Military and Strategic Affairs

Volume 8 | No. 1 | July 2016

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 8 | No. 1 | **July 2016**

CONTENTS

Military and **Strategic Affairs**

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

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

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

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

The Institute for National Security Studies (INSS)
40 Haim Levanon • POB 39950 • Tel Aviv 6997556 • Israel
Tel: +972-3-640-0400 • Fax: +972-3-744-7590 • E-mail: info@inss.org.il

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

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

Editor's Note

Dear Readers,

This year marks the eighth year of publication of the journal *Military and Strategic Affairs*. Over the years, we published articles that addressed diverse topics. With the evolution of knowledge of cyberspace and the increasing number of requests by readers and authors alike to engage in this topic, we began publishing articles addressing cyber technology, gradually expanding in number and scope in *Military and Strategic Affairs.*

At the Institute of National Security Studies, we have been encouraged by the evolving knowledge and burgeoning activities in the cyber sector both in Israel and across the globe. As a result, we have decided to shift the focus of the journal and to publish articles relating to the cyber sector. The name of the journal will be changed to *Cyber: Intelligence and Security*. Therefore, this edition will be the last edition of *Military and Strategic Affairs*.

Considering its new focus, the journal will invite authors and readers from diverse spheres involving the cyber sector, including those in policy and government, the military, intelligence, economics, law and, of course, those developing and providing cyber solutions, as well as the industries seeking such solutions. All of these are extremely important to developing knowledge and shaping the discourse about the cyber sector.

We at the Institute of National Security Studies hope that this shift in focus will be welcomed, so that we may continue to strengthen research in this critical field and stimulate informed public debate on the entire spectrum of activities in cyberspace.

Sincerely,
Gabi Siboni
Editor

The Challenges Facing the Israel Defense Forces, 2015–2016

Gadi Eisenkot

The challenges facing the Israel Defense (IDF) Forces (IDF) in the foreseeable future are composed of three main factors. The first is Israel's rapidly changing strategic environment. The nuclear deal between Iran and the superpowers and the subsequent lifting of the sanctions against Iran constitute a strategic turning point for the IDF's major threat over the past decade. The crumbling of the old order in the Middle East, existing since the Sykes-Picot Agreement of 1916, as well as the weakening of the state framework over the past four to five years illustrate the region's instability, which will continue to characterize it for many years to come. In addition, the phenomenon of the Islamic State and global jihad has become a major moving force in the Middle East. The IDF's General Staff began discussing this challenge in late 2013 and early 2014, and since then it has continued to develop.

The conflict in our region between Sunnis and Shi'ites, which has found expression recently in the conflict between Iran and Saudi Arabia, is actually a reflection of the struggle over the superpowers' involvement in the Middle East. The Soviet Union had been involved with the Arab states that surround Israel until the Yom Kippur War. The United States operated for a brief time in Lebanon in 1958 and again in 1983. Currently, both superpowers are active in the region as part of an ongoing operation to defeat the Islamic State — an event of great significance for the State of Israel and for the IDF.

The second factor that influences the IDF's capabilities and the use of force over the short term is the operative environment in which it works. Over the past decade, we have learned from experience how tactical incidents

This essay is an edited transcript of the chief of staff's speech at the annual conference of the Institute for National Security Studies in January 2016.

develop into battle and even into war. The events in Syria; the explosives that Hezbollah plants along the roadside on Mount Dov; the explosives used against the IDF in the Gaza Strip; and the wave of terrorism of recent months make us realize all the more how narrow the space is between tactics and strategy, and how tactical incidents are liable to develop into events that have strategic significance for the State of Israel. After a decade-long lull in suicide terrorism, which until 2005 claimed the lives of 1,178 civilians and soldiers and wounded more than 15,000 people, we have been facing a renewed escalation of terror over the past several months.

The IDF's mission for the long term is to build up its strength and adapt it to the challenges of the future. It must do so with the understanding that the IDF could be put to the test within a very brief time frame, and that the challenges it will encounter in another decade will be even more complex than the already difficult ones of today. Still, the considerable dangers contain opportunities as well.

The third factor is the internal social environment in the State of Israel and the wish to change national priorities. The phenomenon, which began in the summer of 2011 with the slogan "The people demand social justice," expressed a desire to direct resources to needs other than security. Israelis have expressed this wish daily in discussions about the cost of security within the financial pages of every national newspaper, as well as in a number of violent instances. This wish was also manifested by the establishment of a committee to examine how priorities could be changed and the costs of security reduced.

One consequence of this phenomenon is that the IDF operates without a multi-year plan. It is difficult to optimize security and the military without a well-organized and well-reasoned plan, which facilitates the development of the IDF's strength, existence, preparedness, human resources, and other components of the army's work. The past four years were characterized by a defense budget that had a shortfall of five to eight billion shekels between the base budget and the actual expenditure at the end of the year. This situation harmed the IDF's ability to optimize security, stay within the planned budget, and gain the public's trust. Fortunately, this situation was avoided this year, to the benefit of the State of Israel and its security.

The Strategic Changes

The major threat that forms the IDF's main mission since late 2005 has been Iran. The nuclear deal between Iran and the West is definitely a strategic

turning point. It constitutes a significant change in the vector along which Iran has moved and has changed the way the IDF views the Iranian threat. The nuclear agreement harbors many risks, but it also presents opportunities.

The role of the IDF and its Chief of General Staff is, naturally, to look at the spectrum of risks and capabilities and judge the situation accordingly. Still, they must do so not by assuming the worst-case scenario, as making decisions according to such a scenario is just as dangerous as basing them on overly optimistic scenarios. The IDF is studying and assessing the situation in light of the strategic watershed marked by the nuclear agreement with Iran, its meanings, and its consequences for force build up and its employment.

We must deal with this issue in two different time frames. The first time frame is the next five years, with the assumption that during this period, Iran will undertake great efforts to fulfill its part of the deal in order to benefit from the advantages inherent in the agreement. The second time frame is the next fifteen years, during which Iran must be made a high priority; it must be made a target for tracking and monitoring to see whether it works through secret channels in order to fulfill its vision of acquiring nuclear weapons. The prevailing understanding and assumption in the IDF, as well as in other places, is that there has been a turning point and significant change in Iran, even though it has not shelved its aspirations to acquire nuclear capability in order to realize its self-perception as a regional power.

At the same time, the process that has been taking place over the last few years in the countries surrounding the State of Israel is expected to continue – an increased risk resulting from Iran's efforts to gain influence and hegemony in the region. Iran is conducting a war against Israel by proxy, the foremost being Hezbollah, which constitutes the gravest threat to the State of Israel. Hezbollah is a terrorist organization that has been equipped, funded, trained, and even led by the Iranians since 2006. Iran's involvement is also evident in Syria, where it provides not only financial and political support, but also practical military support; Iranian commanding officers are waging battles in Syria in which Iranian soldiers and Shi'ite militias take part. Iran is paying in blood for this involvement, as more than one hundred Iranians so far have been killed in battle in Syria, and hundreds more have been wounded.

In addition to supporting Syria and Hezbollah, Iran is investing substantial efforts in the Gaza Strip, as well as in attempts to influence Israeli Arabs. The assumption is that within one to two years, Iran will allocate a considerable

budget for use against Israel directly. Iran has significant capabilities, together with an advanced and developed military industry. So far, the Iranians have transferred between 800 million and one billion dollars per year to Hezbollah, and tens of millions of dollars annually to Hamas. It is estimated that as Iran's economic situation improves due to the lifting of the sanctions, Iran will direct greater resources towards the Middle East. Iran also works to transfer weapons to Hezbollah and Hamas, as was proved roughly a year ago when the IDF seized the cargo ship Klos-C, which was carrying an arms shipment on its way to the Gaza Strip.

Syria has undergone significant change in recent years. Approximately five years ago, I completed my term as head of the Northern Command, during which I saw battalions, divisions, brigades, and line regiments, forming a constant picture of the enemy who had logic and an obvious state target. When we walk around on the Golan Heights today and move on from the area where Israel's borders meet with Jordan and Syria from the south toward the Hermon region in the north, in the first few kilometers you can see, on the right, outposts of the Islamic State, which is known there as Shuhada al-Yarmuk. A deployment of the global jihad movement is visible further on. Farther north, in the Quneitra region, one can see Shi'ite militias, and in the northern Golan Heights one can see the Syrian army and Hezbollah troops. The situation along the Israeli-Syrian border has become, therefore, highly complex, and it changes frequently.

Over the past two years, a group that had never been on the IDF's agenda has taken over Syria – an organization that rose up and conquered very large swathes of Syrian territory. This group is the Islamic State. It is a military organization of sorts that has been joined by thousands of Arab Muslims from the Middle East, but also by thousands of people from western countries, including six hundred from Belgium and close to a thousand from France, as well as supporters from Britain, Australia, and even Israel. They undergo three to four weeks of basic training, after which they go out to fight against regular armies and even make meaningful gains. Despite the significant coalitions that are working against this phenomenon, the one that showed the most effective gains in 2014 and 2015 was the Islamic State, even though it is not a military force in the conventional sense and, unlike regular armies, does not operate airborne, naval, and ground forces and does not carry out organized attacks. Because of these characteristics, the Islamic State may be seen more as a phenomenon than as an organization.

In recent months, we can see a significant change in Syria. The success of the groups operating against Bashar Assad's regime has ceased and even has been rolled back in some locations. Still, it seems that the fight over Syria, which is also a struggle between the Shi'ites and the Sunnis, will continue for many years to come. Despite the involvement of the two superpowers, which are the key to operational successes and to reaching any agreement in the Syrian crisis, it is extremely difficult to gain real military accomplishments in battle. We can learn from Israel's experience in battle in the Gaza Strip and in Judea and Samaria that it takes a great deal of time to reach a situation in which it can be said that the war has been won, particularly when it is a war of terror. Israel began dealing with suicide terrorism in 2000, and it was only towards 2004 that Israel was able to establish that it had defeated terrorism and won. Achieving this goal required control over territory and population, excellent intelligence, and a great many troops on the ground. It looks as though the incidents and the fighting in Syria will continue for a long period of time, making a sustainable solution to the situation difficult to achieve. Even if the Islamic State and the global jihad movement should suffer a severe blow in Syria, we should assume that the fight against Salafist groups will continue there for many more years. As a rule, it will be very difficult to find an entity that will be able to effectively control Syria's territory and population.

The gains in the war against the Islamic State increase the likelihood that its operatives eventually will aim the barrels of their guns at Israel and Jordan too. This is both because of the strategic logic that guides their actions, according to which Israel and Jordan are linked together, and because the forces of the Islamic State and the global jihad movement are deployed in the border area between Israel and Jordan. So far, these forces have been maintaining their routine and have refrained from attacking the State of Israel.

If there is a place in the countries around the State of Israel where a quick defeat of the Islamic State is possible, it is in the Sinai Desert. A group affiliated with the Islamic State, known as Sinai Province, is operating in the Sinai Peninsula and numbers between six hundred and a thousand fighters. The Egyptian army controls the territory and the population in that area, making it very likely that it will make substantial gains against the group within a short period of time.

A highly disturbing and worrying phenomenon is the support in the Palestinian arena for the Islamic State. Groups of Salafists in the Gaza Strip

have carried out all of the rocket launches aimed at Israel over the past year and also tried to plant explosives to detonate against IDF troops in the area. These groups pose a challenge to Hamas and Islamic Jihad, which have not fired even a single rocket at Israel since Operation Protective Edge, and want to use rocket fire aimed at Israel to ignite the arena. Support for ideas of the Islamic State has also spread to Judea and Samaria. Recently published polls indicate that 13 to 16 percent of those polled in Judea and Samaria and the Gaza Strip back the Islamic State – a worrying statistic.

The Threats to Israel

The major threat currently facing the IDF is Hezbollah. This is a terrorist organization, which over several decades has built a simple strategic idea that challenges the superiority of the IDF's intelligence, as well as its aerial and ground warfare. They have deployed in 240 Shi'ite villages, cities, and towns throughout southern Lebanon and have established defense systems, high-trajectory and anti-tank fire, and command and control systems in each community in preparation for the day of reckoning. Hezbollah's main efforts at this time are to achieve precision-rocket capability, which has increased over the past decade from 10,000 rockets to close to 100,000 rockets. Still, the primary goal of Hezbollah and its head, Hassan Nasrallah, is to achieve Shi'ite hegemony in Lebanon.

This preparation by Hezbollah, and especially the fact that its troops are deployed within a civilian environment, is a significant challenge for the IDF since it limits the IDF's freedom of action. In addition, such deployment has been a restraining factor for Hezbollah and a major reason why the border between Israel and Lebanon has been quiet for the past decade, especially since Hezbollah is well aware of what a military escalation in southern Lebanon means for the area's inhabitants.

The reality in the border region with Lebanon has also changed vis-à-vis Israel's capabilities. Both the IDF's operational capability and, in particular, its intelligence capability have improved since 2006. Despite the bragging of Hezbollah's leaders in their weekly speeches, they know perfectly well that Israeli intelligence has infiltrated Hezbollah, and they are also aware of Israel's capability and power. Hezbollah perceives the IDF as a very strong and unpredictable army, and this fact also explains the quiet that has prevailed in the region over the past decade. Still, the capability that Hezbollah has acquired is disturbing, since it includes not only high-trajectory weapons, but also the ability to deploy ground forces.

Through its involvement in the fighting in Syria over the past two years, Hezbollah has gained experience in much larger operations than the ones it took part in and initiated in the past. While roughly 1,300 Hezbollah operatives have been killed and close to 5,000 wounded in these battles, it has still increased its regular order of battle to roughly 20,000 combat troops and another 25,000 combat troops in reserve. This order of battle and the number of losses have raised quite a few questions in Lebanon itself about Hezbollah's status and role there.

The Palestinian arena is the most disturbing one in the short term. After a decade of relative quiet in Judea and Samaria, unrest in Israel's south and three rounds of fighting in the Gaza Strip, a new wave of violence began in October 2015, with different characteristics than in the past. Young men and women who do not belong to any organization have set out without warning to carry out stabbing attacks, which, at times, claim a heavy death toll. These attacks are inspired and nourished by what these young people see and hear in their immediate environment, including the new media outlets, where they absorb ideas of the Islamic State and other elements of radical Islam.

The first tendency is to deal with the new acts of violence by casting them into molds from the past. But we must realize that this is a new situation, and in order to deal with it, we need to understand the currents at work within Palestinian society. Armies and intelligence organizations usually advance along two axes: one axis includes the enemy's decision-makers and command systems, and the other axis – its capabilities. The currents at work on the other side are a subject that is difficult to understand, and they are actually the most disturbing.

Operation Protective Edge, which lasted for fifty-one days, caused damage to both sides and mainly to the Palestinian one. Since that operation, relative calm has reigned in southern Israel. While Hamas has made great efforts to regain its capabilities, including its rocket capabilities, and continues to dig attack tunnels toward Israel, 2015 was still the calmest of many years. Not one soldier suffered a scratch, and not one civilian was harmed. The twenty-four rockets that were fired from the Gaza Strip into Israeli territory fell in uninhabited areas and did not cause any injury. Yet this region, too, is potentially volatile, which stems from Hamas' considerable intelligence-operational-engineering efforts and Iranian aid, amounting to tens of millions of dollars, only some of which is invested

in reconstruction, while the other share is used for building up Hamas' capabilities against the State of Israel.

In the short term, two of the threats to the State of Israel are expected to increase and two are projected to decrease. It is anticipated that the sub-conventional and sub-state threats of Hezbollah, Hamas, the global jihad movement, and the Islamic State will grow. These organizations will continue their efforts to develop high-trajectory and precise weapons, dig improved attack tunnels, and dispatch terrorist and guerrilla cells. They will glean others' ideas in order to perpetrate resounding terror attacks and sow fear and terror, and in doing so, will make political gains. The cybernetic threat is also expected to intensify. The inherent danger in this threat is that it can be exercised from afar and yield impressive gains. The challenges in this sphere are many, and the IDF is working to strengthen its response to them.

We estimate that the two threats of conventional and non-conventional warfare will soon diminish. The conventional threat from the air forces, navies, divisions, and brigades of the enemy states is declining, although the IDF is built and prepared to withstand such a threat in the future. The non-conventional threat is expected to decline over the next three to five years for two reasons. First, the nuclear agreement between Iran and the West rolls back Iran's nuclear potential by dismantling Iran's existing capabilities and increasing the supervision of its nuclear program. In addition, it seems that Iran will have a strong interest to maintain this agreement in its first few years in order to enjoy its benefits. Secondly, as a result of the removal of the chemical weapons from Syria, the threat of chemical warfare against Israel no longer exists for all practical purposes. But another worrying possibility has arisen: the possible use of unconventional terrorist methods as part of the struggle among various rivals, Syria first and foremost.

The Use of Force against the Threats

The IDF recently published its strategy for the Israeli public. It did so out of a desire to explain its mission of protecting the State of Israel, ensuring its existence, and defeating its enemies should war break out. The document was based on work that was conducted in previous years, and more intensively over the past year. The IDF has another document in its possession, classified as top secret, of the same strategy.

When we survey the capabilities and power of the IDF in relation to the capabilities of other armies in the Middle East or in the world, we note with satisfaction that it possesses a high level of capability. The IDF has aerial, intelligence, and naval superiority, as well as cybernetic superiority. In addition, its ground capabilities are highly complex. The superiority of the IDF versus enemy armies is offset by sub-state organizations, which are located in inhabited areas where they are protected by defensive positions and by the civilian population, and are able to develop underground capabilities. This situation has implications not only for the IDF, but also for other armed forces that deal with terrorism. Hezbollah, Hamas, and the Islamic State challenge the IDF's basic concepts that have served the State of Israel well over the years — warning, deterrence, power, and security.

The question that arises is how deterrence can be created vis-à-vis terrorist groups that do not have any commitment to any particular state or ethic. If the IDF had to provide a deterrent vis-à-vis the armies of the past, today the demands are for high-level intelligence of sub-state groups. The IDF has the privilege of equipping itself with highly advanced weapons systems that enable it to deal with many threats; defending itself against the threats of terrorism on the ground, by sea and by air, as well as cybernetic terrorism, however, has become more complex than in the past. While the duty in past wars was to be victorious against regular armies, today it is the decisive defeat of groups situated among civilian populations while taking into consideration elements of time and the significance of this kind of combat in a democratic, law-abiding country such as the State of Israel. All these things have made combat much more complex. The IDF's challenge is to adapt the intelligence and operational response to the ground and to the changing threats, and provide a sense of security without excuses.

If we take the Palestinian arena as an example, the change that has occurred is prominent, in comparison to the situation a decade ago in the fight against suicide terror. What helped the IDF to cope with Palestinian terrorism in the past was the preventative approach, which relied on intelligence superiority and the ability to prevent terror attacks before they happened. This approach was based on excellent intelligence of the Shin Bet, the Military Intelligence Directorate, and other agencies. The current phenomenon of stabbing attacks eludes the most effective component of combating terror: advance warning. Today, terror attacks take place without any warning; the terrorist pulls out a knife and runs toward the target, be it a soldier or a civilian. For all practical purposes, since the stabbing incidents

began, we have been unable to provide advanced warnings. A stabbing incident usually lasts seconds from the moment the terrorist pulls out the knife until launching into an attack, and its prevention relies, for the most part, on the operational capabilities of the soldiers in the area. 8 percent of the stabbing attacks took place in front of soldiers who stood between the terrorist and civilians. In places where the security forces arrived a few seconds late, or were not in proximity to a civilian who had been stabbed, the price paid has been loss of life in some instances.

There are 161 communities in Judea and Samaria, inhabited by 400,000 Israelis who live among approximately two million Palestinians. These two populations are interspersed with one another, creating a significant operational challenge. The IDF's duty is to provide security, so that the inhabitants of Judea and Samaria are secure and feel a sense of safety. At the same time, the IDF follows an expansive civilian policy toward the Palestinian population, making a clear distinction between those involved in terror and the rest of the population. Within this framework, it allows 120,000 Palestinians to go out to work in Israeli cities and in the industrial zones in Judea and Samaria; these workers support 600,000 to 700,000 family members. This serves as a restraining factor, and is a common interest of both the State of Israel and the Palestinian Authority, like the mutual security coordination between them.

Terrorism in Judea and Samaria has occurred for many years, and one does not need to be a strategist or intelligence official to understand that it will continue for many more years. Looking back fifteen to sixteen years, we can see that not a year passed without people being killed or wounded in terror attacks: in the worst year, 453 people were killed and 3,000 were wounded, and in the year with the fewest number of attacks, six people were killed and 253 were wounded. The IDF's challenge then is to squash terrorism and defeat it everywhere possible, fulfill its responsibility to provide security and a sense of safety, and allow the political echelon the freedom to make decisions from a position of strength and not under pressure of terror incidents.

Regarding the other fronts facing the IDF, if in the past it was customary to quote the statement attributed to Clausewitz that an army was in one of two states – that of preparing for war or that of war – in this new reality is another situation. The wars of today are based first and foremost on very high intelligence capability and on covert and overt capabilities. Their objective is to harm and weaken the enemies, to prevent them from

growing stronger and from gaining advanced capabilities, and to do so in a manner that will not lead to a broad escalation.

In parallel with the IDF's use of force throughout the year, which is done out of sight and by covert means, it is making great efforts to improve its preparedness. The IDF has learned lessons during the past decade when its main effort was combating terrorism, and it was not overly strict about maintaining a methodical and intensive training system. As a result, the price paid was very high. The IDF realizes now that it must be prepared for outbreaks of war within a short period of time, and that it must make preparedness a priority among its other tasks. For all practical purposes, preparedness is the IDF's top priority.

If we are to fulfill the IDF's responsibility, we can no longer base ourselves on the "Precious Time" program that was used in the past, whose main principle was that the army would improve its fitness, organization, and preparation for a military operation when it faced a state of escalation. The current understanding is that the IDF must be prepared in advance and within a very brief amount of time in order to deal with violent outbreaks so that it can do its job and fulfill its purpose. One of the lessons learned was that it is impossible to base oneself on the elusive concept known as "deterrence." While deterrence is holding its own in southern Lebanon, its effectiveness could change at any time. For that reason, the IDF's test must be and is that of capability.

The Gideon Multi-Year Plan

In addition to carrying out the policy on the use of force, over the past year the IDF has begun drawing up a new multi-year plan. This process is extremely significant. The previous multi-year plan was drawn up in 2007. While it strengthened the IDF's capabilities, no new multi-year plan has been approved since. The new multi-year plan, named Gideon, was put into use in early 2016. It was based on the idea of reducing the IDF's size and having it focus on its core missions, strengthening its key components, improving its preparedness, instruction, training, and inventory, and putting these fields above all other tasks. At the same time, the fight against terrorism must continue, while wisely managing the risks. Still, it would be a mistake to direct all the IDF's resources and capabilities towards the war against terrorism; when a broader pattern of activity and operations is necessary, requiring brigades and divisions, district-wide regiments and

commands, and even the General Staff, the IDF will find itself in the place where it was in the past and where it does not wish to be again.

As stated, the Gideon multi-year plan seeks to adapt the IDF to its proper size and reduce the size of the regular army, the career army, and the reserve army. The hope is to cultivate strong, well-trained, and sustainable units while reducing the size of the IDF, which is still very large compared to other armies in the area. The IDF has made significant decisions to establish a cyber corps to deal with developments in this sphere; merge the Ground Forces with components of the Logistics Corps; organize the special units into a single brigade and incorporate the Depth Corps within it; make the 98th Division into a regular Depth Corps division; and solidify auxiliary capabilities, which rest upon cyber connectivity or "jointness." The purpose of all this is to reach a higher level of effectiveness.

