2013.

# Response Article
# Don't Terminate: Deter to Prevent

**Uri Rechav**

In "On Nuclear War: Deterrence, Escalation, and Control" (*Military and Strategic Affairs*, December 2012), Professor Stephen Cimbala discusses various reasons for the failure of nuclear deterrence and expresses doubts about deterrence for several reasons. These include decisions (by the target of deterrence) that are not based on cost-benefit analysis; irrationality; and misunderstandings. (In another section, he mentions the heightened nuclear alert in 1995 in Russia under Boris Yeltsin after the launch of a Norwegian research missile that had been planned and reported to the Russians in advance, but was believed to be an American missile because of a communications failure within Russia.)

In his discussion of failed nuclear deterrence, Professor Cimbala asks how to end a nuclear conflict that has started, i.e., how to nip a nuclear conflict in the bud. He recognizes the difficulties inherent in the discussion and admits that there is "intellectual resistance... based on the assumption that deterrence is undermined by a willingness to plan seriously for its possible failure." He illustrates what he sees as the need to terminate a nuclear war with the example of an Iranian strike on Israel or a Pakistani attack on India. On the one hand, he discusses the considerations of the state with a limited supply of nuclear weapons ("a nuclear armed Iran or Egypt"), and on the other, he notes that a state that has long had nuclear capability could initiate a nuclear strike no less than small states, whether they are rogue states or new members of the nuclear club. He questions the ability of leaders in states such as North Korea and Israel to maintain control over decisions on force employment, including on nuclear weapons.

Deterrence involves preventing incidents and developments, and therefore it is inherently full of paradoxes. In deterrence between two sides, there is a deterring party and a deterred party. There can also be mutual

deterrence between the two parties, with each of them playing the role of the deterring party and the deterred party. Deterrence is expressed in a declaration of intentions, be they threats or warnings. Party B declares to party A (and sometimes, to the entire world), "If you do such and such, I, party B, will repay you sevenfold. It is not worth it." Party B announces and demonstrates to party A and implicitly, to the entire world, its ability to strike back hard, even after it is struck or in the case of a surprise attack. In nuclear deterrence, the strikes are nuclear. The resolve of the deterring party and the value of the actions from which party A is deterred are the main parameters.

We saw an example of deterrence among three players (type II according to Herman Kahn) when then-US Secretary of State James Baker III warned Saddam Hussein not to use chemical weapons against Israel lest the United States turn Baghdad into a place that would not be inhabitable for 100 years. Iraq was deterred.

A party that is in fact deterred will not rush to declare this publicly. How, then, will we know? And in particular, how will the deterring party know? Even if the deterred party did indeed refrain from carrying out an action, perhaps it did not do so because it was deterred. Perhaps it had not intended to carry out the action in the first place. An example from criminal law is that the prohibition on pilfering exists even when we have no intention or plan at all to pilfer (for instance, an orange from an orchard).

Deterrence literature discusses in detail the differences and the relationship between the act and the retribution. There is a detailed discussion of the value of the act for the potentially deterred party. This value may be very high (such as, for example, for Iran—destroying Israel or turning it into a shadow of its former self). The scope of the retribution is also discussed. There is discussion of retribution (nuclear) so awful that the chances of its occurrence are ostensibly negatively affected. The expression "termination of a nuclear war" seems to me to belong to this category.

When deterrence has failed, things are clear. If there was deterrence—that is, before it failed, there was a warning in effect by the deterring party to the potentially deterred party that it should not carry out the act; there was a rule or law or threat in effect that if the potentially deterred party did not heed the warning, the deterring party would take retaliatory steps against it—and if the potentially deterred party did the deed in spite of the warning, then deterrence has failed, and anything that happens, whether retribution or not, belongs to another theory.

Herein lies the basic paradox of deterrence. Any party that wishes to deter must prepare very well for the possibility of "failure." The better prepared it is, the more it ensures that the deterrence will not fail. But when it has failed, this is another chapter that is not part of the doctrine. This is not only semantics: when we discuss a complicated hypothetical subject and exercises abaut what the other party thinks, it is very important to be precise and to impose a framework or at least a rigid title for each sub-section.

When there are several parties, as in the article by Professor Cimbala, the picture becomes much more complicated, and we must be even more careful. He begins with the possibilities between India and Pakistan, but my impression from his article is that he is talking mainly about other areas of the world, and that there is to steer clear of superficial discusssion.

I view Professor Cimbala's suggestion to terminate a nuclear conflict in its early stages as worrisome. Termination means giving a prize to the first attacker, the surprise attacker. If everyone knew that party C (the world) would terminate a nuclear conflict and not allow it to develop after a nuclear attack, the party attacked would not be allowed to retaliate against the attacker (whether the party attacked explicitly threatened to retaliate or the threat of retaliation was vague). To an attacker with intentions and plans, such a world is more convenient than a world in which each side is entitled to deter its adversary from aggression.

A world in which only one nuclear strike is "permitted" or is possible is a more dangerous world than a multi-nuclear world. In a nuclear conflict between two parties that differ significantly in size and power, this distinction is even more valid: the party that sees itself as stronger has a much more powerful incentive to be the aggressor, to launch a surprise attack feeling confident that the world will prevent the party attacked from launching a retaliatory nuclear strike against the aggressor (or will make it difficult to do so).

I believe that Cimbala's idea is extremely dangerous and should be kept in the field in which it was planted—the field of theoretical articles. Even from a purely theoretical point of view, it is better to prevent nuclear war in the world than to "terminate" it, and since in fact, as Cimbala himself writes, a discussion of "termination" could weaken deterrence, the discussion should be terminated and deterrence strengthened à la Baker: proven, reliable, determined, clear, and explicit, and many times stronger than the strength of the threat.

# Call for Papers

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

Articles may relate to the following issues:

- Military and strategic thinking
- Lessons learned from military organizations throughout the world
- Military force developments 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

Submitted articles should not exceed 6000 words (including citations and footnotes). Please include an abstract of 120 words and a list of up to 10 keywords. 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 Warfare Program
Tel: +972-3-6400400/ext. 488
Cell: +972-50-5772338
danielc@inss.org.il