The State of Israel has noteworthy capabilities in industry and science, rendering the question of where the IDF should direct its strength into a constant subject of debate. The IDF is in a large-scale process of acquisition, after having decided that to entrench its strengths, it needs to augment its unique powers instead of developing new capabilities. In addition, the project of moving the IDF to the Negev continues, and as part of that project, some of the army's capabilities will be transferred there during the next decade; this is a process requiring many resources, including vacating the army's headquarters in central Israel. Emphasis is also being placed on strengthening the IDF's status as a national army – a people's army – and we will undertake significant measures that will affect Israel's society and economy, as well as the relationship between the army and Israeli society.

The Challenges of the Future

The first challenge that the IDF faces is to maintain regional deterrence, help defeat the Islamic State, and increase the security calm as much as possible. The IDF seeks to do this while preserving the peace treaty and Israel's special relationships with Egypt and Jordan, as well as while dealing with the volatility of the Palestinian arena. This is no simple challenge amid the upheaval in the region.

The second challenge is to strengthen the IDF's multi-dimensional capability for aerial, naval, and ground defense and maneuvering. For this purpose, the IDF has been allocated tremendous resources, enabling it to protect the State of Israel both during ordinary times and in time of war. This refers, among other things, to active defense of multiple layers, giving

Israel the most advanced defensive response in the world. This challenge includes fortifying naval defense by purchasing ships for defense, as well as strengthening the cybernetic dimension. Overall, this means reinforcing intelligence, aerial, naval, and cybernetic capabilities opposite the ground capability of our enemies in Lebanon and the Gaza Strip and the challenges they present. In addition, this challenge includes the necessity to create synergy between all the military systems and increase the jointness between the Mossad, the Shin Bet, and the other security agencies, which constitutes a power multiplier for the IDF and the State of Israel.

It is a serious task to maintain the situation in the Gaza Strip and to prevent attempts to violate Israel's sovereignty below ground. The highest priority in this sphere is the formulation of a defensive and offensive response to the tunnels. Another priority is strengthening the security and sense of safety in Judea and Samaria in light of the current wave of escalation of terror. On the one hand, this means combating terrorism effectively, professionally, and with a great deal of operational initiative and intelligence, which will provide a response to the terror attacks by individuals and to the shooting attacks by organized cells. On the other, it means providing hope and allowing the Palestinian population to live their lives and support their families. It would be a grave mistake to impose closures and restrictions on the Palestinian communities, since such punishment will also work against Israel's interests in the end.

We must continue to maintain deterrence in the northern arena vis-à-vis the global jihad movement, the Islamic State, the Iranian forces that operate Shi'ite militias from there, and Hezbollah. In addition to deterrence, we must also uphold the IDF's justifiable image and its capability as an unpredictable adversary that is able to provide a harsh response.

The IDF understands the situation as it is, makes courageous decisions, and even takes risks in order to adapt to the many challenges it faces. It does so out of its intention and effort to turn the vision into reality and be a first-rate army that is physically fit and able to defeat its foes, while concurrently developing its future capabilities. The IDF works to be the people's national army, composed of high-level, committed people who are devoted to their country; a modest army that is by and for the people; an army that is based on an effective organizational culture and has the public's trust. It is not to be taken for granted that the IDF receives the highest level of trust in polls that are conducted each year. It is a valuable asset that must be nurtured and preserved.

We are in a time of risks and opportunities. We must preserve the State of Israel's standing in the region as a democratic country; an island of stability; and of military, scientific, and ethical power, even as we prepare for future risks and manage the current, familiar ones. Without wise risk management, it will be difficult for the IDF to proceed and be well prepared to face the challenges. The IDF is marching in that direction, and proof of that can be seen even now, both in the IDF's strategy and in the Gideon multi-year program.

Principles of the Israeli Political-Military Discourse Based on the Recent IDF Strategy Document

Kobi Michael and Shmuel Even

Relations between the military and political echelons in Israel are complex and multifaceted, both in theory and in practice. The problems resulting from the interface between the two have at times resulted in ineffective military deployment or a crisis of expectations. Moreover, as the positions of the political echelon are never unanimous, its directives to the military have not always been aligned with the government's position, and sometimes even have been nebulous.

In August 2015, the Israel Defense Forces (IDF) released a document entitled the "IDF Strategy" directly addressing the issue. Signed by the chief of staff, the document is notable in part for its proposal to adjust the discourse between the military and political echelons as well as to clarify the role of the chief of staff and his functional autonomy. In this document, the chief of staff suggests to the political echelon how it should formulate directives to the military so that military action will match the political objective in question, and thereby prevent a crisis of expectations. According to the document, the IDF sees its role of achieving "victory," which does not necessarily mean defeating the enemy; the political echelon together with the chief of staff must define the concept of victory before the military is deployed. The publication of the "IDF Strategy," unprecedented in Israel's civil-military relations, also highlights the chief of staff's sensitivity to Israeli public opinion.

Keywords: IDF, civil-military relations, strategy, discourse space, learning, civil control

Dr. Kobi Michael is a senior research fellow at the Institute for National Security Studies. Dr. Shmuel Even is a senior research fellow at the Institute for National Security Studies.

Introduction

In democratic states, the political echelon controls the military echelon. The notion, however, that the lines of responsibility between the two can be demarcated is fundamentally erroneous. In practice, the relations between the political and military echelons are fraught with tensions, which has been keenly felt in Israel since its establishment. Shortcomings in the discourse between the two were apparent in most of the wars and large-scale operations; at times, the tensions between them even have been scrutinized by commissions of inquiry, such as the Agranat Commission after the Yom Kippur War and the Winograd Commission after the Second Lebanon War.

In August 2015, Chief of Staff Lt. Gen. Gadi Eizenkot released the "IDF Strategy" to the public.[1] It is a non-classified version of a document that discusses military strategy, formulated during the preparation of the Gideon multi-year plan for which the chief of staff sought approval and funding (it was, in fact, approved in April 2016). The chief of staff is the only signatory to the document, but it is safe to assume that the defense minister and prime minister do not object to it.[2] The document presents the options of operation and the security outputs that the Israel Defense Forces (IDF) can provide on a given budget. In addition, it proposes to the political echelon how it should formulate directives to the military in order to attain the goals and objectives sought, and calls for discussions between the two before these directives are issued. The goals of the discussions are to mutually clarify the situation as both sides see it, elucidating to the chief of staff the goals and constraints of the political echelon, and informing the political echelon of the IDF's capabilities. The fact that the chief of staff felt the need to invite the military and political echelons to engage in a discourse – and to do so in a public document – is evidence of the gap in this sphere, which has persisted, as already noted, since the early days of Israel's statehood.

This essay deals with the discourse between the political and military echelons in Israel, and focuses on the principles and patterns that the chief of staff would like to use to shape this discourse, as well as the way these principles and patterns deviate from the commonly accepted theories in this field and from the past relations between the two echelons. The essay is divided into two parts. The first part covers theory on relations between political and military echelons in general and presents an overview of the obvious problems in the discourse between the two in Israel as revealed

by various events. The second part presents the chief of staff's position on the relations between the two echelons as reflected by the "IDF Strategy" document, followed by our analysis of that position, the implications, and recommendations.

Theoretical Background: Relations Between the Political and Military Echelons

Relations between the military and political echelons are part of a broader relationship between the civil sector and the military. Complex and multifaceted, these relations are a motherlode for academic research and legislation in Israel and elsewhere.[3] A fundamental convention in a democracy is that the political echelon is in charge of the use of force. It does so by controlling the military through a mechanism of civilian control and guidance. The theory in this field deals with the essence of civilian control of the military in democratic nations and, concretely, with questions such as: To what extent should the political echelon be involved in the work of the military? What is the division of responsibility between the two echelons? Is some of that responsibility shared? How should the discourse between them be conducted? What kind of relationship should the two echelons have?

Civil control of the military is essentially the mechanism that regulates relations between the civilian and military echelons in a democracy. Some would describe civil control as being quite broad and absolute. Richard Kohn claims that the authority of the civilian echelon should be absolute and comprehensive and that it should be responsible for directing the military in every field and on every subject, including questions of force construction and force deployment. According to Kohn's definition, any functional autonomy of the military is the result of the political echelon's decision to grant the army authority that may be withdrawn at any moment.[4] Less rigid definitions exist, however, and some even replace the concept of "civil control" with the idea of "civil guidance."[5] In this essay, we shall define civil control as the responsibility of the political echelon to ensure that the military action adheres to the political objectives.[6]

Samuel Huntington's 1959 work *The Soldier and the State: The Theory and Politics of Civil-Military Relations*[7] was most influential in the field for a long time. Huntington developed the principle of "objective civilian control" in a democracy, whose implementation is supposed to ensure harmony between the political and military echelons and prevent the interference of the latter

in the political sphere. Objective civilian control is based on a very clear distinction between the military and civilian spheres and on maintaining the military's functional autonomy (force construction and deployment), according to the military's professional principles. Morris Janowitz, who together with Huntington was one of the founding fathers of this discipline, presented a contradictory position in his book *The Professional Soldier: A Social and Political Portrait,*[8] in which he expresses reservations on the clear distinction between the military and civilian spheres. His position derives from the fact that modern armies are increasingly assuming constabulary functions and liable to alienate the military from the society as the separation between the spheres grows. According to Janowitz, any effective civilian control mechanism must be based on the officer class being well exposed to society and educated to internalize social values in order to ensure that military officers apply military force only for objectives that society deems worthy and appropriate.

The tension between the two approaches, as developed by the founding fathers of the discipline, and their criticism led to the development of a theoretical foundation of the field of civilian-military relations. Unlike Janowitz's sociological approach, Huntington's theory reflected a political science approach and dominated the field until the late 1980s. At that time, some competing theories emerged, as part of the critique of the Huntingtonian approach.[9] Three prominent theories are relevant to this essay's discussion about the mutual relationship and discourse between the political and military echelons.

Douglas Bland's theory of shared responsibility[10] emphasizes the distinction between the legal, normative authority of the political echelon and the obligation of consensual division of responsibility between the political and military echelons. The two share responsibility for formulating national security strategy from the military perspective and the manner in which the military should implement it, subject to the instructions of the political echelon. Maj. Gen. (res.) Gershon Hacohen, former commander of the IDF National Security College, adopted Bland's concept of shared responsibility. In his opinion, "shared responsibility is not manifested in the question of where the source of authority comes from, because the source of authority is always, and asymmetrically, in the hands of the political echelon, but rather in the question of how did the idea come into being, who initiated it, and who is the architect. There is room for both to express themselves in generating an idea and both are in this field with

shared responsibility."[11] Hacohen is vehemently opposed to the approach that views the defense establishment, including the military echelon, as being merely a tool in the hands of the political echelon. He distinguishes between the constitutional-institutional aspect and the cognitive one, which is connected to processes of knowledge development of civil-military relations:

> When delving into strategic questions, the military as architect isn't merely a broker between the entrepreneur and the construction workers, but functions in a much greater capacity. Hence it is necessary to address the working relations between the architect and the entrepreneur, the civilian echelon being a type of entrepreneur in this metaphor. I would expect the military leadership and the heads of the defense establishment to act like the good kind of architect. This relationship is complex.[12]

Rebecca Schiff's concordance theory also includes citizenry in the equation of civil-military relations.[13] This theory posits that the essence of civilian control depends on the cultural context and is the result of an agreement among three players – the political echelon, the military, and society – regarding the military's autonomous space and its conduct vis-à-vis the political echelon. Schiff criticized the American ethnocentric point of view in previous research on civil-military relations, which led to a universal notion about the essence of civilian control in democratic nations; Schiff examined India and Israel where she found different models of civilian control.

Schiff developed the targeted partnership theory based on the concordance theory and analysis of the American experience in Iraq and Afghanistan.[14] This theory stresses the importance of a discourse between the political and military echelons. According to Schiff, the political-military discourse during Secretary of Defense Donald Rumsfeld's term in office was characterized by his contempt for military officers, rigidity, formality, and by efforts to demarcate the military and the political spheres. The result was a failed US strategy; the political echelon was kept out of the military echelon's loop of knowledge, and the military ignored its obligation to voice its professional opinion, choosing instead to fully obey the political echelon even though it was clear that the politicians' objectives and directives were problematic and at times even irrelevant to the emergent reality. Unlike during Rumsfeld's tenure, the discourse between the echelons during the

tenures of Secretary of Defense Gates and General Petraeus as commander of the US forces in Iraq was characterized by great openness and sharing between military and civilian experts. This discourse helped the political echelon understand the complexity of the environments as well as the military's capabilities and limitations; therefore, the strategy formulated was more relevant than it had been previously and the results were better.

The RAND Corporation's report on the thirteen years of US military involvement in Iraq and Afghanistan also validate the importance of an open, ongoing discourse between the echelons.[15] Out of seven lessons presented in the RAND Corporation's far-reaching study was that "the blurry line between policy and strategy requires both civilians and the military to engage in a dynamic, iterative dialogue to make successful strategy, but that often failed to occur ...The ends, ways, and means did not align, whether because the policy objectives were too ambitious, the ways of achieving them ineffective, or the means applied inadequate." The RAND report, which, as noted, stresses the importance of an interactive dialogue between the sides, criticizes the current situation in the United States:

> The current process does not routinely produce effective strategy...Civilian policymakers require an active dialogue with the military and other sources of information to inform the diagnosis of the situation, as well as to develop realistic policy objectives. That iterative process must continue through the development of options...Formulating strategy is further inhibited because there is no established integrated civilian-military process that would rigorously identify assumptions, risks, possible outcomes, and second-order effects ...The lack of such a process inhibited timely adaptations of strategy in response to the evolution of understanding and events.[16]

The relationship between the political and military echelons, shaped by preserving a hierarchic, conservative model that demands absolute separation between the political and military spheres, reduces the room for discourse between them. With limited discourse between the two, the political echelon will find it hard to realize civilian control over the military in terms of coordinating the military action with the political objective.[17] For example, when there is no discussion between the sides about the objective of the use of force, it is easy to imagine a scenario in which military force is overused in order to resolve political problems or when the military takes unnecessary risks. When the political echelon reveals its strategic

intentions to the military, however, the military echelon can present its own assessment of the situation, based on the knowledge developed as well as relevant military options.[18]

An open discourse usually enables information and preexisting assumptions to be challenged by means of renewed thinking about conceptual forms. It enables decision makers to develop suitable terminology and a foundation for a system of interpretation that may facilitate a new understanding of the situation, the objectives, and the means of achieving them.[19] At the same time, an open discourse allows for the expression of other opinions and criticism that are not easily expressed in a (closed) discourse of directives.[20] The political echelon's need to learn is critical as it lacks the experience and knowledge about the complexity of military strategy and operational planning, and thus is liable to err about the costs and risks involved in deploying the military. The targeted partnership model provides greater space to military experts to demonstrate their expertise, and enables the political echelon to formulate objectives for the military that are aligned with the chances and risks it is willing to take.

The two approaches – the functional autonomy of the chief of staff and the joint responsibility between the military and the political echelons– have their advantages and drawbacks, and it is therefore likely that in extreme scenarios, tensions will develop between them, especially when one tries to apply the joint responsibility approach through an open discourse, which is inherently anti-hierarchic. In such a case, government ministers will summon the chief of staff, the military leadership, and assorted military experts and demand that they render their opinions. In such an encounter, the government or the cabinet may accept majority-based decisions that are not necessarily aligned with the chief of staff's position or the work of the General Staff (the highest commanding forum in the military); they may even align with the prime minister's own objectives. Alternately, the rigid adoption of functional autonomy, meaning an exclusive connection between the political echelon and the chief of staff, would prevent the civilian sector from receiving first-hand exposure to additional information and other opinions prevalent in the military.

In order to analyze the "IDF Strategy" document, we will distinguish between two types of discourse that take place between the political and military echelons: a learning discourse and a discourse of clarifications and directives.

A learning discourse refers to a broad, deep, and ongoing discussion over fundamental – albeit not necessarily concrete – issues, designed to exchange information and points of view for the sake of shaping policy, strategy, planning, periodic situation assessments, and updates. In such a discourse, the political echelon learns security threats and military capabilities in depth, while the military echelon examines the objectives of the political ranks in order to provide them with an appropriate military response. Together, the military and political echelons create strategic outputs that are coherent and valuable to both.[21] A learning discourse can only develop in a climate of openness in civil-military relations and when the political echelon is willing to acknowledge the gaps between the policy objectives and the military's capabilities. Such a discourse has the potential to change the political aims or increase the resources to enhance the capabilities of the military.

A discourse of clarification and directives refers to a concrete and focused discourse designed to assess the situation and clarify positions before the political echelon makes certain strategic decisions, such as embarking on a military operation or changing the direction of an operation already under way. This discourse may address the military efforts needed to achieve the political objectives; the means to attain those military achievements; the contextual risks, and so on. Following this discourse, the chief of staff can jumpstart learning processes within the military that may lead to formulating strategy and plans. A discourse of clarification and directives is more effective if it is preceded by a learning discourse between the political and military echelons.

Prominent Shortcomings in Civil-Military Relations in Israel

The Agranat Commission, the state commission of inquiry over the Yom Kippur War, placed full responsibility for the war on the military command, and refrained from addressing the culpability of the political echelon. The public rejected this position. Yitzhak Rabin, too, who was a minister in Golda Meir's government and later prime minister, dismissed several of the commission's recommendations. He stressed that each was accountable and emphasized that there was an inherent risk in allowing the political echelon to shrug off responsibility, as it would affect the willingness of the military rank to present its position clearly and honestly, be proactive, and take risks.[22]

The Agranat Commission, however, explicitly stated that "the absence of a definition of authority (in the triangle of the government – the defense minister – the chief of staff) in the current reality of the defense establishment – a field that is unsurpassed in terms of its crucial importance – hampers the effectiveness of action, reduces the focus of responsibility, and also causes the public to feel disconcerted and unclear."[23] As a result, in 1976 the Knesset passed the Basic Law: The Military, which regulates the hierarchy of authority and responsibility for the IDF. According to the law, "the military is subject to the authority of the government"; "the minister appointed by the government for military matters is the defense minister"; "the supreme commanding echelon in the military is the chief of the General Staff" and he "is subject to the authority of the government and subordinate to the defense minister." The prime minister is not mentioned in this law, and the political echelon's responsibility towards the military is not defined. In fact, the law failed to solve some of the problems, particularly that of regulating the direct responsibility of the prime minister, who is deeply involved in military matters on virtually a daily basis.[24]

The significance of the Basic Law: The Military is that the government is the supreme commander of the IDF and the chief of staff is subordinate to the government in two ways: by being accountable to the defense minister and by being subject to the government's authority. The government's authority overrides the subordination of the chief of staff to the defense minister. Consequently, the directives issued by the defense minister must have the government's backing and the chief of staff is supposed to be kept abreast of them, and not only via the defense minister. The discourse is liable to break down when either the chief of staff or the defense minister or both operate without the support of the government (whether intentionally or not); when either the government or the defense minister or both in conjunction direct the IDF through channels that bypass the chief of staff; or when either the defense minister or the chief of staff or both perform their roles improperly.

In the First Lebanon War, there was a wide gap between the objectives that were approved collectively by the government and the far-reaching objectives by which Defense Minister Ariel Sharon and Chief of Staff Raphael Eitan chose to lead the IDF.[25] Relations between the two echelons had become blurred as the defense minister functioned as the prevailing chief of staff while also having wide political latitude. Thus, an IDF investigation showed that on June 7, 1982, Sharon had instructed the commanding officer

of the Northern Command "to hurry up and move" towards the Syrian military without consulting the government,[26] which had been trying to prevent a military confrontation with the Syrians. The chief of staff obeyed the defense minister's directives even though these were not aligned with the government's position, thereby abusing his position as subordinate to the government; the move led to a significant expansion of the war's boundaries and dimensions. Later on, Lebanese President-elect Bashir Gemayel was assassinated, and Christian militias perpetrated a massacre in the Sabra and Shatila refugee camps, located in an area under IDF control. Unlike the Agranat Commission, which placed full responsibility on the military echelon alone, the Kahan Commission, which investigated the slaughter in the refugee camps, held the political echelon accountable, and, in particular, Defense Minister Sharon.

The first months of the Second Intifada, which erupted in 2000, revealed shortcomings in the relations between the political and military echelons. The political echelon failed to make sure its directives were realized by the military; later on, the political echelon gave the directive to evacuate Abu Sneina Hill in Hebron (in Area A) on the basis of an understanding that the Israeli government had reached with the Palestinian Authority; Chief of Staff Shaul Mofaz, however, thought an evacuation would be a mistake from a military standpoint and preferred to ignore the instructions issued by Prime Minister Ariel Sharon and Defense Minister Ben-Eliezer, who were on a state visit to Russia at the time.[27]

The Second Lebanon War in 2006 also highlighted the problematic nature of civil-military relations in Israel. The Winograd Commission, appointed to investigate the war, defined the responsibility required of the political echelon as follows: "The political echelon must direct and steer the action of the professional echelon in the defense institutions and foreign policy, and control them; deepen the discourse between the political echelon and the heads of the intelligence institutions to understand needs and implement the assessments; and demand and guide the development of fundamental strategic documents on key topics and approve them, employing an integrative approach that may lead to a comprehensive political-security vision."[28] The Winograd Commission determined that both echelons bore responsibility for the war's outcome. In fact, both understood this even before the fighting had ended, as indicated by a conversation between Defense Minister Amir Peretz and Chief of Staff Dan Halutz on August 14, 2006, the last day of the war. The chief of staff, who was surprised

by Defense Minister Peretz's suggestion to establish a commission of inquiry, pointed out that "if there is anything that needs investigating it is the military-civilian interface." Later on in the conversation, the chief of staff asserted that "it is necessary to investigate the policy implemented in Israel for the last six years." The defense minister agreed, but made it clear that policy was not within the chief of staff's purview and that the political echelon was responsible for such an investigation. At the end of the conversation, the chief of staff added that it was necessary to investigate yet another matter, that of the "the discourse between the political echelon and military echelon, between you and me."[29]

Operation Cast Lead (late 2008 – early 2009) demonstrated the problematics of the relations between the political and military echelons, stemming from the political echelon's inability to formulate and provide clear directives. The first condition necessary for providing the military with directives is the formulation of a cohesive position by the political echelon. This was not achieved because of a disagreement among Prime Minister Olmert, Defense Minister Barak, and Foreign Minister Livni (the so-called "trio"). At a conference on Operation Cast Lead held in 2012, Lt. Gen. (res.) Gabi Ashkenazi, who was chief of staff at the time of the operation, remarked that "a few days into the operation, the 'trio' fell apart; each went off in a different direction and this affected the decision-making process. These disagreements wasted precious time; you have to sit with your commanding officers and lead them in a way that is in line with what I understand they [in the political echelon] want."[30] At the same conference, Tzipi Livni, the foreign minister during the operation, said: "In the case of Operation Cast Lead, you had the prime minister, the defense minister, and me. There were disagreements before the operation, during it, and after it ...We started the operation without having decided to take the regulatory approach or the deterrence approach."[31]

Israel's attempt to confront the Iranian nuclear threat was also rife with disagreement, this time between the political echelon and the security establishment. According to the investigative journalism TV program *Uvda* ("fact" in Hebrew), in 2010 the leaders of the political echelon, Prime Minister Netanyahu and then Defense Minister Barak instructed the defense echelon, led then by Chief of Staff Gabi Ashkenazi and Mossad Head Meir Dagan,[32] to be on alert in preparing the defense establishment for an attack on Iran.[33] This directive seems to have reflected the recognition that the Mossad's covert effort to foil Iran's nuclear program had been exhausted.

According to the show, Ashkenazi and Dagan disagreed with Netanyahu and Barak. The chief of staff said that "being on alert" would bring closer a war with Iran, and that was something that required a cabinet decision. By contrast, Barak told the interviewer of the TV show that the order given did not consist of going to war and therefore did not need a government or cabinet decision. According to the former minister of defense, "the chief of staff has to construct the operational ability and has to tell the political echelon if it is doable or not doable from a professional point of view. He may – in fact, he should – add his recommendation, but an operation can be carried out even against his recommendation."[34]

Operation Protective Edge in the summer of 2014 was also marred by functional imprecision at the political level, with Israel being dragged into a battle for which it had not prepared. This is reflected by former Deputy Chief of Staff Maj. Gen. (res.) Yair Naveh, in a statement as follows:

> I think there was a new political understanding to which the military failed to conform in its planning and reserves as well as its state of mind. What happened in practice was the opposite of how the military had prepared in the previous years. As the operation was under way, they said that we were actually entering a war of attrition ... If you want dramatically to change the doctrine of operating the military, you have to undertake orderly discussions in the government, decide what the implications and ramifications are, and prepare accordingly, not be taken by surprise by a fifty-day-long campaign.[35]

It is worth mentioning that a long war, contrary to the military's conception, is not necessarily a mishap, because the rationale of short wars is rooted in the need to defeat the regular armies by a general call-up of the reserves. But the gap between the pace dictated by the political echelon in Operation Protective Edge and the military's conception indicates that the ongoing discourse and shared learning between the two were insufficient and ineffective both before and during the campaign, despite the fact that twenty-seven discussions of the political-security cabinet were held during the operation alone.[36]

In addition to these failures, the ground offensive against Hamas' tunnels during the operation demonstrated the gaps between the military's rationale and that of the political echelon, and it was the political rationale that won out. For example, from a military standpoint, launching ground

combat in the tunnels was pointless, and the IDF was not prepared to do so.[37] Militarily, it would have made more sense first to seize control of the tunnels system and only then to destroy them or, alternately, not to make a ground offensive against the tunnels on Palestinian territory at all because it is relatively easy for them to rebuild that system.

The Discourse Proposed by the Chief of Staff to the Political Echelon

The need for a discourse between the military and political echelons is explained in the "IDF Strategy" document as follows: "The directives of the political echelon demand an ongoing discourse and process of clarification between the senior military rank (the chief of staff) and the political echelon. The political directive forms the foundation for the processes of strategic thinking of the General Staff, but is also affected by these processes; the influence is mutual."[38] In addition, the document explicitly refers to the way in which the political echelon is supposed to direct the chief of staff, indicative of just how great the gap really is, as the chief of staff had identified. According to the document, the discourse is supposed to be based on the political echelon's recognition of the status of the chief of staff. The document defines the chief of staff solely as the senior military rank who debates with the political echelon and presents the military's position to the government.[39] He makes it clear that the chief of staff and his command center cannot be bypassed, stating that: "The only campaign commander in the IDF is – through the General Staff – the commander of all the operations the IDF carries out"; "This responsibility of the General Staff cannot be decentralized or transferred"; and "Every commanding officer is subordinate to one commander at every point in time. Orders will be given on the basis of the chain of command."[40]

When referring to "the objective of military action in the IDF's different functional states," the chief of staff suggests to the political echelon "several main political and strategic objectives for the use of force: a) postponing the next round of confrontation by routinely using force; b) preserving the strategic situation or improving it after the enemy has begun violent action, characterized by a change in patterns of action and intentions; c) changing the situation from the bottom up to the point of altering the strategic balance, manifested by the neutralization of players or a fundamental change in their capabilities or status."[41]

The document explains that three states of military functioning have been defined – routine, emergency and war – in order to create a common language. According to the document, "the definition of the military functioning is the chief of staff's definition of the kind of military operation that is needed. The definition is useful to express an understanding of the confrontation on the ground; it helps maintain a discourse with the political echelon; it defines the basic political situation; and it decides on mobilizing the state's resources." According to the document, "the routine state includes everyday security, the limited and ongoing confrontation, and the campaign between wars." The document defines an emergency state as referring to "limited campaigns and operations that are not carried out in the context of war"; and the third is, as noted, "a state of war."[42] The political echelon must be familiar with the three different military states. Central to the issue of discourse is the document's assertion as follows: "When it is necessary to deploy the military, the political echelon should formulate directives to the military as follows: a) what are the objectives and what are the strategically needed end-states; b) what is the military's function and how does it play a role in attaining the objectives; c) what are the constraints in using military force; d) definition of other efforts (political, economic, media, and social) and the IDF's role in those contexts."[43] These declarations and others made by the chief of staff and presented in the "IDF Strategy" document indicate a clear, methodological proposal for the way the political echelon is supposed to provide directives to the chief of staff and for the type of discourse that should take place between the two sides.

An Analysis of the Chief of Staff's Position

The document demonstrates that, according to the chief of staff, the political and military echelons are supposed to maintain an ongoing, constant discourse. The role of the political echelon in this discourse is to define the IDF's objectives, means, and constraints, whereas the role of the chief of staff in this discourse is to execute: build up the military and deploy it in accordance with the directives of the political echelon. In other words, the political echelon is supposed to allow the chief of staff to build appropriate military capabilities and command the IDF during states of routine, emergency, and war, in addition to – as the document infers – providing the military with the resources to carry out these tasks.

In the document, the chief of staff does not address the composition of the political echelon with which he seeks to maintain a discourse. In Israel,

the government stands at the head of the political echelon and the chief of staff is subordinate to it; as are the ministerial committee on national security, the prime minister, and the defense minister, to whom the chief of staff is directly subordinate on behalf of the government. It would seem that when the chief of staff refers to a discourse with the political echelon, he is referring not only to the defense minister, with whom he works closely, but also, at least, to the prime minister who represents the government.

The perception of the chief of staff's functional autonomy vis-à-vis the political echelon is the starting point of the discourse. The chief of staff's understanding of his functional autonomy is manifested by his saying that the military will always be closely led by the chief of staff and the General Staff and not by any other commanding group. This is in contrast to the First Lebanon War, which was led by the Northern Command, with the involvement of Defense Minister Sharon, and the Yom Kippur War in which Defense Minister Moshe Dayan tried to bypass the government and the General Staff and gave orders directly to Commander of the Southern Front Israel Tal.[44]

This reading of the chief of staff's position and functional autonomy is consistent with Huntington's principles of objective civilian control of the military in a democracy. These principles stress the distinction between the military and civilian spheres and the functional autonomy that should be given to the military. The chief of staff's understanding of the discourse between the political and military echelons, however, also includes principles from the theories of shared responsibility and targeted partnership, both stressing the importance of the encounter and discourse between the political and military echelons in order to achieve harmonic, responsible relations that will help them better understand one another and improve the decision-making process. In other words, while the chief of staff presents a very rigid approach to his authority in the military and the autonomous space of the IDF – leaving no room for the involvement of the political echelon – he also requires an ongoing discourse with the political echelon, mainly for the sake of clarifying the latter's directives. It would thus seem that the chief of staff is seeking what he considers an appropriate balance.

The document provides additional dimensions to the chief of staff's formal standing as defined in the Basic Law: The Military. According to the document, any action taken by the political echelon that affects the military must be done in coordination with the chief of staff, and only after

discussion with the chief of staff, can the use of force be acted upon. This suggests that the government should not guide the IDF's force construction on the basis of recommendations made by external committees, such as the Locker Commission, without making sure that they are aligned with the strategy formulated by the chief of staff.

In addition, the "IDF Strategy" document does not refer at all to the concept of shared responsibility, and most likely this is intentional because the inclusion of the phrase could be interpreted as the military's partnership in a political act. Nonetheless, the chief of staff asks the political echelon to bear responsibility for the task of coordinating the military action with the political objectives, a task in which the chief of staff plays a major role. This is done in order to improve chances of success and to prevent the political echelon from shirking responsibility should an incident occur, by claiming that it was unaware of the IDF's capabilities and the scope of the threat.[45]

From the document, it can be inferred that updated rules of discourse between the political and military echelons are especially needed because the IDF's new strategy is essentially different from the traditional security doctrine,[46] given the radical changes that have taken place in the security environment. Consequently, deterrence does not prevent violent rounds of fighting; early warning is not needed for massive, urgent call-up of the reserves; and the exclusive objective of the military campaign is no longer defeating the enemy, but rather achieving victory. In order to gain victory, the political echelon must define it ahead of time, using terminology readily understood by both sides. The document makes it clear that a military defeat of an enemy does not necessarily have to be the objective, unless the political echelon explicitly directs the military to do so.

Given the new reality, the document also underscores that the chief of staff understands the limits on the use of military force and the importance of non-military aspects (political, economic, media, and social) in the current environment as significant in the discourse with the political echelon. Moreover, the document explicitly refers to a discourse of clarification and directives in the context of the use of force, but there is not any explicit reference to the concept of a learning discourse. Nonetheless, the document does infer the need for one, which, in certain cases, could become a precondition for holding an effective discourse of clarification and directives.

The timing of the distribution of the document in August 2015 was not incidental, and may be viewed as part of the discourse that the chief of staff

maintains with the public, including elected officials, administrators, and others who are not privy to sensitive materials, but have been exposed to criticism of the IDF. The timing of the document's release may have been affected by the vociferous altercation between the Defense Ministry and Finance Ministry over the defense budget and demands for far-reaching reforms in the IDF (subsequent to the findings of the Locker Commission), which did not adhere to the chief of staff's Gideon Plan that was subsequently approved by the cabinet. In the background is the despondence of many IDF commanders that the military's status in the society has been severely eroded, in part because of the public's harsh criticism of the military expenditures and disappointment with the IDF's capabilities to attain expected goals. In this sense, the document was probably meant to coordinate the public's expectations while sharing information about the threats, the types of possible military responses, and their implications. Distributing the document to the public at large – a first in Israel's history – could be an important contribution to the public discourse and to strengthening civilian control of the military.

Implications and Recommendations

The political echelon bears supreme responsibility for coordinating between the military action and the political objective. It must direct the military echelon and control it before and during the military action and allocate resources to achieve the objectives. Both the historical background and the fact that the military echelon turns to the political echelon for directives, as presented in the "IDF Strategy" document, indicates that there is a real gap between the two, which has yet to be closed. To do so, the political echelon – in various constellations – must have sufficient knowledge of military matters, which means preparation and study time. In addition, the political-security cabinet must discuss and adopt solutions to bridge the gap in the discourse between the political and military leadership, at least in the field of directives as the chief of staff requests.

Clarity in political objectives is a prerequisite for an effective discourse between the political and military echelons in Israel, in which the government, as a collective, is the military's supreme commander. The historical overview shows that a large part of the confusion in the discourse between the two sides results from internal disagreements within the political echelon itself, whether within the government as a whole or within the smaller group who represent the government to the military. Such, for example, were

the disagreements about the defense budget between the defense minister and the prime minister on the one hand, and all the other government ministers, on the other, as well as during Operation Cast Lead in which the top political leaders could not agree among themselves on the end objectives and military methods for achieving them.

In coalition agreements, obscurity sometimes serves as a tool for bridging gaps. When directives to the military echelon are at stake, however, this is not true. The IDF has neither the mandate nor the ability to deal with multiple opinions or uncertain positions of government and cabinet members. In such a reality, the military is liable to operate based on its own interpretation of the political echelon's intentions, and this might lead to results that are far removed from the political objectives. A joint discussion between the civilian and military leaderships will encourage the government to formulate its position and engage in a discourse with the military that will result in preparing a number of possible plans and deciding upon a course of action. The prime minister and defense minister are both responsible for presenting the government's position to the military, while the chief of staff has the task of preparing military plans of action after holding discussions with the political echelon.

Both the political and military echelons require not only a discourse of clarification and directives in the spirit of the "IDF Strategy" document, but also a learning discourse during which the two sides will learn which military moves are possible and what costs are needed to achieve various military and political objectives. This discourse will also allow the political echelon to study the military's capabilities in depth and the meaning of force construction and its use in various confrontation scenarios. It will require the political echelon to make decisions on the allocation of resources (the defense budget) and be responsible for the outcomes of these decisions. As part of a learning discourse, it behooves the government already to begin a discussion of the "IDF Strategy" document and adapt it to its political objectives as well as discuss the many issues not raised in the document.[47] All of these would improve the congruence between the political objectives and the military action, and they would reduce the probability of a crisis of expectations within both the political echelon and the public vis-à-vis the IDF's performance in the next round of fighting.

As for coordinating expectations of the IDF, based on possible confrontation scenarios and military responses to them as described in the "IDF Strategy" document, it should be understood that every method

of action has its risks and opportunities. Therefore, it seems unreasonable to instruct the IDF to embark on a limited campaign and expect an overall victory, as perhaps some segments of the public and their elected officials expected in the last rounds of fighting with Hamas. Although in the document the chief of staff asks for directives from the political echelon on deploying the military "when necessary," we do not think that the military should wait for the moment of truth, as was the case in the abductions that led to the Second Lebanon War and Operation Cast Lead. Rather, the military and political echelons need to prepare together in advance for responses to situations in which the IDF may find itself, many of which can already be anticipated: various terrorist attacks, unusual armament of the enemy, disaster scenarios, and so forth. Already now the cabinet should debate missions and objectives that the IDF will be asked to carry out and achieve in predictable scenarios, so that when the moment of truth arrives the relevant plans will already be in place. For its part, the political echelon will have the knowledge, be prepared to speak with the military, and be able to decide on one of the three basic states of military functioning as described in the "IDF Strategy" document.

When the chief of staff feels that a situation necessitates the deployment of the military, even though the political echelon does not ask for it, then it is the chief of staff's responsibility to initiate contact with the political echelon. During a conference about Operation Cast Lead, former Chief of Staff Gabi Ashkenazi expressed to that effect that "strategic decisions must be made in a discourse between the political echelon and military echelon before the war. That is when you formulate the objectives. The military echelon and the chief of staff must be there, must be partners in the discourse, and if such a discourse does not exist they must generate it; that is their obligation. When such a discourse is created, the chance for error is reduced."[48]

The "IDF Strategy" document does not name those who should participate in the discussions between the military and the political echelon other than the chief of staff. Even though the connection between the two echelons runs through the chief of staff alone, it is recommended that many military officers should participate in the discussions with the political echelon and voice their opinions, even if they do not agree with the chief of staff. Furthermore, we suggest to include the deputy chief of staff, as number two in the senior military ranks, in all contact with the political echelon. We also propose expanding the presence of the military echelon in discussions with

the political echelon as part of the learning discourse while differentiating between professional military and political positions.

Notes

1 Chief of Staff's Bureau, "The IDF Strategy," August 13, 2015, http://www.maariv.co.il/news/military/Article-493493.
2 According to the media, the document was approved by the defense minister and one may assume also by the prime minister. See Ron Ben-Yishai, "This is How We Will Operate. This is How You Will Deploy Us: IDF Strategy" *Ynet*, August 13, 2015, http://www.ynet.co.il/articles/0,7340,L-4690634,00.html (Hebrew).
3 Mordechai Kremnitzer and Ariel Bendor, *Basic Law: The Military* (Jerusalem: Hebrew University, 2000), (Hebrew).
4 Richard H. Kohn, "How Democracies Control the Military," *Journal of Democracy* 8, no. 4 (1997): 140-153.
5 Douglas L. Bland, "A Unified Theory of Civil-Military Relations," *Armed Forces & Society* 26, no. 1 (1999): 7-25.
6 Kobi Michael, "The Dilemma behind the Classical Dilemma of Civil-Military Relations," *Armed Forces & Society* 33, no. 4 (2007): 518-546.
7 Samuel Huntington, *The Soldier and the State: The Theory and Politics of Civil-Military Relations* (New York: Vintage Books, 1959).
8 Morris Janowitz, *The Professional Soldier – A Social and Political portrait* (Glencoe: Free Press, 1960).
9 For more on competing theories and basic concepts, see Kobi Michael, *Between Militarism and Statesmanship in Israel: The Military's Influence on Transitional Processes from War to Peace* (Tel Aviv: Tel Aviv University, 2008), pp. 17-45 (Hebrew).
10 Bland, "A Unified Theory of Civil-Military Relations."
11 Gershon Hacohen, *What Is National about National Security*? (Ben Shemen: Modan and the Defense Ministry, 2014), p. 55.
12 Ibid, pp. 52-53.
13 Rebecca L. Schiff, "Civil-Military Relations Reconsidered: A Theory of Concordance," *Armed Forces & Society* 22, no. 1 (1995): 7-18.
14 Rebecca L. Schiff, "Concordance Theory, Targeted Partnership and Counterinsurgency Strategy," *Armed Forces & Society* 38, no. 2 (2012): 318-339.
15 Linda Robinson, Paul D. Miller, John Gordon IV, Jeffrey Decker, Michael Schwille, and Raphael S. Cohen, *Improving Strategic Competence: Lessons from 13 Years of War* (Santa Monica: RAND Corporation, 2014), pp. xii -xiii, http://www.rand.org/content/dam/rand/pubs/research_reports/RR800/RR816/RAND_RR816.pdf.
16 Ibid, p. xiii.

17 Kobi Michael, "The Israel Defense Forces as an Epistemic Authority: An Intellectual Challenge in the Reality of the Israeli-Palestinian Conflict," *Journal of Strategic Studies* 30, no. 3 (2007): 421-446.
18 Charles D. Allen, and Breena E. Coates, "The Engagement of Military Voice," *Parameters* 39, no. 4 (2009): 79.
19 Zvi Lanier, "The Conceptual Failure of Armies in Low Intensity Confrontations," *Maarakhot*, 365 (1999): 4-12 (Hebrew).
20 Kobi Michael, "The Failure of Learning in the Test of Matching Statesmanship to Militarism in the Middle East Fight against Terrorism," *POLITIKA: The Israeli Journal of Political Science and International Relations* no. 25, (2016): 1-25 (Hebrew).
21 For more on the learning discourse between the echelons, see Ibid.
22 Yitzhak Rabin and Dov Goldstein, *Service Book*, vol. 2 (Tel Aviv: Maariv Publishers, 1979), pp. 412-414 (Hebrew).
23 Kremnitzer and Bendor, *Basic Law: The Military.*
24 Shmuel Even and Zvia Gross, "Proposed Legislation on the IDF: Regulating Civil-Military Relations in the Wake of the Second Lebanon War," *Memorandum* (Tel Aviv: Institute for National Security Studies) 93 (April 2008), (Hebrew), http://www.inss.org.il/uploadImages/systemFiles/Memo%2093_Hebrew.pdf.
25 Amir Oren, "The Report the IDF Preferred to Bury: Sharon, Begin and Raful's Fraud in the Lebanon War," *Haaretz*, May 4, 2014 (Hebrew).
26 Amir Oren, "IDF study: Sharon Contributed to the Failures of the Lebanon War," *Haaretz*, September 17, 2012 (Hebrew).
27 For more on these issues, see Michael, *Between Militarism and Statesmanship in Israel*, pp. 121-189.
28 Winograd Commission, *The Commission of Inquiry into the Events of the 2006 Campaign in Lebanon: The Final Report of the Winograd Commission*, vol. 1 (January 2008), pp. 578-581 (Hebrew), http://www.nrg.co.il/images/news/doah.pdf.
29 Ben Caspit, "'Mano a Mano': The Peretz-Halutz Conversation that Caused a Storm," *Maariv*, October 8, 2008 (Hebrew).
30 Lt. Gen (res.) Gabi Ashkenazi, "On Operation Cast Lead," Conference on Operation Cast Lead: Strategic Decision-Making Processes, Fisher Institute for Air and Space Strategic Studies, July 7, 2012, Youtube video, https://www.youtube.com/watch?v=D5XsEyYV-nE&feature=plcp.
31 Tzipi Livni, "On Operation Cast Lead," Conference on Operation Cast Lead: Strategic Decision-Making Processes, Fisher Institute for Air and Space Strategic Studies, July 7, 2012, Youtube video, https://www.youtube.com/watch?v=9XE6O8ch2wg.
32 The Mossad and the General Security Services are subordinate to the prime minister and are counted as part of the security services.
33 *Uvda* investigative journalism program, aired on Israeli television, November 2012.

34 Shmuel Even, "The Israeli Strategy against the Iranian Nuclear Project," *Strategic Assessment*, 16, no. 4 (January 2014): 7-20, http://www.inss.org.il/uploadImages/systemFiles/ADKAN%20-%2016.4999618133.pdf.
35 Amir Rapaport, "Yair Naveh in First Interview about Operation Protective Edge and the IDF's Professional Conduct," *ISRAELDEFENSE*, January 10, 2015, (Hebrew), http://tinyurl.com/rapaport2015.
36 Yotam Hacohen, "From Decision-Making to Learning – Thoughts in the Wake of the Drucker-Amidror Debate," *Dualog Blog*, August 14, 2014 (Hebrew), http://tinyurl.com/hacohen2014.
37 Gili Cohen, "Procedure on destroying the tunnels distributed only during the fighting, soldiers on the ground had to improvise," *Haaretz*, August 16, 2014 (Hebrew), http://www.haaretz.co.il/.premium-1.2398360.
38 "The IDF Strategy," Section 6-7, p. 10.
39 Ibid.
40 Ibid, pp. 23-24.
41 Ibid, Section 3, p. 14.
42 Ibid, Section 3, p. 14.
43 Ibid, Section 7, p. 10.
44 Mordechai Bar-On and Pinhas Ginossar, "Interviews with Maj. Gen. (res.) Israel Tal," *Studies in Israel's Rebirth* 10 (2000): 48 (Hebrew).
45 Amir Oren, "Renewed war possible," *Haaretz*, June 8, 2012 (Hebrew), http://www.haaretz.co.il/1.1726596.
46 Shmuel Even and Kobi Michael, "IDF Strategy and the Dimension of Time," (in preparation).
47 Shmuel Even, "The IDF Strategy and the Responsibility of the Political Leadership," *INSS Insight*, no. 736 (August 19, 2015), http://www.inss.org.il/uploadImages/systemFiles/No.%20736%20-%20Shmulik%20for%20web.pdf.
48 Lt. Gen (res.) Gabi Ashkenazi, "On Operation Cast Lead."

Information-Sharing Challenges in an Intra-Sectorial Environment

Gabi Siboni and Hadas Klein

Information sharing in cyberspace includes the sharing of attack methods, tools and means of attack, targets of an attack, weaknesses discovered, and ways of dealing with threats. Information sharing constitutes a strategic defensive principle. It is aimed at enhancing general strength in cyberspace. Various and diverse information-sharing initiatives are currently operating in Israel and throughout the world, but they are not as effective as they could be.

This article addresses a number of economic and political challenges facing intra-sectorial information-sharing initiative, and examines the extent of their influence, and gives examples of similar challenges in other fields. Finally, we make recommendations in order to minimize the effects of the challenges imposed upon the design and implementation of information-sharing plans in an intra-sectorial environment.

Keywords: cyber security, cooperation, information sharing, privacy, regulation, information security, trust, competition, "free-rider problem"

Introduction

One of the developing principles for strengthening cyber defense is the sharing of concrete and reliable information about existing weaknesses,[1] methods of attack, identification of attackers and motives, and so forth. This sharing is designed to enable the party receiving the information to quickly put defenses in place, thereby preventing the threat of attack from spreading. There should be a model for information sharing among organizations operating in the same market sector and exposed to similar

Dr. Gabi Siboni is the head of Cyber Security Program at the Institute for National Security Studies. Ms. Hadas Klein is the Cyber Security Program Manager at the Institute for National Security Studies.

threats from within their own sector due to having a common denominator, such as political affiliation, common enemies, and so forth or threats from other sectors. This is in addition to information sharing between the private and government sectors as well as state authorities from various countries. More comprehensive information sharing will create better defenses and enable more effective handling of cyberattacks.[2]

Information sharing contributes to the strengthening of general cybernetic resilience[3] at all stages of a cyberattack – from the early states in which the attacker gathers intelligence in order to locate his target to the advanced stages in which the attack actually takes place. Effective and extensive information sharing can contribute to better defense against a cyberattack,[4] among other things, by keeping early-warning mechanisms up-to-date, precise, and relevant; supporting actions to prevent cyber threats from being implemented; improving detection efforts in order to identify an attack at an early stage; facilitating precise analysis of the extent of the damage; and improving reaction and recovery processes when an attack is detected.

One famous cyberattack, highlighting the acute need for information sharing, is the "Great ATM Heist."[5] As part of this attack, a gang of hackers stole $45 million in two individual operations. Members of the gang succeeded in increasing the credit ceiling in bank accounts all over the world, and in making tens of thousands of cash withdrawals before being caught. The heist took place in two stages. During the first stage, on December 21, 2012, the hackers obtained information from five bank accounts, and increased the credit ceiling for those accounts. On the same day, field teams withdrew $5 million in cash from 4,500 ATM machines. During the second stage on December 19, 2013, the cyber thieves were more daring. This time, they obtained information about twelve bank accounts, and began a series of 36,000 withdrawals from ATM machines in New York and twenty-four other states in the United States and around the world, netting $40 million.

An important lesson in this case is the lack of cooperation between the agencies investigating the affair and between the parties at the banks responsible for preventing attacks and securing information assets. Law enforcement agencies were provided with details about the method of attack and the characteristics of the attack tools almost from the moment the first theft took place. Although they shared their analysis of the attack with the banks that had been attacked, due to a lack of effective sharing procedures, an overall picture of the situation did not emerge, and nobody

communicated relevant information to other financial institutions in a way that would enable them to prepare for similar attacks.

Together with the obvious advantages of information sharing, the drawbacks should also be noted, including the possibility that information-sharing mechanisms are liable to help the attackers and also provide useful information for new attackers, in addition to other risks that exist as part of the information-sharing process.[6] Nevertheless, the consensus among content experts is that the advantages of information sharing outweigh the disadvantages and risks, and that wise use of information-sharing mechanisms will enhance overall cybernetic resilience.

The aim of this article is to focus on the challenges and complexities facing information-sharing initiatives operating in the intra-sectorial sphere; analyze successful examples of intra-sectorial cooperation from other content areas; and finally provide recommendations for increasing the effectiveness of information-sharing initiatives in the intra-sectorial sphere.

The Sharing Space

In an ideal situation, companies whose databases are hacked – whether for criminal, espionage, or political objectives – will undertake a number of measures during the recovery process so that they can return to their routine functioning. First and foremost, they will contact law enforcement agencies and ask them to investigate the attack and prosecute the perpetrators. They will also inform their clients in order to jointly monitor actions and assess the effects of the attack in order to reduce the likelihood that it will spread, in addition to their duty to report the incident to the authorities, consumers, suppliers, and so forth. This is especially critical in the event of hacking of databases containing users' particulars. In cases in which the company attacked is a public one, the details of the attack will also be reported to the relevant securities authority and to the general public so that investors can make decisions about their investments in the company. Finally, the company will share information about the attack with other companies in the same sector,[7] which are likely to be exposed to the same threat. This information sharing should take place through a sectorial information-sharing center, which will receive the data, draw up a status report, and pass on the relevant details of the attack to the other companies in the sector, while simultaneously giving relevant information to inter-sectorial sharing agencies, such as national situation rooms.[8] For sharing to be effective and comprehensive, it must be focused and solidly based,

and it must take place in the **inter-sectorial** area – that is, among entities belonging to different sectors – and in the **intra-sectorial** area, among entities belonging to the same sector.

Every year, on April 7, the hacker organization "Anonymous" attacks entities identified as Israeli, labelled as an OpIsrael# attack. Preparation for this attack requires inter-sectorial information sharing among different sectors (media, health, transportation, financial, energy, and so forth). As part of this information sharing, state agencies, such as the national situation room, the Israel Security Agency, and the National Cyber Bureau convey information to all the relevant sectors in the Israeli economy. In some cases, the information is conveyed to sectorial cybernetic centers, which are currently being created in Israel, such as those of the energy and banking sectors.[9]

Intra-sectorial information sharing is also of great importance. Many investigations of cyberattacks indicate that the methods of operation, exploitation of breaches and weaknesses, and even phishing attacks typically spread throughout a single sector. Investigations of the modes of operation of criminal groups in cyberspace show that they are very active in gathering preliminary information on a sectorial level.[10] Furthermore, the malware development industry is characterized by specialization, sometimes based on sectorial systems. One such group is the Lizard Squad hacker group,[11] which focuses on developing malware specifically for gaming websites and attacking them.

Intra-sectorial sharing should be based on a model in which a group of information producers and consumers share information with each other. Instead of sending it directly to each other, however, the information is sent to a central administration, which then disseminates it to all the other consumers. This information is shared on the basis of its relevance for each sector – for example, information about a tool that attacks an existing weakness in a system that is widely used in a specific sector. Indeed, the sharing center serves as a clearing house for information for various organizations that serve as both producers and consumers of information.

One example that highlights the need for simultaneous, two-dimensional intra-sectorial and inter-sectorial information sharing is among developers and vendors of cyber defense technologies who share information with their colleagues in the sector in order to maintain a database of threats and weaknesses that is up-to-date, relevant, and precise as possible for all cyberspace users. This is in addition to the inter-sectorial sharing of

information with law enforcement agencies and state authorities in order to assist in the battle against cybercrime.[12]

The following is a schematic description of the information-sharing space:

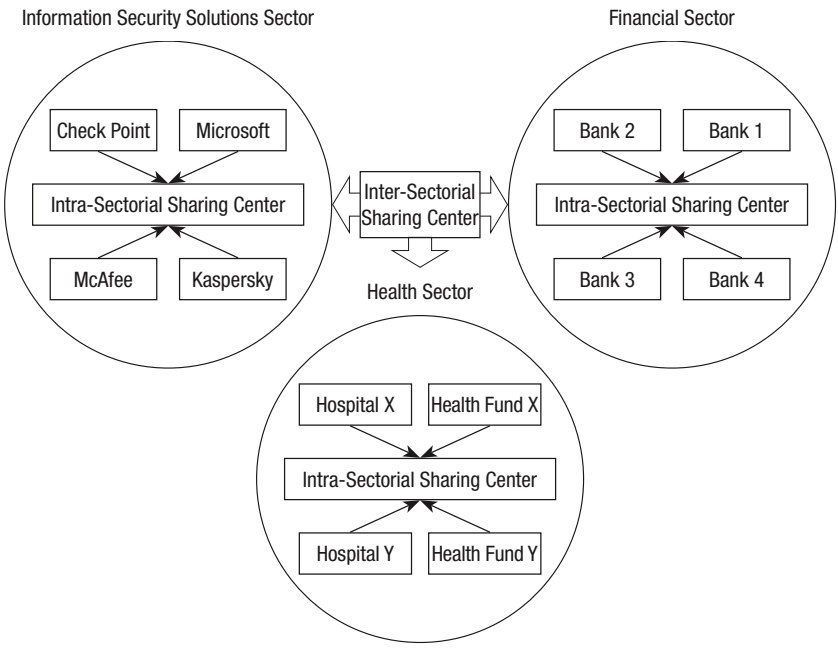

Figure 1: The Information-Sharing Landscape

Information-Sharing Challenges within the Same Sector

Even though information sharing has become a frequently-used term with a clear purpose among those working in cyberspace security, actual information sharing is only partial. Not many entities actively share information, while the volume of shared information and its relevance do not meet the needs of a given sector.

A study that examined the incentives and obstacles to sharing information about cyber threats found that the obstacles included economic ones, resulting from economizing, and concerns for the quality of the shared information, its value, and its use.[13] Concerns about receiving information of poor quality, exposing information security incidents that are liable to affect an entity's reputation, and poor management in information-sharing enterprises were the main impediments. It also emerged that companies

and organizations are reluctant to share information, out of fear that the information could prove useful to their competitors,[14] or that information sharing could harm a company's public image, by giving the impression that it is unable to protect its assets, leading to a drop in its sales and value.[15] Another impediment is what economists call the "free rider problem"[16] – a situation in which there is a lack of reciprocity; that is, competitors use the information received for their benefit, but do not contribute their own information to benefit others.

Most of the studies describe impediments to information sharing that are common to the specific sectorial environments of the companies and organizations. If they were not operating in the same sector environment, it would be reasonable to assume that these impediments would not have any impact. In fact, it can be concluded that that one of the significant factors hindering the development of successful information-sharing enterprises is the competitive factor. Organizations operating in a competitive environment find it difficult to launch information-sharing enterprises, even though it is clear to them that such sharing is useful to all the participants.

Competition and Cooperation – The Theoretical Background

Competition and cooperation are ostensibly two fundamentally opposite principles. The question, therefore, is whether they can exist together. Under conditions of competition without cooperation, the individual interest takes precedence over the group interest. On the other hand, when those cooperating rely entirely on their partners, a state of inefficiency prevails. It is therefore essential to find a point of equilibrium at which a certain level of cooperation occurs between the organizations active in the same sector and that is useful to all. Later, it is important to invest efforts in creating a solid basis for cooperation, so that competition and cooperation complement each other and coexist simultaneously.

Cooperation between competing entities will work in practice, and will improve their defense only if it includes a combination of competition and cooperation in a way that provides advantages to all the participants in the long term. Brandenburger and Nalebuff introduced the concept of "co-opetition" in a book they wrote in 1996.[17] They define co-opetition as a business strategy consisting of both cooperation and competition, aimed at achieving cooperation between competitors in order to obtain advantages that cannot be acquired any other way.

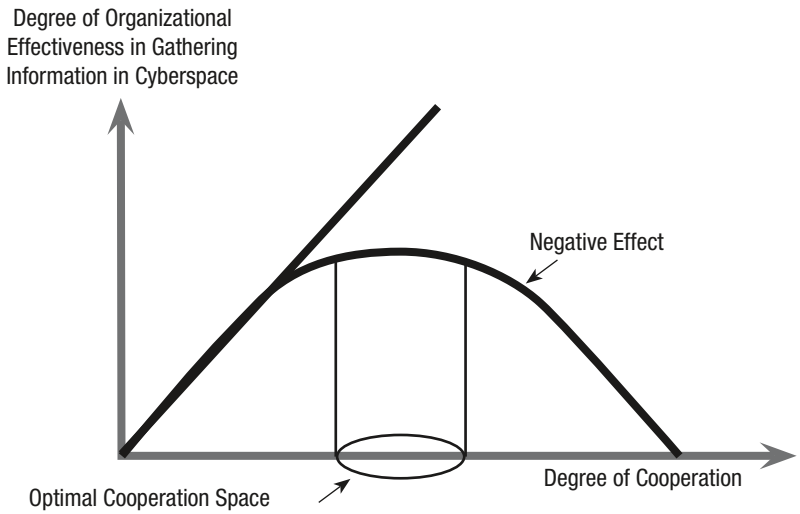

Figure 2: Point of Equilibrium in Cooperation

According to the co-opetition strategy, in order to obtain more business opportunities and increase profits, it is preferable to increase the total number of shared opportunities with competitors through cooperation, rather than making endless efforts to be better than them; in the context of cyberspace security, cooperation has great value. One example of co-opetition can be found in the challenging competition between the South Korean company Samsung and the Japanese company Sony; the two giant companies significantly improved their innovation processes and also encouraged small manufacturers to take part in the process and promote shared intra-sectorial interests.[18] On the other hand, some companies working in development believe that there is no room for cooperation based on an exchange of information. This thinking usually reflects their concerns that competing organizations will steal their ideas, or that cooperation will cause the competitors to produce better products.

Finding a balance requires analysis of the success factors in other sectors where structural processes of cooperation have been adopted, despite competitiveness and careful guarding of intellectual property. One example of a successful cooperative sectorial enterprise is in banking. In the early days of ATM machines in Israel, a customer could withdraw cash only from the banking network to which he belonged, and only from machines located within that network's branches. For example, a Bank

Hapoalim customer could not withdraw cash from a Bank Leumi machine. A few years later, the Automated Banking Services (ABS) company was founded and placed ATM machines in public places, serving customers of all banks. At a later stage, the banks agreed to improve their service by allowing every customer to use all of their ATM machines in Israel. In the past, ABS also considered establishing a cyber center for the financial sector in Israel, and submitted a request for this purpose to the director general of the Antitrust Authority, who was asked to assess the matter in the context of antitrust regulations in Israel. Recently it was decided to establish the financial cyber center as part of the national Cyber Event Readiness Team (CERT). One of the challenges facing the new center will be eliminating the "free-rider problem," − that is, finding a balance between the banks that will ensure continued optimal information gathering and sharing.

Another example of sector-wide cooperation can be found in the pharmaceutical industry. This industry regards cooperation as essential, and it shares information through a third entity that mediates between information requests and research. Many drugs were developed on the basis of research conducted in an open-source environment. One example is an enterprise formed in 2010 in which major drug companies, entrepreneurs, and research institutes combined forces in order to promote research methods for the development of drugs for two common mental illnesses.[19] This enterprise was created with the understanding that despite the enormous progress of knowledge in molecular biology and the prodigious efforts of all the parties engaging in drug development, the pace of developing new drugs had slowed; this was most likely due to the intensifying competition between rival drug companies on the one hand and the limited scope of information exchanges between academic institutions and the industry on the other.

The world of information technology can learn from cooperation between competing technological companies that have joined forces in order to establish standards for products and new technologies. For example, establishing standards for various detachable information-storage devices, such as video, DVD, and so forth, is a regular area of both cooperation and competition between Sony, Philips, Kodak, and many other companies.

Cyber-Information Sharing in a Competitive Environment

Two principal motives for competition between organizations in the context of cyber security and the players operating in the information-sharing sphere can be discerned: economic competition and competition for credit.

Economic Competition

Economic competition results in difficulties in cooperating, due to desires to achieve commercial supremacy and to increase the market share. This type of competition exists mainly among profit-driven organizations. In the context of cyber security, this type of competition can be found among companies that develop cyber defense products and services, such as anti-virus producers, firewall producers, managed security-service providers (MSSPs), and so forth.[20]

The purpose of information sharing between companies that provide cyber-security services is to create an optimal sharing infrastructure that will enable every threat discovered in one company's products to result in the updating of all the companies' security solutions, thereby improving the overall protection for cyber-security consumers. In order to bring about such information sharing, these companies must realize that despite the element of competition, cooperation between them is worthwhile. One especially difficult challenge is with the group of producers whose main business is cyber security.

From a commercial standpoint, companies that develop defense products understand that the databases on which their various products rely (such as the digital signatures of malware) are the raw material at the core of their systems. A security engine, however sophisticated, will not provide an appropriate and up-to-date solution if it relies on partial or irrelevant data. The reliability and current validity of the data are therefore among the most important factors in the quality of the systems and a key factor in their commercial success. Under conditions of competition, conveying information across-the-board among the producers of the various technologies is very difficult to achieve, especially among companies for whom this information constitutes the basis of the competition between them. Cooperation between MSSPs is also very limited. This sharing takes place only occasionally, and there are no structured mechanisms or processes for keeping the data up to date.

We are now witnessing a number of information-sharing initiatives in the cyber-security technologies sector. These enterprises are operating

simultaneously, and the companies that promote the enterprises have called upon others in the sector to join them. This has created a situation in which various companies within the cyber-security technology sector try to promote solutions to a problem; in doing so, they aggravate one of the greatest obstacles to finding a solution, and in effect, contravene the basic principle for which the enterprises were founded – cooperation for the purpose of creating added value. An example of this can be seen in the announcement in October 2014 of the establishment of the Cyber Threat Alliance enterprise by the companies of Fortinet, Palo Alto Networks, Symantec, and Intel Security, all which deal with cyber security technologies, while Microsoft is also promoting a similar initiative called VIA.

For information sharing to be effective in the way that the companies convey and receive the information when it is still "hot and relevant," it must be based on automated information-sharing solutions. A number of standardization activities are taking place in this area, supported by the US Department of Defense, under a shell architecture called CyBOX.

Competition for Credit

This competition stems from the difficulty of sharing information, resulting from the desire for professional esteem and a good reputation; the idea that knowledge is power; and an inter-organizational culture sometimes characterized by power struggles. This type of competition is also found among countries; agencies working to promote and improve the level of national cyber security; and non-profit entities, such as research institutes and academic institutions.[21] The advocates of inter-organizational coordination and integrative plans assert that the problems facing a country are complicated, and dealing with them therefore requires an integrated approach. They recognize the fact that coordination can create economies of scale, and that a measure taken by a number of organizations is more powerful and effective. Nevertheless, multiple plans and the overlap between them requires great coordination, which complicates information sharing and detracts from its effectiveness.

One of the models,[22] which examined ways of dealing with obstacles within the framework of cooperation between state agencies, raised a number of points that require attention in order to overcome these impediments:

1. **Sovereignty**: An organization customarily regards itself as a sovereign entity within its content world and within its authority. A state organization will therefore cooperate only if it directly contributes to the

organization's objectives and goals. Even in cases in which cooperation is backed by a binding policy, a certain degree of voluntary participation is needed. People consider first and foremost the direct contribution that cooperation will provide for their organization before they will consider cooperative efforts that will benefit others.

2. **Complexity of cooperation**: Defining processes of information sharing is complicated, and includes a certain degree of uncertainty about the right way to proceed. It is important to address this aspect in the process-outlining stage by adding monitoring and feasibility tests.
3. **The dimension of size**: Smaller organizations are likely to perceive cooperation with larger organizations with ample budgets as threatening and non-voluntary. This lack of balance leads to opposition in the coordination processes.
4. **Organizational culture and work methods**: Every organization has its own unique organizational culture, including planning methods, monitoring, and timetables. Each organization tends to regard their own work methods as the best and most suitable.
5. **Communication and language gaps**: Every organization has its own patterns of communication and unique terminologies. It is important to define a common language that all the partners can understand.
6. **Asymmetry of the participants**: Assuming that the participants are not equal in strength and size, they should be asked what volume and quality of information they will be able to supply, compared to the volume and quality of the information received.
7. **Instability and uncertainty**: Cyberspace is characterized by many risks. Thus, sharing technological tools that contain elements of a company's intellectual property could expose the information to undesirable parties.
8. **Incentives for sharing**: Cooperation through an agency responsible for coordination will not solve all the problems and obstacles encountered. It is important to devise incentives that will encourage all the partners to contribute to the joint effort.

One fruitful example of information sharing can be seen in the activity of a forum called Intellipedia, which was founded after the terrorist attack on the United States in September 2001. As a result of the attack, decision makers in the American security services realized that the idea of each agency developing and managing knowledge by itself did not contribute to national security; the intelligence information did not flow between the country's various security agencies, resulting in their inability to thwart the

attacks. The American security apparatus therefore established a joint forum facilitating information sharing between various organizations. Although here, too, we see competition for resources, sources of information, and prestige, the forum's success is based on the realization of the various organizations that information sharing can only benefit the public and enhance national security.

Since the beginning of the twenty-first century, initiatives for data-sharing centers have been operating in the United States in various sectors, such as health, finances, and so forth. These initiatives are called information sharing and analysis centers (ISAC), and they all operate according to similar principles. The National Council of ISACs (NCI) was formed with the objective to encourage intra-sectorial information sharing by formulating work principles and procedures, and to promote connections between the various centers. Member organizations share ownership of these enterprises, and receive technological and economic support from the US Department of Homeland Security.

Companies operating in the same sector naturally compete with each other, but they cooperate in this area because cyberspace is not the essence of their business. For example, the Financial Services Information Sharing and Analysis Center (FS-ISAC) focuses on information sharing in the financial sector in the United States. This center operates according to the following operative principles: the organization belongs to its members, is managed by them, and maintains databases containing information about cyberattacks, physical security attacks, threats, weak points, and solutions. The information is gathered from both the organization's members and external parties, such as government security agencies and other ISACs. There are several levels of membership in a center, and payment is determined according to level of service: a higher level of membership means the organization receives more services and is exposed to more information. In the operational aspect, information can be conveyed to the FS-ISAC either anonymously or openly. The information is checked by a team operating around the clock, which analyzes and classifies the data, and conveys the information to the members in accordance with the principles.

A study conducted following a number of serious cyberattacks in the financial sector and among the FS-ISAC member organizations examined alternative models for promoting and improving information sharing from both a quantitative and a qualitative perspective.[23] The study included the

use of game theory tools, which were used to examine the existing models for payment of membership fees in ISACs and their effect on the level of sharing. The research showed that most of the existing models in ISACs create an imbalance between the high expectations of the members to obtain information and their reluctance to share information, and is inconsistent with the declaration of intent made by each member upon joining the ISAC.

The study also considered an innovative theoretical model based on the idea that payment for membership in ISAC can be used as an insurance policy providing coverage for damage caused by a cyberattack, in contrast to the accepted models based on payment of membership fees according to the level of use. The developers of the new model showed that when payment for membership in ISAC is based on levels determined by the extent of use, the member organizations do not have any incentive to share information about cyber incidents with their colleagues. In contrast, when the model is based on paying a premium according to the size of the expected loss for all the organizations, and for which in exchange they receive an insurance policy funded from a general pool of premiums, the members show an interest in information sharing; each organization is safer when all the other organizations are more secure.

Recommendations

Given the above analysis, and based upon the assumption that intra-sectorial information sharing is extremely important to improving the overall defense of a sector, several recommendations can be made to assist in the successful establishment of cyber-information-sharing initiatives in a single sector environment:

1. **Mapping of partners**: At the stage of initiating, developing the idea, and understanding the expected results, potential partners should be mapped, and thought should be given to the desired composition of the partners. At this stage, initial exploration of potential partners should be conducted, and each party should consider whether it is willing in principle to join the partnership. It is best to define as precisely as possible the results that the sharing enterprise seeks to achieve and the tools at its disposal, including technological, regulatory, economic, public relations, and other capabilities.
2. **Cost-benefit ratio**: Organizations are not eager to share information at any price. Successful information sharing requires that the benefit for each party outweighs the time and costs involved in the partnership. In

certain cases, incentives should be considered to encourage support for information sharing. It is important that organizations recognize and understand the quantitative advantage and economic value of successful sharing. This method has been found to be effective in creating an incentive for sharing processes, as well as within the context of securing the budget for the information-sharing enterprise. The budget should be determined in the initial stages of the enterprise, so that it will be clear to all the partners who is bearing the costs of the plan.

3. **Types of partners**: It is recommended to define the partners for the enterprise. A distinction should be made between three types of partners – interested parties, owners of information, and parties that have authority – as well as an assessment of their importance and contribution to making the enterprise more effective. Every partner has a unique perspective. In order to increase trust among the partners, communications between them should be structured, and a common language created. It is important to create a "shared experience," and to devise routine operations, which should be agreed upon in the planning stages of stage of the enterprise.
4. **Commitment and authority**: All the partners should give a minimum commitment at every stage, from the initiating and planning stage to the implementation and periodic assessment of the plan's effectiveness. A number of key questions concerning the authority to make decisions, leadership of the entire process, and timetables need to be considered, as well as who should be included, when they should be included, and how it should be done. The partnership's success depends on each partner knowing in advance what they are expected to contribute to the process and what they will receive in return. The sphere of action and areas of responsibility should be determined for each partner, and the interdependence between the partners should be stressed. It is recommended to announce the leading party that has authority and responsibility for the process and its results in the early planning stage. Two types of leadership can be specified: professional, led by the most relevant responsible and professional partner, and operational, led by a partner with methodological expertise in managing cooperative processes, and who is perceived as being free of any personal interests. An individual committed to the common goals should be appointed to head the project.

5. **Ego and prestige**: Dealing with ego and prestige requires advance preparation. Instead of assuming that ego does not play a role, and that everyone acts according to professional considerations, it would be better to assume the opposite. The uniqueness of the players should be emphasized, and the ego regarded as a professional value that each entity brings to the information-sharing plan. It is important to recognize the limits of responsibility of every organization, and to give space to each organization's accumulated experience and knowledge,
6. **A decision-making mechanism**: Solving disputes requires a mechanism for making decisions within the framework of the partnership. The decision-making mechanism in situations of conflicts already should be defined in the planning stage. It is important to recognize that when dealing with disputes, it is essential to clarify them and reach agreement among the partners about the nature of the dispute. Discussion and dialogue need to be thorough before a decision can be made, and a large degree of transparency should be encouraged.
7. **Monitoring**: Monitoring and assessment mechanisms are critical for success. Monitoring should take place through orderly mechanisms anchored in joint activity, upon achieving periodic targets and measures. These targets and measures should be taken into consideration during the implementation stage, and they will assist in making correct data-based decisions, preferably by an objective external agency. Based on the summary assessment, a decision can be made regarding the extent of implementing the plan, and whether it needs innovations and changes. It is important also to periodically evaluate the external changes that are likely to affect the effectiveness of the enterprise, such as regulatory and technological changes.
8. **Cooperation at the national level**: Public agencies at the national level, such as national CERTs and other government institutes, should be encouraged to share information with each other. It is important that these agencies are active in promoting cooperation and developing platforms that will provide solutions to the various obstacles that impede information sharing. A training program should be devised for creating, developing, and maintaining the skill and expertise necessary for operating information-sharing centers. At the same time, it is crucial to find a balance between state involvement in managing and carrying out sharing processes and the need of certain sectors to protect the shared information, due to its nature and sensitivity. There are some

sectors (e.g., the insurance sector) whose information is highly sensitive to privacy. In such cases, the state should allow independence in information sharing, with minimum intervention.

At the operative level of planning an information-sharing enterprise, it should be verified that the information is relevant to the partners, of appropriate quality, and timely. Forums should be held for this purpose, with the aim of defining all aspects of the sharing process. For example, sharing information about the Internet Protocol (IP) of a specific attacker is essential. At the same time, other unique attack characteristics should not be shared with others, in order to prevent misuse of the information shared.

Conclusion

Information sharing in the field of cyberspace is very important, as the information critical to coping with cyber threats is dispersed across countries and organizations all over the world. Information sharing can include reciprocal briefings about attacks (methods, means, targets); weaknesses; and methods for dealing with specific and general threats. Sharing of optimal information makes it possible to present an up-to-date and relevant picture of cyber threats at the sectorial, national, and global levels. Information sharing also lends support to decisions to invest in appropriate and relevant resources against the developing threats. Finally, successful information sharing also assists processes of research and development of solutions designed to counter cyber threats.

Currently many information-sharing initiatives are managed as state, sectorial, or private initiatives. One of the leading and most significant mechanisms is the information that security and defense companies provide to their clients – information that usually originates with the company's clients who have been attacked. The assumption is that this mechanism operates optimally. Another information-sharing mechanism regarded as highly effective, although not ideal, can be found in the sectorial CERTs. Many organizations are intuitively, informally, and only partially setting up information-sharing mechanisms. It is important to establish a global enterprise that will operate according to the operational principles of the information-sharing enterprise of the security companies. All the information gathered in the framework of a global enterprise will be cross-referenced and analyzed, as is done by the security companies' enterprise, and the processed information will then be sent back to all the clients of all the partners.

Despite the many obstacles that must be overcome in order to operate information-sharing initiatives, the establishment of CERTs is critical for improving general security in cyberspace. It is therefore appropriate for the mechanisms proposed here to be included as part of the "toolbox" for initiating, designing, and operating such centers.

Notes

1 This refers to weak points, sometimes identified and known, and usually resulting from faulty design, which an attacker is able to exploit in order to penetrate a system or disrupt its operation.

2 Experts on information sharing in cyberspace frequently have clamed that information sharing is risky, in that the information is liable to be revealed to the general public, thereby helping the attackers while also providing useful information to new attackers, in addition to other risks incurred in the process. For a thorough review of this subject, see ENISA, *Incentives and Challenges for Information Sharing in the Context of Network and Information Security*, (ENISA, 2010).

3 This is a broad concept that relates to the endurance and strength of cyberspace when facing the threats and risks liable to disrupt its activity or the way it is used.

4 Gabi Siboni, "An Integrated Security Approach: The Key to Cyber Defense," *Georgetown Journal of International Affairs*, May 7, 2015.

5 Marc Santora, "In Hours Thieves Took $45 Million in A.T.M. Scheme," *New York Times*, May 9, 2013, http://www.nytimes.com/2013/05/10/nyregion/eight-charged-in-45-million-global-cyber-bank-thefts.html?_r=1.

6 As noted above, a full review of the advantages and risks can be found in ENISA, *Incentives and Challenges for Information Sharing in the Context of Network and Information Security*.

7 A sector is a group of entities in the economy sharing similar characteristics, operating in a similar business environment, and having similar objectives, such as the "business sector."

8 National war rooms exist in many countries around the world. Their purpose is to assemble a national status report in cyberspace and coordinate information sharing between sectors and between state agencies and civilian entities.

9 Ami Rojkes Dombe, "Meet the Cyber Center for Energy in Israel," *Israel Defense*, November 25, 2015.

10 Lillian Ablon, Martin C. Libicki, and Andrea Golay, *Markets for Cybercrime Tools and Stolen Data*, (National Security Research Division, Rand Corporation, 2014), http://www.rand.org/content/dam/rand/pubs/research_reports/RR600/RR610/RAND_RR610.pdf.

11 Jimmy Blake and Amelia Butterly, "Who are Lizard Squad and What's Next for the Hackers?" *BBC*, January 27 2015, http://www.bbc.co.uk/newsbeat/article/30306319/who-are-lizard-squad-and-whats-next-for-the-hackers.

12 For a broad survey review covering the entities and initiatives promoting the sharing of cyberspace information, see Aviram Zrahia, "A Multidisciplinary Analysis of Cyber Information Sharing," *Military and Strategic Affairs* 6, no. 3 (December 2014): 59-77.

13 ENISA, *Incentives and Challenges for Information Sharing in the Context of Network and Information Security*.

14 Andrew Nolan, *Cybersecurity and Information Sharing Legal Challenges and Solutions* (Congressional Research Service, March 16, 2015), https://www.fas.org/sgp/crs/intel/R43941.pdf.

15 Maria Cristina Arcuri, Marina Brogi, and Gino Gandolfi, "The Effect of Information Security Breaches on Stock Returns," Università di Roma La Sapienza, 2014.

16 Russell Hardin, "The Free Rider Problem," *The Stanford Encyclopedia of Philosophy*, Spring 2013.

17 Adam M. Brandenburger and Barry J. Nalebuff, *Co-opetition* (New York: Doubleday, 1996).

18 Devi R. Gnyawali and Byung-Jin Park, "Co-opetition between Giants: Collaboration with Competitors for Technological Innovation," *Research Policy* 40, no. 5 (June 2011):650-663.

19 "Prof. Jonathan Rabinowitz from Bar Ilan University is one of the leaders of an international project to bring about a breakthrough in the development of a drug for common mental illnesses," Bar Ilan News, Spokesperson's Office, Bar Ilan University, December 7, 2010.

20 This consists of continuous monitoring services for information security systems and analysis and adjustments between data for early and proactive detection of threats. This analysis is conducted by cross referencing all the data obtained from all of the company's clients and sending the relevant information back to the companies.

21 In certain cases, this sector also features economic competition.

22 Susanna P. Campbell and Michael Hartnett, *A Framework for Improved Coordination: Lessons Learned from the International Development, Peacekeeping Peacebuilding, Humanitarian and Conflict Resolution Communities*, October 31, 2005, https://www.regjeringen.no/globalassets/upload/ud/vedlegg/missions/framework.pdf.

23 Charles Zhechao Liu, Humayun Zafar and Yoris A. Au, "Rethinking FS-ISAC: An IT Security Information Sharing Network Model for the Financial Services Sector," *Communications of the Association for Information Systems* 34 (2014).

The Israeli Home Front Command: Missions, Challenges, and Future Prospects

Meir Elran

The Israeli Home Front Command has undergone many phases of change until having reached its present level of preparedness for providing the adequate response to man-made security challenges. This level of performance raises several serious questions regarding its capacity to serve as Israel's primary agent of response to major disruptions, extensive man-made security hazards, and natural novel risks. Its future success in standing up to wide-scale challenges will depend not only on its own level of preparedness, but also on its capacity to work together with the other governmental agencies, the local authorities, NGOs, and the civilians as a whole. This will also depend on the level of societal resilience of the Israeli public. The Home Front Command is well aware of this precondition, and is investing lavishly to enhance it. But above all, it has to be remembered that the ultimate challenge is still ahead of us, be it security related or by natural cause, like a major earthquake.

Keywords: Home Front Command, resilience, man-made risks, natural hazard

Introduction

The IDF Home Front Command (HFC) was established as a territorial military command in 1992, as part of the lessons learned after the Gulf War, when – in a side theater – the Israeli civilian rear was attacked by thirty-nine Iraqi Scud ballistic missiles. While the actual damage to the Israelis was negligible, the psychological effect, however, was profound and opened a new era in the long history of military conflicts between Israel and its adversaries. From that episode until today, the nature of wars in the region has been completely transformed, placing the home front at the core of

BG (ret.) Meir Elran is the Director of the Homeland Security Program at the Institute of National Security Studies.

the military confrontations. This is in total contrast to the past, when the conflicts where shaped by the engagement of military formations on the borders and beyond them. This historical shift raises a series of questions that are still being debated in Israeli military discourse: What are the best strategies for protecting the civilian home front? What is the role of defense versus deterrence and offense in that sphere? Is it primarily the military's mission to protect the civilian front from the security threats it repeatedly faces? And consequently, how much should the IDF invest in this front, at the expense of its purely military missions?

These are the main issues that will be dealt with in this article. It will open with a historical analysis, followed by an examination of the HFC's present and foreseeable challenges. The article will conclude with some thoughts regarding the future role of the HFC and other agencies in providing appropriate answers to the various threats that challenge the Israeli civilian front.

Historical Background (1948-1992)

In May 1948, when the State of Israel was founded and as the Israeli Defense Forces (IDF) began to take shape, the Civil Defense (HAGA) was also established, and entrusted with the mission of "Bombardment Defense Service."[1] This took place following heavy bombings of Tel Aviv by the Egyptian Air Force, which resulted in 172 fatalities, many of them women and children.[2] LTC Mordechai Nimtza-Bi (1903-1949) was appointed to command the new force.[3] In 1951 the Israeli parliament (the Knesset) passed a law defining HAGA's legal status. It specified its mission as "to take all measures required to protect the civilian population from attacks by hostile forces, or to limit the results of such an attack, with an emphasis on saving lives."[4]

Generally speaking, from the War of Independence until 1990/1991, the Israeli home front did not face any real external threat, apart from occasional terrorist attacks. This was the case during the 1956 Sinai Campaign, the Six-Day War of 1967, the War of Attrition along the Suez Canal in 1968-1970, the Yom Kippur War of 1973 and the First Lebanon War of 1982. During these clashes, the civil defense was not challenged. HAGA units were neither equipped nor organized for dealing with major threats to the civilian population. The overriding notion was that the IDF was capable of sealing the borders to the extent that the regular police force, together with other civilian agencies, would be able to provide an adequate response to

any threat. The outcome was a slow deterioration of HAGA's professional effectiveness, and its marginalization in terms of resources.

In addition to HAGA, elements of HAGMAR, the Israeli Regional Guard, were incorporated into the rear forces. Initially, this quasi-military body was formed to protect the agricultural communities along the borders. Following the Yom Kippur War, it was decided to reinforce HAGMAR; in August 1977, HAGMAR was incorporated into the HAGA framework.[5]

The Immediate Background for the Establishment of the HFC

Operation Desert Storm in Iraq completely changed the course.[6] After the Iraqi invasion of Kuwait in August 1990 and the consequent US attack, the Iraqis attempted to draw Israel into the crisis. Indeed, on the night after the opening of the Coalition's attack (January 17-18, 1991), Israel was hit by a salvo of six conventional Scud missiles launched from western Iraq. Such attacks continued almost nightly throughout the Gulf War, mostly targeting the city of Tel Aviv. Altogether, by February 28, thirty-nine missiles had landed in Israeli territory; one person was killed and three others suffered heart attacks.[7]

It would be safe to state that Israel was far from being prepared for the Iraqi missile offensive. In terms of military defense, it had to resort to direct US support, manifested by the Patriot anti-missile batteries. Passive physical defense was scarce, particularly the one designed to deal with chemical warheads. Civil response capacities were minimal, mostly composed of primitive early-warning and alert systems; improvised "sealed rooms"; hastily distributed gas masks; as well as hastily established national information-dissemination systems. Many Tel Aviv residents left their homes, especially at night, thus raising a sharp public controversy on the issue of mass civilian evacuation under fire. Overall, public anxiety was quite high;[8] although in retrospect, the general impact of the episode on Israeli security doctrine was relatively minimal.

By and large, the country was ill-prepared for such a threat. The late General Ze'ev Livne, the first commander of the HFC, stated two decades later that the civilian rear was prepared for the war according to the standards of World War II.[9] This was the case both conceptually and practically. The surprise factor, that the country could be attacked by ballistic missiles, can presently be perceived as unrealistic. It was well-known that the Iraqis possessed the military capabilities. It should have been assumed that they might use them. This was not Israel's first major strategic surprise. Another

one happened in the 1973 Yom Kippur War. These should shed light on the possible severe impact of surprise attacks and on the country's need to prepare itself for future strategic surprises. In any case, it was clear that Israel's home-front capacities required drastic change.

The Establishment of the HFC

On February 2, 1992, almost a year after the end of the Gulf War, the Home Front Command was established as the fourth IDF command. General Ze'ev Livne was appointed its first commander. This was not an easy decision for the IDF leadership. The notion of granting the HFC even the image of a territorial command, supposedly equal to the other commands, was alien to the IDF's DNA, which is still uncomfortable with the concept of defense as a viable strategy. Hence, it was clear from the beginning that even though the HFC was officially declared to be a territorial command, its standing and, consequently, its resources would be far from equal to those of the other commands. The front combat commands would continue to share the primary burden and responsibility for the ground forces operations within their respective theaters of war. It was assumed that the HFC could not be trusted to effectively engage with serious challenges from hostile forces operating in critical arenas.

Three major considerations shaped the initial model of the HFC.[10] The legal consideration granted the HFC with the professional responsibility for the civilian rear, but denied it any authority in the field. The second consideration was operational, perceiving the HFC as a force designed to relieve the territorial commands from dealing with the civilian rear in times of conflict. Thirdly, the organizational consideration was meant to enable greater effectiveness and efficiency in coordinating with the other civilian emergency first-response forces. Based on that, the mission of the newly established HFC was:

a. To design and disseminate the doctrine of the civil defense;
b. Together with the civil agencies, to guide and train the civilian population in order to prepare it for emergency and equip it with the necessary means of defense;
c. To direct and guide first-response agencies in fulfilling their duties in the civil defense sphere, and to activate them and employ the equipment they hold;
d. To coordinate the activities of government ministries, local authorities, and the private sector in the realm of civil defense;

e. To act under the authority of the minister of defense to secure lives and property in circumstances not necessarily directly related to civil defense.

The functions of the HFC were officially defined as follows:[11]

a. To serve as the primary professional authority for all matters relating to civil defense, including rescue and recovery and handling hazardous materials;
b. To serve as a civil defense service;
c. To serve as the chief operational command for the activation of the units deployed in the rear;
d. To serve as the general headquarters for the buildup of the HFC units;
e. To serve as a territorial command.

These directives, while well-intended, raised some critical problems, which turned out to be real obstacles to the HFC's effective operation in years to come. The HFC was positioned from its inception as a relatively weak organization wedged between regular military commands on the one hand and civilian agencies on the other. It had to carve its professional base of operations in a narrow space between well-entrenched and relatively robust organizations that possessed legitimacy, reputation, resources, and professional clout. The net result created serious limitations on the young HFC, which was not provided with the necessary means to properly fulfill its mission. Indeed, the military high command, which was not supportive of the move,[12] as well as some of the high-ranking officers of the newly established HFC, did not grasp at the time the depth and breadth of their responsibility. For them, the HFC was meant to represent merely a quantitative or organizational expansion of the old HAGA. The only difference for them was that rockets and other high-trajectory explosives replaced the previous threats from aircrafts, against which the Israeli air force had managed to build an effective defense. At the time, and for another fifteen long years, the HFC was supposed to provide physical protection from enemy bombardments and to save lives. The security situation during those years (1992-2006) contributed to this narrow approach and to the HFC's marginal position. In fact, it was hardly called upon to participate in the dramatic security conflicts of the period – the First Intifada (1987-1993) and Second Intifada (2000-2004) – during which the civilian population was severely challenged.

The only positive development at the time was the one related to the sphere of passive defense. Based on the lessons of the Gulf War, Israel entered a new era in which it became obligatory for new residential buildings to

have a fortified room that could provide adequate shelter from conventional explosive and chemical weapons. Consequently, all new dwellings since 1994 have been equipped with shelters. The HFC was entrusted with the role of controlling this venture. Altogether, these shelters presently are found in more than one-third of all apartments in the country.

The Turning Point

The Second Lebanon War in the summer of 2006[13] found the HFC at its lowest ebb regarding its operational capacity.[14] Years of neglect, a paucity of means, and mostly a misguided conceptual framework contributed to the insufficient preparedness for the asymmetric war against Hezbollah. In this unbalanced hybrid conflict, the IDF suffered from numerous shortcomings,[15] only a few of which involved the HFC. Still, the challenge to the home front during the thirty-three days of that conflict was severe. Altogether, close to 4,000 rockets – an average of 120 a day – were launched against civilian targets in the northern part of the country. Although only less than a quarter of those actually reached populated centers, this was sufficient to cause 39 civilian fatalities, more than 2,000 injured, and approximately 12,000 buildings damaged, most of them slightly. Hundreds of thousands of inhabitants abandoned their homes for the duration of the conflict, and the total losses to the national economy reached about thirty billion Israeli shekels.

Despite these relatively moderate damages, it has been agreed that the home front was far from prepared for the challenge. The most important reason for the poor performance of the HFC was related to the issue of responsibility and accountability for the home front. Theoretically, the relevant laws, originating back in 1951 and later reinstituted in the 1990s, granted the civil defense system and later the HFC the authority to provide protection for the civilian rear. These regulations, however, are far from granting the legislative umbrella necessary for the HFC to operate effectively in the field. In fact, the 2006 Lebanon War attested to the fact that the HFC was unable to provide civilians with what was necessary under rocket fire, whether in the physical sense of passive or other means of defense, or in the broader sense of psycho-social civilian response. It was not only the HFC that was unprepared to provide the needed services; other agencies, including the national police force, the first-response civilian organizations, and numerous NGOs, were hardly prepared, not to mention the lack of meaningful cooperation between them.[16]

Furthermore, in the years before the 2006 war, the HFC had mostly focused on the establishment of search and rescue units,[17] and other tactical and logistical forces. It did not perceive its mission to holistically prepare and assist the population at large under emergency situations.

The Renewed HFC: Profile and Challenges

The 2006 conflict marked a turning point in the history of the HFC and the entire approach to the home front in Israel. The failures of the HFC and the lessons learned from previous conflicts brought about changes which contributed to better performance in the home front. Still, these changes have not yet resulted in the necessary transformation of preparing the home front as a whole to cope effectively with the growing challenges, posed by both man-made and natural hazards.

The 2006 Lebanon War was the second conflict – after that of 1990/1991 - which engaged the civilian rear in a widespread rocket and missile attack. It introduced Israel to the hybrid military conflict, which is characterized by parallel engagements on the military and civilian fronts. The initial concept was that the HFC was meant to relieve the armed forces from civilian concerns, so that they could focus solely on the military sphere. This proved to be a faulty assumption. One of the major lessons of 2006 was that it was practically impossible to disentangle the two fronts and operate separately on each, as one front influences the other in various ways. On the one hand, risks to civilians are a major factor for military decision-makers in determining what they should accomplish at the front in order to minimize or remove enemy threats to the rear. On the other hand, the events at the military front have a strong impact on the mood, morale, and resilience of the civilians. These central issues still need to be confronted and resolved.

Under these circumstances, the national strategy for the home front has, at least theoretically, undergone a transformation, beginning with the conceptual transition of the HFC from having a "narrow" to a "broad" approach regarding its core missions.[18] Hence, the HFC presently perceives itself as the leading body responsible not only for technical and logistical operations in the civilian sphere, but also for the entire spectrum of the civilian emergency routine, which encompasses all the needs of the civilian population and infrastructure in times of crisis. Consequently, the HFC now prepares itself in parallel tracks: It conducts its traditional missions by providing adequate and sophisticated early-warning systems, issuing

instruction for sheltering,[19] evacuating civilians from wreckage, and disseminating information to the civilian population on all relevant risks. When the chemical threat was present – until it was neutralized in Syria[20] – the HFC was also engaged in distributing gas masks, a massive logistic undertaking.[21] Presently, the HFC takes upon itself wider responsibilities for the enhancement of social resilience, even if at times encroaching on functions that traditionally have been the province of government ministries and local authorities. The HFC today understands and invests heavily in the realm of the behavior of the civilian population in emergency situations, at the preparatory stages, as well as during crises.[22]

These developments stem from dramatic external changes in the area, which make homeland security in Israel more complex and demanding:

a. The high-trajectory weapon systems possessed by Israel's immediate adversaries are becoming increasingly abundant and effective. Israel is presently faced with rockets and missiles of various types, which have reached a staggering number of more than 150,000 held by Hezbollah in Lebanon, and Hamas in the Gaza Strip. Together they not only cover the entire populated areas of Israel, but have gradually become more sophisticated and precise. The future trend will be a lethal combination of short- and medium-range statistical rockets and longer-range guided missiles, which represent a serious threat, primarily to critical infrastructures and military bases. Generally speaking, published HFC scenarios envisage an onslaught of up to 700 rockets and missiles per day for a possible duration of more than thirty days.
b. The high-trajectory threat represents a massive man-made hazard for the State of Israel and the HFC, even if one takes into consideration the highly sophisticated robust three-layered active defense system,[23] which is gradually being introduced into the IDF. Despite the system's proven effectiveness, as tested successfully in recent rounds of conflict with Hamas in the Gaza Strip, it should be taken into consideration that no defense system can provide a hermetically sealed response. The quantities of explosives and barrages of warheads expected to be launched against Israeli targets will constitute a profound challenge for the civilian population and the infrastructure, and consequently for the HFC.[24] It can be added that the civilian high confidence in the active defense systems might paradoxically represent a special challenge for the HFC, causing people to possibly refrain from adhering to early-warning calls and not take the necessary precautionary steps.

c. Since 2006, Israel has undergone three consecutive rounds of active hostilities against Hamas in Gaza.[25] Each of these rounds produced rocket attacks of varying intensity against civilian population centers in Israel. The last one in summer 2014 lasted fifty days, during which more than a hundred rockets and mortars on average were launched daily.[26] As far as the HFC is concerned, these episodes were all relatively minor compared to the overall potential damage that Hezbollah could inflict upon the Israeli home front. This means that the HFC must be prepared for more severe scenarios in the future. An important lesson that can be learned from these rounds is that the civilian population in Israel is highly resilient, even if future conflicts might pose greater risks and overshadow past experiences in this context.
d. Despite its clear focus on man-made security conflicts, the HFC is cognizant of the natural hazards and tends to invest some resources in it. The Israeli case focuses on the risk of earthquakes, which might call upon intensive intervention of the HFC, both in search-and-rescue operations and in massive evacuations.[27] This is a demanding field for the Israeli authorities, as it represents a field of less preparedness[28] compared with that of the man-made security risks.[29]

To fulfill its tasks in these changing circumstances and meet the growing needs, the HFC has been undergoing a major buildup in its organization and order of battle. Presently it engages more than 65,000 soldiers, about 90 percent of them reservists, whose number is declining due to cuts in the IDF's general reserve forces. Apart from a professional general headquarters, located in Ramla, the HFC maintains six regional headquarters, which correspond to the national police force's territorial division; four new regular rescue regiments (Shahar, Kedem, Ram, and Tavor), which are incorporated into a newly-established brigade; numerous reserve regiments, some of them specifically for rescue missions; and medical, logistic, and light infantry units. The HFC operates a military school (Training Base #16), in which all its recruits and units are trained.[30] The HFC invests heavily in training its own units, as well as conducting numerous drills together with other first responders and the population at large. At the same time, the HFC is a life saver and an enabler of an "emergency routine" for the population in times of disruption.[31]

In order to assess the role of the HFC in the Israeli homeland security field, it would be worthwhile to shed light on the overall governmental home front structure. Here, the most striking fact is that Israel has no

official regulatory body that is legally defined as the chief authority on home front affairs. Unlike the military establishment, which is clearly hierarchical, and headed by the Ministry of Defense, the civilian sector does not have a leading organ. It has been advocated repeatedly in the past that, because of the complexity and sensitivity of the civilian front, it is imperative that such an entity be established and entrusted with the responsibility for directing and coordinating the many bodies that play a role on the civilian front. This entity should guide and inspect the different public agencies at the national and local levels, the private and industrial sectors, as well as the NGOs.[32] This was almost realized in 2011, when the Ministry for Homeland Defense was formed, only to be closed three years later, mostly because of political considerations and strong opposition on the part of the Ministry of Defense and the HFC.[33]

Resulting from the lessons of the 2006 War, the National Emergency Management Agency (NEMA) was established in 2007.[34] It was initially designed to coordinate and synchronize the activities of all organizations operating in the civilian front, without infringing on the jurisdiction of any other government agency in the field. NEMA has passed through several stages since its inception, including a short period when it was subordinate to the Ministry of Homeland Defense. Presently, NEMA is under the auspices of the Ministry of Defense, but neither it – nor any other agency – plays the needed role of official supreme authority for the home front.[35]

If the HFC and NEMA are expected to find the appropriate *modus operandi* to work smoothly together, all the more so is the case with regard to the HFC's working relations with other agencies. The HFC does not have jurisdiction and priority over the other government ministries and agencies. Consequently, it requires the right framework for horizontal collaboration. This is the reality in most cases. However, it can deteriorate into controversy and friction in face of challenging circumstances. A worthwhile example may be found in the HFC's relations with the local authorities, perceived to be critical for engaging the citizens. This brought the HFC to establish a framework of Liaison Units to the Local Authority (LULA).[36] The rationale behind this important and successful model is that the community, represented by the local authority, should be the "cornerstone" of emergency management. This concept, while theoretically sound, is far from being actually realized in many localities in Israel, especially the weaker ones. Still, LULA has been found to be a meaningful collaborative factor in the

field, affording the HFC good access to municipalities and, through them, to the communities at large.

Conclusions

In the twenty-three years since its inception, the HFC has built itself up gradually into a robust and resourceful machine, the largest operational agency in the challenged Israeli civilian front. It would be impossible to perceive the beleaguered homeland security scene in Israel without it and without its high-profile presence in emergency situations. It would be safe to suggest that it operates as a dynamic agency, with high and flexible learning capabilities, and a reasonable proven performance level. The truth is that, apart from the failed conduct in 2006, the HFC has not faced any major operational hurdle, as the three rounds of high-trajectory assaults from Gaza against the civilian home front amounted to no more than a low-to-medium level threat. The real test is still waiting, either from major man-made or a severe natural disruption. The HFC is well aware of the high stakes involved in this sphere, and has continuously invested heavily in the long and challenging journey of preparation for the expected and perhaps also the unexpected scenario. Its success in future large-scale disruptions will depend not only on its own capabilities, but also on those of the military at large and those of the civilian agencies, the level of cooperation between them, and the rate of the preparedness and resilience of the nation at large.

Indeed, the key to the HFC's future success lies not only in its operational capacities to protect the civilian rear, to mitigate the damage, or to effectively respond to the various challenges. It also will be gauged by its ability to prepare itself and the Israeli society for its core mission enhancing and preserving national resilience in future emergencies. In 2009, the HFC defined its approach to the concept of national resilience as follows:

> We examine the options of the HFC's influence on national resilience in emergency situations and adopt a broad approach . . . and particularly how it impacts the preparedness of civilians, local authorities and government ministries. The HFC's contribution is made primarily by guiding and preparing in the fields of civil defense. The HFC will be ready to assist . . . in issues which are not within its responsibility by law, but rather from the understanding of the national need . . . to

> continuous (civilian) functioning and the preservation of a reasonable 'emergency routine.'

And as a consequence:

> The capacity of the HFC to impact . . . the strengthening of national resilience is manifested in two dimensions: firstly, in building up our force and its operation . . . and secondly, in preparing the civilian population and the rear at routine times, in order to improve its preparedness for emergencies. The preparation of the population will be carried out particularly by preparing shelter infrastructures, training and guiding the civilian population and . . . assist populations with special needs.[37]

This focus on the civilian resilience represents a true understanding of the essence of disaster management. The HFC should be commended for this holistic approach and for its efforts to enhance the social and physical civilian capacities, which contribute to social resilience. This raises a basic question, however, as to the role of the military – and the HFC as its arm – in engaging in purely civilian processes, particularly in a democratic society. In most countries, this sphere is understood to be the domain of the civilian authorities, which are normally supposed to be equipped to deal with the civilian population at routine times and in crises. It is one thing for the military to provide protection for citizens from enemy attacks, or support the civilian efforts with technical and logistic assistance when needed. Taking an active role, or rather a proactive role, in civilian matters, such as the conduct of schools or the behavior of people with special needs, is quite another matter. There is a fine line here between what is suitable for the military to be engaged in, and what is not. The Israeli HFC should be sensitive to this distinction, especially in a situation that lacks normative guidelines and a clear division of labor between military and civilian homeland security agencies.

A final reference should be made to the initial set of questions that were raised in the introduction to this article: What is the best strategy for protecting the civilian home front? The answer lies in the adoption of the balanced "all hazard" approach, which would give the proportional priority to the security challenges, but which would also properly address the challenges of natural hazards. In the security realm, the suggested strategy should strike the right balance between the robust required investment

in the sphere of resistance, namely deterrence, protection, active defense, and mitigation on one hand, and the sufficient investments in the field of resilience, both in the community sphere and the infrastructure domain.

What is the role of defense versus deterrence and offense in the homeland security strategy? It is suggested that in the Israeli case, the offensive approach and its associated arm of deterrence are both significant and worthwhile. However, Israel has learned, during years of low intensity, hybrid conflicts, that the offensive posture alone carries profound challenges, both operational and diplomatic. It also does not provide a total response to the complex challenges This frames the defensive approach as a valid complementary strategy, which, of course, warrants the needed resources for both active and passive protection, but mostly the broad investments in ensuring the resilience of the national systems. Those should focus on the capacity of the impacted systems to bounce back rapidly following major disruptions.

The role of the military to protect the civilian front from the security threats is clear, but complex. It is expected from any military anywhere to harness its multiple resources in order to assist its respective communities in time of need. Quite another question is to what extent should the military – in this case the IDF –be entrusted with the mission of serving as the national primary first responder to any threat? In the Israeli case, which is characterized mostly by security-based challenges, the HFC is the only viable candidate for the mission. Consequently, the HFC has to be well prepared to stand up to the challenge, which means also that it should enhance its professional capacity to successfully deal with the civilian environment in the most severe circumstances. This means that the HFC still has a long way to go in building itself for the mission. To achieve a high capacity for success, it needs the understanding and support of the IDF and the government as a whole.

Notes

1 Home Front Command, "Home Front Command Throughout the Years," http://www.oref.org.il/1045-en/Pakar.aspx#par_1.

2 Moshe Naor, *In the Front of the Rear, Tel Aviv and the Mobilization of the People in the War of Independence* (Jerusalem: Yad Ben Zvi, 2009), pp. 161-168 (Hebrew).

3 Mordechai Nimtza-Bi had been the chief of the Haifa Fire Fighters Department and a senior policeman. He wrote a pamphlet entitled "Your Home as a Shelter During Aerial Bombardments"; an article entitled "The

Anti-Aircraft Defense in England and in Israel" in the military magazine *Maarachot* no. 2 (November 1939); and a book in Hebrew called *The Flag* (Tel Aviv, 1948), offering different versions of the state flag and ways of handling it in public. See Rachel Neiman, "Every Home a Shelter," Israel 21c website (July 13, 2014), http://www.israel21c.org/every-home-a-shelter/. For the book *The Flag*, see, http://il.bidspirit.com/portal/?lang=en&searchAgentRequest=true&sessionId=02ee9caa6fc5439f8bc2068777736ae9#!/lotPage/source/catalog/auction/548d4f9ae4b057edd0377479/lot/550bfcc1e4b0943ee74294a4.

4 Law of Civil Defense 5711-1951, (Hebrew), http://www.2all.co.il/web/files/Sites5/ergun-ktzenim/Files_211362_(4026).pdf.

5 Yitzhak Zaid, "Regional Defense and Civil Defense in Future Wars," *Maarachot* 270-271 (October 1979): 81-84 (Hebrew).

6 Joseph Alpher, ed., *War in the Gulf: Implications for Israel* (Jerusalem: Westview Press and the Jaffee Center for Strategic Studies, Tel Aviv University, 1992).

7 Aharon Levran, *Israeli Strategy after Desert Storm: Lessons of the Second Gulf War* (London: Psychology Press, 1997).

8 Moshe Zeidner and Hasida Ben-Zur, "Coping with a National Crisis: The Israeli Experience with the Threat of Missile Attacks," *Personality and Individual Differences* 14, no. 1 (1993): 209-224.

9 Tomer Simon, "Viper: Then until now in the Israeli Home Front: An Interview with General (Res.) Ze'ev Livne," *Ready* (October 24, 2011), (Hebrew), http://ready.org.il/2011/10/israelihomefrontevolution/.

10 "Home front command throughout the years," Home Front Command, http://www.oref.org.il/1045-en/Pakar.aspx#par_3.

11 "Objectives of the Home Front Command," Home Front Command, http://www.oref.org.il/10862-en/Pakar.aspx.

12 As suggested by Gen. Livne in an interview to *Ready*.

13 Shlomo Brom and Meir Elran, eds., *The Second Lebanon War: Strategic Perspectives* (Tel Aviv: Institute for National Security Studies, 2007).

14 Meir Elran, "The Civilian Front in the Second Lebanon War," in *The Second Lebanon War 2007*, pp. 103-122.

15 Gabi Siboni, "The military campaign in Lebanon," in *The Second Lebanon War 2007*, pp. 61-77.

16 The State Comptroller, *The Deployment of the Home Front and its Function during the Second Lebanon War* (Jerusalem, 2007) (Hebrew).

17 "Home Front Command Search and Rescue Unit," Home Front Command, http://www.oref.org.il/10953-en/Pakar.aspx.

18 Amir Rapaport, "The IDF and the Lessons of the Second Lebanon War," *Mideast Security and Policy Studies* (Begin-Sadat Center for Strategic Studies, Bar-Ilan University) no. 85 (December 2010), http://besacenter.org/mideast-security-and-policy-studies/fixes-and-flaws-in-the-idf-four-years-after-the-second-lebanon-war-3-2/.

19 The Home Front Command, Department of Shelters, "The Physical Sheltering Doctrine: Home, Institutions and Public Shelters," (n.p.: January 2010), (Hebrew), https://drive.google.com/file/d/0B4ZJn6Rmd8gDSGFicTlQOE8yeW8/view.

20 Meir Elran and David Friedman, "Gas Masks: Toward the End of the Line," *INSS Insight* no. 487 (November 24, 2013), http://www.inss.org.il/index.aspx?id=4538&articleid=5992.

21 "Chemical weapons," Home Front Command, http://www.oref.org.il/11133-en/Pakar.aspx.

22 Home Front Command, Population Department, "The Doctrine for Population Behavior in Crises," (n.p.: June 2011), (Hebrew), https://drive.google.com/file/d/0B4ZJn6Rmd8gDNDd1c1BfLTdzbWs/view.

23 Short-range tactical Iron Dome, Rafael Defense Systems, Ltd., http://www.rafael.co.il/Marketing/186-1530-en/Marketing.aspx; Medium-range David's Sling, "Terminal Missile Defense Interceptor," Rafael Defense Systems, Ltd., http://www.rafael.co.il/Marketing/186-1607-en/Marketing.aspx; Long-range "Arrow 3," Missile Threat, http://missilethreat.com/defense-systems/arrow-3/.

24 Home Front Command, Population Department, "The Behavior of the Civilian Population During Hostilities (War and Low Intensity Conflict) and the Principles of Intervention," (n.p..: July 2011), (Hebrew), https://drive.google.com/file/d/0B4ZJn6Rmd8gDdmN5VlRfV2tHbEk/view.

25 On the role of the HFC in these rounds, see Meir Elran, "The Civilian Front in Operation Cast Lead: Proper Functioning in Face of a Limited Challenge," *INSS Strategic Assessment* 11, no. 4 (February 2009): 19-23. http://www.inss.org.il/uploadImages/systemFiles/adkanENG11_4%20_corrected_Elran.pdf; Meir Elran and Alex Altshuler, "The Civilian Front in Operation Protective Edge," in *The Lessons of Operation Protective Edge*, eds. Anat Kurz and Shlomo Brom (Tel Aviv: Institute for National Security Studies, 2014), ppp.121-127, http://www.inss.org.il/uploadImages/systemFiles/The%20Civilian%20Front%20in%20Operation%20Protective%20Edge.pdf.

26 Meir Elran and Alex Altshuler, "Operation Protective Edge: Lessons from the Civilian Front – Interim Summary," *INSS Insight* no. 581 (July 31, 2014), http://www.inss.org.il/index.aspx?id=4538&articleid=7388.

27 "The Behavior of the Civilian Population in an Earthquake and the Principles of Intervention," Home Front Command, Population Department, February 2012, (Hebrew), https://drive.google.com/file/d/0B4ZJn6Rmd8gDNUpFOHlSNXVIVVk/view.

28 The State Comptroller, "Sustainability of Buildings and Infrastructure in Earthquakes – Situation Report," (Jerusalem: March 2011), (Hebrew), http://www.mevaker.gov.il/he/Reports/Report_116/1220891e-0b0b-49e5-b1a7-597913a13a6d/6658.pdf.

29 Meir Elran and Alex Altshuler, "How Prepared is Israel for an Earthquake?" *INSS Insight* no. 380 (October 30, 2012), http://www.inss.org.il/uploadImages/systemFiles/380.pdf.

30 Amir Bohbot, "Rockets on Tel Aviv Towers: Is the Home Front Ready?" *Walla*, March 25, 2015, http://news.walla.co.il/item/2840631; "Home Front expands," IDF, March 19, 2012, http://www.idf.il/1133-15334-he/Dover.aspx; "The Home Front Command Throughout the Years."

31 In 1990 Israel was divided into six early warning zones. By 2007 there were twenty-five zones and now 250 East-West zones, which enable the majority of civilians to continue with their daily routine when specific and identified areas are targeted. See, Yossi Hatoni, "Home Front Invests 400 million NIS in Development of Emergency Alert," *PC*, October 8, 2015, http://www.pc.co.il/it-news/196218/.

32 Meir Elran and Alex Altshuler, "Responsibility and Authority (or lack thereof) on the Israeli Home Front," *INSS Insight* no. 452 (2013), http://www.inss.org.il/index.aspx?id=4538&articleid=5282.

33 Meir Elran and Alex Altshuler, "Closing the Home Front Defense Ministry," *INSS Insight* no. 545 (2014), http://www.inss.org.il/uploadImages/systemFiles/No.%20545%20-%20Meir%20and%20Alex%20for%20web.pdf.

34 Jack L. Rozdilsky, "Emergency Management in Israel: Context and Characteristics," in *Comparative Emergency Management: Understanding Disaster Policies, Organizations, and Initiatives from Around the World*, ed. David A. McEntire (n.p.: 2009).

35 The State Comptroller stated in September 2015 that, "There still does not exist a broad legislative arrangement that holds all the affairs concerning the rear in emergency situations and clarifies the scope of responsibilities and areas of authority of each of the government ministries and the other organizations that are involved with the rear. The lack of such an arrangement constitutes a severe shortcoming." See, "Publication of Reports on Preparation and Readiness for Emergency," The State Comptroller, http://www.mevaker.gov.il/he/publication/Articles/Pages/2015.09.09-Emergency.aspx.

36 Home Front Command, Population Department, "The Liaison Unit to the Local Authority (YAKLAR)," December 2013, (Hebrew), https://drive.google.com/file/d/0B4ZJn6Rmd8gDdlNtNExVSkVBMUU/view.

37 Home Front Command, Department of Doctrine and Development, "The Basic Doctrine of the Home Front Command," September 2009, pp. 38-39, (Hebrew), https://drive.google.com/file/d/0B4ZJn6Rmd8gDcFNuNjRTTTdsbmc/view.

The Death of Human Intelligence: How Human Intelligence Has Been Minimized Since the 1960s

Bradley A. Lewis

Since the beginning of time, the collection of human intelligence (HUMINT) has been the cornerstone of gaining an advantage over one's enemies. Over the past fifty years, the United States, under three particular administrations, has tried to end the process of HUMINT collection. HUMINT has always been associated with tradecraft and the necessity to work with unsavory characters. The information gleaned from these characters, however, has proven both vital and important in terms of defending against a threat as well as pursuing an objective. The derision expressed toward the methods of collection and those involved in the process has gone from a clandestine operation to front-page headlines. This image has been changed by political factors not associated with winning or losing.

Keywords: HUMINT, SIGINT, Collection, President, Church Commission, Attorney General, Intelligence, DNI, tradecraft

Introduction

Attorney General Eric Holder's decision to ask a special prosecutor to investigate for possible criminal prosecution Central Intelligence Agency (CIA) operatives who interrogated terrorists in overseas locations is the latest and most egregious instance of political gamesmanship by Holder, who strode into office promising to remove the taint of politicization from the Justice Department.[1]

Perhaps the correlation between the 1970s Church Commission and the current Obama administration can provide a basis for the prevailing mindset regarding the workings and methods of the Intelligence Community

Bradley A. Lewis is president and founder of Beartrees LLC.

(IC). The Church Commission hearings concluded with fourteen published reports about the operations and abuses of US intelligence agencies, which included assassination plots to murder foreign leaders. Attorney General Eric Holder refocused examination of intelligence operations, specifically the CIA's Human Intelligence Operations (HUMINT), once again. For example, Holder pronounced himself obligated to "follow the facts and the law."[2] One critical fact, however, he entirely ignored; professional prosecutors had already examined the allegations of the CIA's misconduct, conducted an inquiry, and made a determination not to prosecute − although one contractor outside the interrogation program was prosecuted for assault. Holder never mentioned that a task force (informally dubbed the "Detainee Abuse Task Force") in the Eastern District of Virginia had already considered all of the applicable information, including the CIA inspector general's 2004 report that had been made public. Following standard procedure, the task force drafted "declination memos" and set forth the rationale for not proceeding with prosecutions.[3]

By proposing to prosecute members of the IC for their role in interrogation, the attorney general of the United States essentially neutered the IC. In one of the first pronouncements, Attorney General Holder, with backing of the White House, essentially took away the power of the CIA and rendered the agency useless and irrelevant. Without the ability to use enhanced interrogation techniques, information gathered in the field would no longer prove to be beneficial as it had been in the past. The Global War on Terrorism (GWOT) has been dependent upon HUMINT methods. By removing the human factor from intelligence operations, the reliance on technological means of intelligence gathering supersedes all other forms of intelligence collection. According to the *Wall Street Journal*, "by threatening to prosecute CIA officials, the Obama Administration is taking ownership of future troubles in a way that will only do itself harm. Like the Church and Pike probes of the 1970s."[4]

The Church Commission of the mid-seventies was created around intelligence failures during the Vietnam War. At the same time, a group of senators led by Senator Frank Church from Idaho was looking to deal a severe blow to the Department of Defense (DoD) and the Intelligence Community. As the war ended and the agenda switched to budget cuts and non-proliferation, the mindset became increasingly against the DoD and the IC. These hearings were used not only to study the cause-and-effect, but also to embarrass the hierarchy of these two organizations. While this

commission was blamed for future failures due to the restrictive nature of its findings, its worst example of failure was the neutering of the intelligence apparatus in general. Oversight and approval became the means to an end for the Senate and the House. This led to failures in subsequent years that cost many lives.

The White House and Justice Department is working toward the goal of a similar kind of Intelligence Community. This would mean that the ability to collect Human Intelligence and Signal Intelligence would be greatly limited by the White House and Justice Department. In other words, the ability to protect the homeland would be influenced by decisions made in meeting rooms, not battlefields. If one lesson was learned from the Vietnam War, it was that politicians were not qualified to win the battle or protect the troops. This is where the United States is heading today.

HUMINT Collection

Perhaps one of the most comprehensive definitions of HUMINT is found in the website of the Federal Bureau of Investigation (FBI), which states that:

> Human Intelligence (HUMINT) is the collection of information from human sources. The collection may be done openly, as when FBI agents interview witnesses or suspects, or it may be done through clandestine or covert means (espionage). Within the United States, HUMINT collection is the FBI's responsibility.[5]

In terms of intelligence collection, all branches of the IC use various means of surveillance and collection for their benefit in terms of their specific missions; this includes all of the "INTs" as well as unmanned aircraft and other forms of collection. O'Hern states that,

> Although intelligence collectors are trained in source protection procedures, this process is not free of risk. In many cases, personal meetings are required between the source and collector to share information. Great care is taken to select a proper site for the meeting, but most must take place in enemy territory or on a coalition forward operating base. Neither offers a safe haven or refuge from the watchful eyes of an enemy insurgent or his allies.[6]

The number and capability of trained intelligence collectors is a limiting factor to the size and scope of a human source network. On average, trained

collectors represent less than five percent of the total organization conducting counterinsurgency operations and their capacity to develop sources and collect intelligence is finite. Communication between a collector and a source is often limited due to security considerations and the timeliness of a source's response to specific intelligence requirements is unpredictable. Rivera and others indicates that,

> Fears of reprisal are palpable and their consequences are dire. In Afghanistan alone, the United Nations observed . . . 462 assassinations in 2010 in reprisal for cooperating with the coalition according to their records, double the number from the previous year. The figures may not include many killings in remote areas, like the mass beheading, because fearful villagers never reported them.[7]

Direct and personal relationships with sources also can also be dangerous for the intelligence collector. In December of 2009, seven intelligence collectors were killed in Afghanistan by a source serving as a double agent who detonated a suicide vest after being granted special access to a coalition base by his handlers.[8]

In the current political environment, the use of HUMINT has been greatly limited by presidential directives and the Director of National Intelligence (DNI). Rules and regulations have been put in place to monitor activities such as HUMINT collection, interrogation and other means of protecting US national security. Whereas in the past the methods were not discussed, today these operations are made in the full view of Congress and must be approved prior to execution. This hinders the ability to collect real time data. Intelligence Community Directive Number 304, dated March 2008, states that,

> The DNI is committed to ensuring that HUMINT activities are executed in a prioritized, coordinated, integrated, and professional manner; that USG elements engaged in the collection of intelligence through HUMINT activities, counterintelligence activities, or activities that involve the use of clandestine methods are coordinated and deconflicted with IC HUMINT activities; that HUMINT practitioners use core common standards; and that there is transparency into HUMINT support capabilities to allow all IC elements to benefit from technical or other advances.[9]

As the attorney general and the president have weighed in on the use and function of HUMINT, the public has been given the impression that wrong doings and needless harm have come to the community. For example, Fox News on September, 21, 2009 urged Obama to stop the probe. Obama stated, "I appreciate the former CIA directors wanting to look out for an institution that they helped to build. But I continue to believe that nobody is above the law."[10] Additionally, on the CBS news program *Face the Nation*, Obama said, "I want to make sure that as president of the United States that I'm not asserting in some way that my decisions overrule the decisions of prosecutors who are there to uphold the law."[11] While the politicization of intelligence gathering has been brought to the forefront, the methods and responsibilities remain the same. If the academic side of the world strives for clarity, the political side strives for acceptance; these rarely occupy the same sheet of music.

Seven former CIA directors, whose tenures span back as far as thirty-five years, wrote to the president that the cases have already been investigated by the CIA and career prosecutors, and that to reconsider those decisions makes it difficult for agents to believe they can safely follow legal guidance. They stated that the decision to reopen a criminal investigation created an atmosphere of continuous jeopardy for the intelligence community, especially those involved in HUMINT.

A decision by Attorney General Holder to investigate would have stood as a defining gesture of independence from President Obama, and would have been in sharp contrast to his predecessors, who were said by lawmakers in both parties to have run the Justice Department as a satellite office of the White House. Holder had told associates he was weighing a narrow investigation, focusing only on CIA interrogators and contract employees who clearly crossed the line and violated the Bush administration's guidelines and engaged in flagrantly abusive acts. In taking that route, Holder would have run two risks. One is the political fallout if only a handful of low-level agents had been prosecuted for what many critics see as a pattern of excess condoned by the top of the government. The other is that an aggressive prosecutor would not stop at the bottom, but would work up the chain of command, and end up with a full-blown criminal inquiry into the intelligence agencies – just the kind of broad, open-ended criminal investigation the Obama administration said it wanted to avoid. In a sense, Attorney General Holder put himself in this awkward position. Earlier in 2013 he successfully argued, in the face

of CIA protests, for the release of legal memorandums produced by the Justice Department during the Bush administration. The memorandums showed that the administration had authorized the use of interrogation tactics such as head slapping, walling, and waterboarding. The documents also brought accusations of torture into the public eye.[12]

The basis of this paper is both academic as well as political. In today's environment, the two are very difficult to separate. While the standards of practice of intelligence gathering have changed over the years, the mission has remained the same. While the idea of political interference in national security is frowned upon, many people have different theories as to which is more important. The lack of human intelligence and the concentration on technology has led to both poor gathering and missed opportunities. As the literature shows, three administrations did not believe, or were not comfortable with the use of HUMINT. The Ford and then the Carter administrations believed that HUMINT was a cause of the mistakes and errors made in the Vietnam War. These ideas led to the Church Commission, which placed the IC under the direct control of Congress. This was a reaction to the need to find the reasons for the failures in the Vietnam War. Most recently, the Obama administration has elevated the use of technology to a much higher level than that of HUMINT. While the growth and sophistication of technology add to the science of intelligence collection, it does not have the same effect as direct human contact in the gathering of real-time information. While the Obama administration does not believe in the value of HUMINT, it has made the issue more difficult than it should be. By threatening to prosecute operational employees of the IC for their methods, the trust-in- government factor has been completely destroyed. The trust of the IC is difficult to repair, and towards the end of Obama's presidency, the damage in the areas of HUMINT and clandestine service is still very obvious.

Findings and Analysis

When researching a subjective matter, such as the decline in the use of HUMINT during different time periods or administrations, the results can be confusing. This framework led to the Church Commission and the future of relations between the Obama administration, the Justice Department, and the Intelligence Community. The Obama administration has weakened the resolve and the purpose of the Intelligence Community to such an extent that the collection methods and results have been adversely

affected. During the Carter and Obama administrations, the reliance on HUMINT was at its lowest levels in recorded history. This is not to say that the methodologies and practices were not in place. The reliance on new means of technology grew from the 1960s to the present day; the idea that HUMINT was key to providing reliable intelligence changed during each administration from 1960 to the present. As technology changed, the reliance on electronic means became more prevalent. This allowed for less human interaction, and for distance to be employed in gathering data. The problem arose when the data became corrupted, based on the knowledge of the enemy, and the unwillingness of the administrations in power to use the data for productive means. The role of the HUMINT analyst was, and always will be, to gather information and analyze the raw data for useful means. If this is not followed through the data becomes dated and irrelevant. This has been the case in these three particular administrations.

Vietnam War and the Church Commission

The use of HUMINT was widely seen as contributing to the failure of the Vietnam War. While many articles and books have been written discussing the ultimate failure of the war, the topic always seems to return to either poor intelligence or misused intelligence data. In keeping with the idea of technology overstepping the use of HUMINT, the Vietnam War was conducted by political theory instead of military intelligence. The nature of the war made the need for on-the-ground intelligence that much greater. Senator Frank Church from Idaho convened a senate committee that spanned the end of the Ford administration and continued through the Carter administration. The sole purpose of this committee was to show the failures of the IC during the Vietnam War and to make changes for the future. As history has shown, this was a major mistake.

The Report of the Committee, dated January 27, 1975, stated that, "The Senate Select Committee on Intelligence Activities has conducted a fifteen month long inquiry, the first major inquiry into intelligence since World War II. The inquiry arose out of allegations of substantial, even massive wrong-doing within the 'national intelligence' system." This mistake centered on oversight and the lack of reporting authority of the IC. The goals of this committee were to control the functions of the IC – not necessarily for mistakes that had been made – but more for congressional control of the community and the information gathered. This committee took into account IC involvement in all areas of the globe. This included

regional conflicts, tribal conflicts, and all events that could destabilize a government or region. It also included involvement in cases like Watergate and internal US issues.

The final recommendations of the Church Commission were the most all-encompassing recommendations ever made by any congress in regards to the powers of the IC. Its resolution was to establish a committee to investigate the nation's intelligence apparatus. It was deemed necessary to investigate methods and results from the Vietnam War and other actions during that time period.[13] This resolution effectively took the power away from the president and the IC and created a senate committee to oversee all intelligence activities. This effectively removed the IC from any role in determining either policy or action. As the Carter administration proceeded under these new rules, the IC was effectively rendered a non-functioning part of government. Technology was beginning to play a larger role and the need for HUMINT was becoming increasingly negligible. The operational directorates of the IC were no longer as useful as they once were, because of the time factors involved in determining action.

Carter and the Church Commission

The Church Commission was formed at the end of the Ford administration, but its decisions and recommendations were put in place during the Carter administration. Research has shown that the Church Commission did more to undermine the IC than anything in history. While the need for oversight and fact-finding was a noble goal, the Church Commission used the results of the Vietnam War to determine the future direction of the use of HUMINT and other forms of intelligence gathering. Senator Church decided to hold these hearings based on the failures of the war itself, and not on the failures in intelligence. While mistakes were made, the failures of Vietnam had more to do with mismanagement than lack of intelligence. A political management system in an overseas war can never work if the commanders in the field are not allowed to do their jobs. In the Vietnam War, the rules of engagement were determined in Washington and not on the battlefield. This led to oversights in troop strength, intelligence, and an overall failure to determine the outcome. The Church Commission used these results to limit the power of the IC and to set forth a perilous path for the future.

One of the main recommendations of the Church Commission was that the IC should answer to the Congress for all matters. This was as ludicrous

as having the IC report to the Joint Chiefs of Staff under Kennedy. The IC works in the shadows and their methods need to be covert. By answering to Congress, the issues would have focused on classification and the time it would take to make a decision. This recommendation was doomed from the start. HUMINT was still the key source of information during the Vietnam War. Technology in terms of weapons and material was moving quickly and the use of satellites and computers was just getting started, but HUMINT was the key. While the methods of gleaning information are not always pretty, they are effective in determining the next move on the chessboard. Without the ability to interrogate enemy prisoners, the use of battlefield intelligence is not an option. The best sources of the next steps come from those involved in the fight. HUMINT proved very successful in the field, but its advantage became ineffective by limiting its use in the future. If in the long run, the IC would have had to ask permission of Congress, the apparatus would have been rendered useless.

The Church Commission and its recommendations were taken at face value by President Carter. The decision to limit the scope of the IC and its methods was put into place not long after he took office. This was a leading cause of the implosion of both the military and the IC. During Carter's presidency, the military strength, including intelligence, was at its lowest levels in history. The recruiting numbers for military service were at an all-time low and the Soviet Union was becoming a more dominant force in the world. It seemed that the era of American exceptionalism was nearing its end, as a result of the economic recession in the mid-1970s, paired with the end of the Vietnam War, and the lack of trust in the military and the political environments. The Carter administration, in agreeing to implement the findings of the Church Commission, allowed the United States to lose its place as the leader of the free world and to bring about doubt, both internally and externally, as to the future of the country. This fear and uncertainty led to the overall feeling of loss-of-face among the population. These attitudes stemmed from the Church Commission hearings and its recommendations to do away with many HUMINT gathering techniques. The direction of the presidency and the country were greatly influenced by the hearings and their recommendations. It took a decade for the United States and its military and intelligence communities to become productive. Only a change in president and attitude allowed the country to get back to being exceptional.

The Obama Administration

Of all the administrations in the past fifty years, the Obama administration has done more to do away with HUMINT. As technology has grown and functionality has improved, the need for HUMINT, as determined by current policy, has increasingly diminished. The Obama administration, and, in particular, the attorney general, have determined that the use of HUMINT in many forms is a punishable offence. At the beginning of the presidency, the attorney general declared that he was going to prosecute intelligence community operators involved in enhanced interrogation. Not only was this incredible, it did more to stop the flow of information than anything imagined. Operations were halted, operators stepped down, and the use and techniques of HUMINT were put in the closet. The research shows that the decline in actionable intelligence dropped greatly during the first six months of Obama's presidency. This was directly tied to the comments and pronouncements of the attorney general.

"Attorney General Eric Holder's decision to ask a special prosecutor to investigate for possible criminal prosecution CIA operatives who interrogated terrorists in overseas locations is the latest and most egregious instance of political gamesmanship by Holder, who strode into office promising to remove the taint of politicization from the Justice Department."[14] Holder pronounced himself obligated to "follow the facts and the law." One critical fact, however, he entirely ignored was that professional prosecutors had already examined the allegations of CIA misconduct, conducted an inquiry, and made a decision not to prosecute (one contractor outside the interrogation program was prosecuted for assault). Holder did not mention that a task force (informally dubbed the "Detainee Abuse Task Force") in the Eastern District of Virginia had already considered all of the applicable information, including the CIA inspector general's 2004 report, which had been made public. Following standard procedure, the task force drafted "declination memos," setting forth the rationale for not proceeding with prosecutions.[15]

Attorney General Holder, with the backing of President Obama, essentially took away the power of the CIA and made its mission irrelevant, and triggered a series of events that weakened the defense posture of the United States for the next several years. Without the ability to use enhanced interrogation techniques, the information gathered in the field would no longer be as beneficial as it had been in the past. These methods of HUMINT had been the cornerstone of activities in the GWOT. To take

the human factor out of play makes the reliance on technological means of gathering intelligence paramount to all other forms of intelligence collection. While technology has been a boon to the industry, it does not allow for the interpersonal methods and means of intelligence. As with all forms of technology, the systems can fail and the information can be corrupted. This is not to say that HUMINT is perfect, but the ability to garner information is more reliable in a face-to-face setting.

With the Obama administration, the use of technology has become the sole driving force in intelligence gathering. This is part of the issue. Technology, be it drones or electronic surveillance, OSINT or MASINT, is the new way of the future. It is relatively clean and somewhat less costly than actual people on the ground. The drawbacks are that verification is more difficult and human verification is needed in order to be successful. Another flaw in the reliance on technology is the 24-hour news cycle. The administration takes credit for the successes of the community in near real-time. The Bin Laden raid was broadcast within minutes of completion to say, "Look what we did."[16] This also provided the enemy with the same access to information, specifically the location and result. This is not the way of the IC. Failures are made public and successes are internalized. The preeminent factor should be the safety and security of the population both at home and overseas, and not who gets credit. This has led to a furthering of "classified" information being released by the participants who retire from active duty and write books. In the past, the operations of the intelligence community and the Special Forces community were private matters that were not used for profit nor as part of the release of information. With Obama's administration, all of this has changed. Judicial Watch has released hundreds of DoD and CIA communications, revealing that the administration leaked classified information to filmmakers about the raid in which Osama bin Laden was killed.

The Obama administration has taken the report of the Church Commission, and has multiplied it several times. The world has changed greatly since the 1970s. For example, the Cold War has ended and the Soviet Union does not exist. Technology has become the means to an end for all types of information and intelligence gathering. The world has become much smaller in terms of travel and communication. The public has taken an active role in both gathering and transmitting information along with their opinions. This has caused the need for covert action to be more important than ever before; the Obama administration, however, looks

at covert action as a means to celebrate the result. The term "spiking the football" has become part of the lexicon when describing how the Obama administration takes credit for the work of those in harm's way. Drone strikes have become the method of choice for neutralizing the enemy without regard to collateral damage. Information is acted upon prior to verification, and information is gathered about citizens, leaders, and just about anyone else. This is not the spirit nor method of the IC. The only thing that can be said is that the Obama administration likes to use the IC for the dirty jobs, but does not stand behind the individuals who are tasked with that responsibility. This is shown by the actions taken by the Department of Justice when it comes to prosecuting CIA operatives involved in HUMINT. By considering interrogation akin to torture, the Department of Justice has placed the lives and the methods of these operatives on trial. These trials have been conducted by the news media, and not by courts of law. The methods of gathering information in a war zone do not have the same benefits as the methods used in a controlled environment. While torture is not an acceptable means of interrogation, the Congress has passed legislation allowing for enhanced means of interrogation.

The use of HUMINT in the protection of the nation has steadily declined with the advent of technology. Over the past fifty years, and particularly during three administrations, the use of face-to-face contact has become a very small part of intelligence gathering. During this time, however, other administrations have recognized the value of HUMINT to the point where many attacks were averted based on information gathered from interrogation techniques. Why the Kennedy, Carter, and Obama administrations failed to see or understand the value of HUMINT is a question that has many answers.

The failure to understand the benefits of using HUMINT is the key to success of most terrorist attacks both in the United States and abroad. While many of the methods used in gathering HUMINT are not mainstream or pleasant, the information that can be provided could be tantamount to the prevention of an attack on the United States. The political leadership, however, prefers intelligence from technology rather than human sources. While this is part of the overall goal, technology is not and never was the only key to a successful intelligence operation. Although technology continues to change on a daily basis and the ability to glean information has taken on a new meaning, this does not preclude the necessity of employing people to provide both battle-field and ongoing intelligence.

As already stated, the technology available has grown exponentially over the past fifty years, with the most advances in the past fifteen years. Electronic Intelligence (ELINT), Signals Intelligence (SIGINT), and other sources now are significant factors in gathering intelligence. The difference is that all of these methods are impersonal, and they require a great deal more analysis than HUMINT. What is said electronically does not have the same nuance or body language of a personal conversation. One cannot read body language to determine the truth electronically. While all of the methods of collection are important, the only personal method is HUMINT.

In the IC there are many types of personnel. There are analysts, who look at the raw data; scientists, who build new methods or programs for analysis; and there are operators. The operators are usually in the field, with little back up or direction. They are responsible for their own safety as well as the safety of their sources. This is what is called the clandestine service. This service is the primary source of HUMINT. All the operator has is the belief that his country will stand behind him if there is a problem. These operators are in the field, alone many times, for months or years at a time. It is their job to embed themselves in very dangerous positions. The idea is that they become part of the group, and they report back with information. That information can be about an upcoming attack or the plans for another 9/11. These people are in harm's way for most of their careers, and they work out of love for their country. When the attorney general threatened to prosecute this type of person, their motivation and trust in government disappeared.

HUMINT has been the source of information that has stopped planned attacks. It provided information as to the whereabouts of targets and leaders, and for all of time it has been the most reliable method of intelligence gathering. The administration seems to feel that it is no longer important and wishes to do away with it. As the research has shown, without the use of HUMINT, the world would be a much more dangerous place, and the future of the United States might be questionable. The terror events of today may be partially the result of the lack of HUMINT since the start of the Obama administration.

The research all shows the benefits of the use of HUMINT. It also shows the problems caused by three administrations that did not believe in its effectiveness. The truth is in the results and the only way that it can be judged is by studying history. This means past history, current events, and the future. This is the only way to see the benefits of HUMINT and

the problems caused by not believing in the methodology. The future will be the key to codifying the results of the current research.

A recent revelation has added to the concerns of HUMINT. While the administration is apt to rely on technical means of intelligence gathering, the CIA has continued to use HUMINT as key to collecting information. A recent report states that the director of the CIA admitted to spying on the email and correspondence of the Senate Intelligence Committee. An internal investigation by the CIA found that its officers penetrated a computer network used by the Senate Intelligence Committee in preparing its report on the CIA's detention and interrogation program. According to the report, the CIA inspector general, three of the agency's information technology officers, and two of its lawyers "improperly accessed or caused access" to a computer network designated for members of the committee's staff who were working on the report and had access to millions of documents at a CIA site in Northern Virginia. The names of those involved have not yet been made available because the full report has not yet been made public.[17]

The White House publicly defended the CIA's director, John O. Brennan, saying he had taken "responsible steps" to address the behavior of CIA employees, which included suggesting an investigation, accepting its results, and appointing an accountability board. This revelation about the CIA's activities is damning in light of the administration's desire not to use HUMINT. A scandal of this nature will be difficult to overcome and make the future direction of HUMINT even more tenuous.

Conclusion: Moving Forward

While moving forward requires an understanding of the past, the key areas of HUMINT have been discussed and argued throughout the years. The three administrations discussed in this article are key to understanding the desire to do away with this type of intelligence gathering. While unsavory and sometimes bordering on illegal, the means used to gather information are not subject to public scrutiny. While at war, the available means of intelligence gathering are to be used and tolerated. The debate about torture is a false argument for the doing away with gathering HUMINT. Most of the public understands the need to gather information, and they are not concerned with the methods. What constitutes torture for one is a successful interrogation for another. The means used are secondary to the results. If a 9/11 style of attack can be prevented by any means, the public

will support it. There are many instances when the public in general does not have the need to know, as the public is concerned only with the results.

By removing the means to gather HUMINT, the United States, in particular, has made a conscious decision to bet the future on technological means of intelligence gathering. While this may be less threatening and more cost effective, the results will be less than satisfactory. Technology has its place, but the difficulty lies in the verification of information and the ability to react to a particular situation. The only method of verifiable intelligence is to have people on the ground and, better yet, embedded with the bad actors. While inherently more dangerous, the rewards outweigh the risks in being able to gather verifiable intelligence. There is a place for the use of technology in terms of analyzing data and conducting surveillance, but these are indirect means of intelligence gathering; rather, a live resource is the best means of gathering information.

Another area of concern is the methods used to gather HUMINT. In the Obama administration, the use of enhanced interrogation is considered illegal. While this is the best way to gather intelligence, the country, or at least the administration, does not seem to have the stomach for the methods. While torture is considered illegal, the use of any means necessary to stop an attack should be considered in the best interest of the population. When the attorney general announced that CIA interrogators would be indicted, the use of HUMINT effectively ended.[18] When a CIA operative does not have the faith of his own leadership, the mission will surely fail. Operations need to be run with the full support of the government, even if they may come close to crossing a red line. The operator needs to know that he will not be in danger of prosecution for doing his or her job. Sadly, this is no longer the case nor the belief of those in the IC.

Technology, communications, and travel have become second nature, making the distances between countries or factions much smaller. For technological means of intelligence gathering to be successful, the information must be verified and analyzed in near real-time. This is not possible due to many considerations. The dissemination of information alone would take more time than is available. Without the benefit of HUMINT, the dangers will continue to gain strength. Once critical mass is reached, attacks similar to 9/11 will take place. Once the United States is hit again, then the rules will change. The Obama administration seems to be more interested in ideology than in safety or protection. While no one wants to prosecute a war, the fact that war is sometimes necessary is being

overlooked. By being reactive instead of proactive (SIGINT vs. HUMINT), the administration is opening the doors to many types of terrorist attacks. What remains to be seen is the size and scope of such an attack and, more importantly, the reaction of the leadership to that attack. Time will be the key to determining the necessity of HUMINT, and the feeling is that time may not be so far off in the distant future.

Notes

1 Jennifer Rubin, "Eric Holder's Anti-CIA Witch Hunt," *Weekly Standard,* August 31, 2009.
2 Ibid.
3 Ibid.
4 "Prosecuting the CIA: Eric Holder unleashes a special counsel on U.S. war fighters," *Wall Street Journal*, August 25, 2009.
5 FBI, "Intelligence Collection Disciplines (INTs)," https://www.fbi.gov/about-us/intelligence/disciplines.
6 Steven O'Hern, "Details on Suicide Bomb Attack at CIA Base – FOB Chapman," *Intelligence Wars*, January 11, 2010.
7 Ray Rivera, Sharifullah Sahak, and Eric Schmitt, "Militants Turn to Death Squads in Afghanistan," *New York Times,* November 28, 2011.
8 Nicholas, Munn, "Crowdsourcing: A New Perspective on Human Intelligence Collection in a Counterinsurgency," *Small Wars Journal*, January 3, 2012.
9 Intelligence Community Directive (ICD), #304, Human Intelligence, March 6, 2008, Amended July 9, 2009.
10 "Obama Backs Holder in CIA Interrogation Probe," Fox News, September 21, 2009.
11 President Obama, interview by Bob Schieffer, *Face the Nation*, CBS News, September, 9, 2009.
12 Scott Shane, "U.S. Intelligence Community under Closest Scrutiny since 1975 Church Committee Hearings," *New York Times*, July 26, 2013.
13 US Congress. Senate. Select Committee to Study Governmental Operations with Respect to Intelligence Activities. *Final report of the Select Committee to Study Governmental Operations with Respect to Intelligence Activities. United States Senate: Together with additional, supplemental, and separate views.* US Congress. Senate. Report no. 94-755. (1976).
14 Rubin, "Eric Holder's Anti-CIA Witch Hunt."
15 Ibid.
16 Mark Owen and Kevin Maurer, *No Easy Day*: *The Firsthand Account of the Mission that Killed Osama bin Laden* (New York: Penguin 2012).
17 Mark Mazzetti and Carl Hulse, "Inquiry by C.I.A. Affirms It Spied on Senate Panel," *New York Times,* July 31, 2014.
18 Rubin, "Eric Holder's Anti-CIA Witch Hunt."

The Khorasan Group

Ariel Koch

The threat posed by the Islamic State to many nations has led to the formation of an international coalition whose forces have been bombing Islamic State targets in Iraq and Syria. Some of the bombings in Syria have targeted the strongholds of the Khorasan group. Very little is known about this group. It appears to be an international terrorist cell that settled in Syria under the cover of the country's chaos in order to plan attacks against the West and train its members to carry them out. In September 2014, the United States labelled the Khorasan group an imminent security threat that is even more dangerous than the Islamic State. The aim of this essay is to shed light on the Khorasan group, its members, and their capabilities, and based on our analysis of this group, determine whether or not it poses a potential threat, which, assumingly, could be aimed at the West and also at Israel and the Jewish diaspora.

Keywords: terrorist, al-Qaeda in Syria, Jabhat al-Nusra, Khorasan group, Islamic State

The Khorasan Group in Syria: The New Jihadist Threat?

At a conference held on September 19, 2014 in Washington, DC, James Clapper, the director of the US National Intelligence, said that an unknown organization called the Khorasan group was posing a challenge to the United States and was perhaps even more dangerous to national security than the Islamic State.[1] Four days later, President Barack Obama said that the United States had targeted the Khorasan group in its airstrikes in Syria, with the objective being "to disrupt plotting against the United States by seasoned al-Qaeda operatives in Syria who are known as the Khorasan group."[2] The

Ariel Koch, who studies radical and extremist movements and organizations, is a doctoral candidate in the Department of Middle East Studies at Bar-Ilan University.

US airstrikes were in the Aleppo region, an area controlled by Jabhat al-Nusra, the Syrian extension of the international terrorist group al-Qaeda.[3]

In the weeks that followed, the media portrayed the Khorasan group as a special forces unit of al-Qaeda, presenting an imminent threat to Europe and the United States.[4] At the beginning of November 2014, the United States carried out additional airstrikes against the group. According to reports, the airstrikes were intended to eliminate a French national named David Drugeon, an expert in sophisticated improvised explosive devices (IED), that are capable of passing through airport security and screening mechanisms without detection.[5] A third attack targeting the Khorasan group was carried out several days later.[6] Despite the portrayal of the Khorasan group as a clear and present danger, the media ceased to show interest in the group in the following months.

Drugeon, who has also been called Abu Hamza al-Faransi (the French Abu Hamza), survived the attack on his life,[7] but only briefly; in July 2015, it was reported that he had been killed together with another senior Khorasan group member named Muhsin al-Fadhli.[8] Following the assassination, FBI Director James Comey said that the danger posed by the Khorasan group had been significantly reduced and that the Islamic State was, from that point onward, a greater risk.[9] Despite Comey's declaration, US authorities still continued to consider the Khorasan group a threat, evident by its addition in September 2015 to the US list of terrorist organizations.[10]

A year after the world became aware of the Khorasan group and two months after Comey issued his statements, the death of the French fighter Abu Hamza al-Faransi (Drugeon) was announced.[11] It appears that the commander who relayed Drugeon's death was Ibrahim al-Sharah,[12] a Saudi citizen and a senior member of al-Qaeda, who was later killed in the American airstrikes in October 2015.[13] Assumingly, there were additional fighters under al-Sharah's command who were not hurt and who still intend to carry out attacks in the West; in other words, the group, which reportedly ceased to be an imminent danger in July 2015, continued to exist after that date, and that the danger continued to be quite real.

The key questions underlying this essay are: What is the connection between the Khorasan group and Jabhat al-Nusra, the Syrian branch of al-Qaeda? Is the Khorasan group a separate organization or a part of Jabhat al-Nusra? If the Khorasan group is, in fact, part of al-Qaeda's Syrian branch – how and from whom do its adherents get their orders: from Jabhat al-Nusra commanders or from al-Qaeda's central leadership, which found

refuge in the mountains on the Afghani-Pakistani border? Furthermore, what are the operative capabilities of the Khorasan group? And what is the difference between the Islamic State, Jabhat al-Nusra, and the Khorasan group in terms of the threats that they pose to the West?[14]

According to senior sources in the US intelligence and security community, the main difference between the Khorasan group and the Islamic State is their ability to carry out their threats against the West. The US intelligence and security community believe that the Khorasan group is capable of carrying out an attack on American and European soil while the Islamic State is incapable of doing so. In other words, according to those sources, the Islamic State only has the desire to carry out mass-casualty attacks in the West whereas the Khorasan group has both the desire and the ability to do so.[15] Despite this assessment, terrorist infrastructures identified with the Islamic State have planned and, at times, have succeeded in carrying out attacks in the West since September 2014. In contrast, as far as we know, Khorasan group operatives have not managed to carry out any attacks. Nonetheless, the United States continues to describe them as an imminent threat.[16] Does the Khorasan group really pose as severe a threat as the United States claims? If so, how and why? To answer these questions, it is first necessary to clarify the meaning of the word "Khorasan." This clarification may help understand the connection between the Khorasan group and the war in Syria, which has become fertile ground for training terrorists to undertake attacks in the West.

Black Flags from Khorasan

Khorasan is a large region in Central Asia, covering Pakistan, Afghanistan, Iran, Uzbekistan, Kazakhstan, and Turkmenistan. The name "Khorasan" in Islamic lore is linked to the end of days and the coming of the Mahdi, a sort of Messiah-like figure who is supposed to conquer the world in the name of Islam.[17] According to Muslim oral tradition (hadith), the Prophet Muhammad was attributed as saying that "an army of black flags" will rise from the Khorasan and head for Jerusalem to conquer it. In 1996, Osama bin Laden found refuge in the Hindu Kush of the Khorasan, where he put into practice the theory of global jihad. It was there, too, that he flew the black flag and turned it into the flag familiar to us today.[18]

Contemporary terrorists drawing their inspiration from al-Qaeda and the Islamic State view the theory of global jihad, its ideologues, and adherents as an indication that the Muslim prophecy is being realized. For

example, Tamerlan Tsarnaev, who together with his brother Dzhokhar, bombed the Boston Marathon in April 2013, shared on his YouTube channel a video clip called "The Rise of the Prophecy: The Khorasan's Black Flags," which describes jihadists from Afghanistan and other fronts, such as Iraq and Chechnya, as the holy warrior emissaries of the "army of black flags."[19] Thus, it seems that al-Qaeda operatives view the Khorasan group as representing a historic mission of theological importance, which may be realized on the Syrian battlefront.

The Khorasan Group: Poised Between Jabhat al-Nusra and al-Qaeda

Aaron Y. Zelin, an expert in jihad studies at the Washington Institute for Near East Policy, does not consider the Khorasan group a new entity, but rather an assembly of al-Qaeda activists from Afghanistan, Pakistan, and Iran who have joined the Syrian branch of al-Qaeda, i.e., Jabhat al-Nusra. In a series of tweets on Twitter, Zelin wondered why the Pentagon does not explicitly state that the threat emanates from Jabhat al-Nusra, and instead prefers to blame this supposedly new organization.[20] An article published in the *Washington Post* claims that the United States may prefer not to stress that Jabhat al-Nusra is the real threat because it would be tantamount to admitting that the American declarations of having defeated al-Qaeda and being victorious over global terrorism were overestimated, if not outright fallacious.[21] This leads to the next question: Is the United States currently exaggerating when it speaks of the severity of the dangers posed by the Khorasan group?[22]

Dr. Matthew Levitt, an Islamic terrorism researcher at the Washington Institute for Near East Policy, claims that the Khorasan group is, in fact, part of Jabhat al-Nusra, and that it has a specific mission of planning attacks against the West; according to Levitt, this mission grabbed the attention of the American intelligence community and led to the airstrikes on the group's targets in Syria.[23] Prof. Bruce Hoffman makes a similar claim that Jabhat al-Nusra is a "local or regional power and the Khorasan is the international strike force" of al-Qaeda.[24] Dr. David Gartenstein-Ross, an American researcher, claims that the minimal information available about the Khorasan group does not shed any light on the group as a whole, but rather only on its operational branch. In this context, he asserts that that group seems to be more than a terrorist cell for foreign operations.[25] This assertion is congruent with media reports according to which Khorasan

members have not participated in the fighting against Assad's army, but rather have concentrated on planning and training for attacks in the West.[26]

Media reports indicate that US authorities have known about the Khorasan group since 2009, when jihadists from al-Qaeda, the Pakistani Taliban, and the Haqqani network[27] formed an underground group called the Association of Holy Warriors of Khorasan (*Ittihad al-mujahidin Khorasan*). In 2012, apparently at an explicit order issued by Ayman al-Zawahiri, the group's members began to move to Syria where they contacted Jabhat al-Nusra operatives and settled into areas under Jabhat al-Nusra's control.[28] Researcher Thomas Joscelyn believes that the United States knew about the Khorasan group's intentions to attack western targets since the beginning of 2014.[29]

According to American officials, the Khorasan group is an entity operating in tandem with al-Qaeda branches all over the world,[30] but very little else is known about the group and its operatives. According to the same sources, the dearth of information about the group has raised many questions about the group and the danger it poses.[31] The uncertainty prompted a Centcom spokesperson to say that "this network was plotting to attack in Europe or the homeland, and we took decisive action to protect our interests and remove their capability to act."[32] Centcom defines the Khorasan group as "a term used to refer to a network of Nusrah Front and al-Qaeda core extremists who share a history of training operatives, facilitating fighters and money, planning attacks against American and Western targets."[33]

All the reports about US airstrikes in Syria indicate that the United States bombed targets identified with the Khorasan group and that it did not carry out any general assault on Jabhat al-Nusra, even though the American forces have been striking at training camps associated with that group. In other words, the United States has tried to differentiate between the Khorasan group and Jabhat al-Nusra. One reason may be that the Syrian opposition groups, who are opposed to President Bashar Assad, consider Jabhat al-Nusra as one of the key rebel organizations. Indeed, after the United States declared Jabhat al-Nusra a terrorist organization,[34] the slogan "We are all Jabhat al-Nusra" has been heard in the streets of Syria.[35] This slogan is meant to show to the United States that the organization operates on behalf of the Syrian people, which is manifested in the organization's full name, *Jabhat al-Nusra lil-ahl al-Sham* (The Support Front for the People of Syria). Moreover, many Syrian Sunnis feel that Jabhat al-Nusra is a local

entity, even though it is the Syrian branch of al-Qaeda; this is in contrast, for example, to the Islamic State.[36]

While researchers disagree about the essence of the Khorasan group, jihadist sources claim that no such group exists or has ever existed. They assert that the group was fabricated and is used as an excuse for the American airstrikes in Syria; those killed are not operatives representing a radical faction of al-Qaeda, but rather members of Jabhat al-Nusra.[37] This claim is supported by American journalists Glenn Greenwald and Murtaza Hussain who assert that the American media networks directly and indirectly serve the United States' war propaganda against Syria by reporting on the Khorasan group. The invention of a new group that poses an imminent danger to the United States, even worse than that of the Islamic State, is meant to justify American intervention in Syria in the form of airstrikes.[38]

Active Members of the Khorasan Group

Social media, especially Twitter, which has evolved into the jihadists' preferred communications platform, reveals information about the Khorasan group.[39] Twitter accounts associated with the Khorasan group can be identified openly by connections to Pakistan-Afghanistan (the Hindu Kush), identification with al-Qaeda in general and its Syrian branch in particular, and of course, by the use of or reference to the name "Khorasan." Twitter accounts as well as media reports indicate the Khorasan group includes al-Qaeda operatives with extensive battlefield experience, and even some who were trained in western armies, such as the French and Australian armies. According to media reports, the Khorasan group consists of forty to sixty operatives – Chechens, Palestinians, Afghanis, Syrians, and even Westerners.[40] One of the key operatives was Muhsin al-Fadhli, a Kuwaiti national and close associate of Osama bin Laden, and one of the few who knew about the 9/11 attacks before they were carried out. Al-Fadhli was a senior al-Qaeda member who, after the attacks on the Twin Towers and the Pentagon, fled Afghanistan for Iran where he found refuge, until al-Qaeda's senior command sent him to Syria to set up an international terrorist network for preparing and training operatives to carry out attacks in Western nations.[41]

Another senior Khorasan group operative is Abed al-Muhsan Abdullah Ibrahim al-Sharah, an al-Qaeda operative from Saudi Arabia and relative of bin Laden; like others in the Khorasan group, al-Sharah also found refuge

in Iran. According to Sami Moubayed,[42] a Syrian analyst associated with the regime, al-Sharah – also known as Snafi al-Nasr – is one of the founders of Jabhat al-Nusra. He had been responsible for the transfer of money, arms, and men from Iran – through Afghanistan and Pakistan – to Iraq. Al-Nasr's Twitter account provides information about other Khorasan group operatives who were apparently killed in Syria, such as Idris al-Baluchi,[43] the nephew of Khaled Sheikh Muhammad who had been a member of Osama bin Laden's inner circle and one of the planners of the 9/11 attacks. Iranian authorities have said that al-Sharah and al-Fadhli had been under house arrest in Iran and that they do not know how they ended up in Syria.[44]

The reports also indicate that Ibrahim al-Asiri, an explosives expert from al-Qaeda's branch in Yemen, is also tied to the Khorasan group.[45] Al-Asiri is the man who planned the bomb hidden in the underwear of Omar Farouk Abed al-Mottaleb, the young Nigerian who tried to blow up Northwest Airlines Flight 253 en route from Amsterdam to Detroit, Michigan on Christmas Day in 2009.[46] Another individual whose name is linked with the Khorasan group is Muhammad Islambouli, a veteran al-Qaeda operative and brother of Khalid Islambouli who assassinated former Egyptian President Anwar Sadat in 1981. Muhammad Islambouli was apparently the link that connected al-Qaeda's central command and Jabhat al-Nusra with the Khorasan group.[47] An interview with Thomas Joscelyn on the podcast of the website Jihadology indicates that Islambouli received reports from al-Fadhli who served as the head of the operations division of the Khorasan group.[48]

The imminent threat attributed to the Khorasan group may stem from the combined and extensive knowledge of its members. For example, the French Abu Hamza was, according to various publications, a former French intelligence office who defected to al-Qaeda.[49] He converted to Islam in 2002 and traveled to Egypt to study religion and Arabic. In 2010, while in France, he told his family he was returning to Egypt; instead he traveled to the tribal regions along the Afghani-Pakistani border where he joined an al-Qaeda training camp. The French Abu Hamza is mentioned in the reports as a dangerous individual who became an expert on homemade explosive devices.[50] As already noted, he was killed in July 2015, apparently in the same attack that killed Muhsin al-Fadhli.[51]

After the first attack on Khorasan strongholds, reports circulated that a senior member of al-Qaeda named Abu Yusuf al-Turki (the Turk) – who had been a graduate of Afghanistan,[52] was a trained sharpshooter, and

had helped establish Jabhat al-Nusra[53] – was also influential within the Khorasan group. A photograph of his corpse alongside an older photograph, supposedly taken in the Afghani mountains, were posted on Twitter by Abu Thabat al-Qasimi (@Mohager44), who identified with al-Qaeda.[54] More information on al-Turki was published on the website From Chechnya to Syria by Joanna Paraszczuk, an investigative journalist studying the connections between Chechnyan jihadists and the war in Syria. According to Paraszczuk, al-Turki was the head trainer for a sharpshooter unit called the "Wolf Unit," which may have been none other than the Khorasan group itself.[55] Jabhat al-Nusra propaganda videos show al-Turki teaching a sharpshooting course to trainees, reminiscent of al-Qaeda's sharpshooting unit.[56] The video was uploaded to YouTube on September 23, 2014, the same day that President Obama first mentioned the threat of the Khorasan group and the American attack on its targets and strongholds in Syria.[57]

The photo of al-Turki's corpse was retweeted by, among others, Usama Korasani (@KorasaN_1428) who noted on his Twitter account that he came to Syria from Khorasan and that he is aligned with Jabhat al-Nusra.[58] This Twitter account had more than 10,000 followers and had over 21,000 tweets. One of the people Usama Korasani followed was Mojahad Korasani (@mojhdk) who, on his account, noted that he came to Syria from the Hindu Kush and that he, too, was a Jabhat al-Nusra operative.[59] This account had more than 12,000 followers, had posted over 1,000 tweets, and followed sixty-three other accounts.

It may be that in addition to the Wolf Unit, the Khorasan group might also be called Jaish al-Nusra (the Assistance Army). This unfamiliar appellation was first published in an English-language online magazine called *al-Risalah* (The Message) produced by the Mujahidin of the Levant. Only two issues had appeared by November 2015 – one in July and the other in October. The October 2015 issue contained an interview with Hamza the Australian, who claimed to be from Australia and had served in the army there where he learned guerrilla fighting skills, converted to Islam before 9/11, went to Afghanistan, and eventually became a senior al-Qaeda operative.[60] In the interview, Hamza the Australian explains that he operates within a group called Jaish al-Nusra, which trains jihadists in various methods of fighting and that al-Qaeda's high command sent him to help Jabhat al-Nusra.[61]

The Khorasan group may also have ties with al-Qaeda in the Indian Subcontinent (*Qa'adat al-Jihad fi Shaba al- Qārrah al-Hindiya*), founded in

September 2014 – the same month in which the Khorasan group first made the headlines.[62] It is also possible that the Khorasan group is linked to a Kashmiri terrorist cell called Brigade 313. A mutual friend of the jihadists mentioned above is Khorasan al-Bala'gh (@Khorasan313).[63] On his Twitter account, Khorasan al-Bala'gh posted a document in English that contains a summary of the declaration of the establishment of al-Qaeda in the Indian Subcontinent. He also linked his Twitter account to a biography of Ilyas Kashmiri, who was said to have served in Pakistan's military intelligence service and its elite Special Services Group. Kashmiri also had participated in the war in Afghanistan and was an adherent of bin Laden's theory of global jihad.[64] According to his biography, Kashmiri established a branch of al-Qaeda, under the name al-Qaeda Brigade 313.[65] He was killed in an American airstrike in June 2011.[66]

The document that Khorasan al-Bala'gh posted includes a call to Muslims in Kashmir, Bangladesh, India, Pakistan, and other nations to join al-Qaeda and the jihadi front in the fight against the regimes in their own countries and against the United States. On September 23, 2012, Khorasan al-Bala'gh published a photograph of a Boeing 747 passenger plane with the caption "Al-Qaeda Airlines."[67] The photo was accompanied by the following statement: "A reminder and message to the United States from Sheikh Osama bin Laden; if our message can reach you in words" followed by a quote of bin Laden threatening that the United States would never know peace and security until the infidel armies left the Muslim lands.[68]

Khorasan al-Bala'gh's Twitter account was suspended in October 2014. Until then, it expressed support for and identification with al-Qaeda and other terrorist organizations, such as the Pakistani Taliban (*Tehrik-i Taliban*) and the Afghani Taliban (the Islamic Emirate of Afghanistan), two groups that have also produced jihadists who formed al-Qaeda in the Indian Subcontinent. Khorasan al-Bala'gh also expressed support for al-Qaeda Brigade 313 – bin Laden's branch in Kashmir[69] – and the Syrian Islamic Front (*al-Jabha al-Islamiyya al-Suriyya*), the umbrella organization for Islamic rebel groups linked to al-Qaeda.[70]

Beyond the meaning of the number 313 in Islamic theology,[71] the number may also indicate ties among various jihadist factions linked to the Khorasan group. For example, there is a connection between Khorasan al-Bala'gh and the Twitter account of Jund al-Fida'a (@313jund) – a fighting brigade of the Afghani Taliban.[72] Defined as "the official account of the Baluchi Mujahidin in the land of jihad, Khorasan Afghanistan," the Twitter account of Jund

al-Fida'a had nearly 200 followers, had posted 461 tweets and followed thirty-two other accounts, one of which belonged to Khorasan al-Bala'gh.

Conclusions

The information compiled about the Khorasan group since it first hit the headlines indicates that the group consists of just a few dozen operatives from different nations. Some of them have military training, especially in guerrilla warfare, and some have technical expertise, such as putting together sophisticated IEDs. They were trained and prepared not for fighting the war in Syria, but rather for carrying out attacks in the West – the United States, Europe, and perhaps also Israel. The group is part of Jabhat al-Nusra, and it is therefore reasonable to assume that it has ties to al-Qaeda factions throughout the world, such as the branches in Yemen and the Indian subcontinent.

The method of targeted killings that the United States has used with regard to the Khorasan group has taken out some of its operatives, albeit only the well-known ones. We can therefore assume the group still exists. The fact that the United States placed the group on its list of terrorist organizations at the end of September 2015 indicates that it may still pose an imminent danger. It is therefore important to continue following elements that might be connected to the Khorasan group as they could represent a threat not only to the United States and other Western nations, but also to Israel as well as Jewish institutions in Europe and throughout the world. The international reserve of operatives at the Khorasan group's disposal magnifies this threat.

The existence of the Khorasan group underlies the threat that is still embodied by al-Qaeda, which is fighting the Islamic State in leading the global jihad. The Islamic State may be rising in popularity among believing Muslims at the expense of al-Qaeda, but the organization that carried out the 9/11 attacks continues to operate under the radar and to prepare for future massive casualty attacks. It may well be that while western decision makers, the media, and the public at large are watching the Islamic State's beheading videos, al-Qaeda members are busy planning strategic attacks on the West, if only to remind the world that the organization is still alive and capable of inflicting a great deal of pain.

Notes

1 Ken Dilanian and Eileen Sullivan, "Al-Qaida's Syrian Cell Alarms U.S. More Than Islamic State Militants," *Huffington Post*, September 13, 2015, http://www.huffingtonpost.com/2014/09/13/syria-obama-isis_n_5815388.html.

2 The White House, Office of the Press Secretary, "Statement by the President on Airstrikes in Syria," September 23, 2014, https://www.whitehouse.gov/the-press-office/2014/09/23/statement-president-airstrikes-syria.

3 The full name is *Jabhat al-Nusra lil-Ahal al-Sham* (The Syrian People's Assistance Front). Since April 2013, the organization has also been called *Qa'adat al-Jihad fi Bilad al-Sham* (The Jihad Command in the Levant) and is known as the official branch of al-Qaeda in Syria.

4 Michael Crowley, "Khorasan: Behind the Mysterious Name of the Newest Terrorist Threat," *Time Magazine*, September 25, 2014, http://time.com/3430960/obama-isis-khorasan-terrorism. For more about the group, see Karl Morand, "Jihadology Podcast: The Khurasan Group: Myth and Reality," Jihadology, October 7, 2015, http://jihadology.net/2015/10/07/jihadology-podcast-the-khurasan-group-myth-and-reality/.

5 Barbara Starr and Paul Cruickshank, "U.S. Strike in Syria Reportedly Kills Key Bomb-Maker," *CNN*, November 7, 2014, http://edition.cnn.com/2014/11/06/world/syria-strike/index.html. The knowledge for putting together IEDs that can pass through security and screening at airports was published in issue 13 of the magazine *Inspire* of the media division of al-Qaeda in the Arabian Peninsula. The issue came out at the end of December 2015 via Twitter accounts identified with al-Qaeda. See "13th Issue of AQAP Magazine Specifies Individuals and Companies as Targets, Provides Bomb-Making and Security Bypassing Manuals," *SITE Intel Group*, December 25, 2014, http://news.siteintelgroup.com/blog/index.php/categories/jihad/entry/332-13th-issue-of-aqap-magazine-specifies-individuals-and-companies-as-targets,-provides-bomb-making-and-security-bypassing-manuals.

6 "US Bombs Al-Qaeda Offshoot Khorasan for Third Time," *Yahoo*, November 13, 2014, http://news.yahoo.com/us-bombs-al-qaeda-offshoot-khorasan-third-time-233406321.html.

7 Barbara Starr and Paul Cruickshank, "Officials: Khorasan Group Bomb Maker Thought Dead Survived," *CNN*, December 11, 2014, http://edition.cnn.com/2014/12/10/politics/kohrasan-group-bomb-maker-survived/index.html.

8 Eugene Scott and Barbara Starr, "Pentagon Confirms Death of al Qaeda-Tied Bombmaker," *CNN*, September 23, 2015, http://edition.cnn.com/2015/09/23/politics/david-drugeon-al-qaeda-bombmaker/.

9 Evan Perez and Tom LoBianco, "FBI Head: Khorasan Group Diminished; ISIS Bigger Threat than Al Qaeda," *CNN*, July 23, 2015, http://edition.cnn.com/2015/07/22/politics/fbi-james-comey-isis-khorasan-group/index.html.

10 Yitzhak Ben-Horin, "Obama: 'Strikes will not Defeat ISIS, Political Struggle Needed,'" *Ynet*, September 29, 2015, http://www.ynet.co.il/articles/0,7340,L-4705246,00.html, (Hebrew).
11 See report published on the Twitter account of Rita Katz, a terrorism researcher and expert on cyberterrorism, Rita Katz, Twitter Post, Sept 10, 2015, 8:14 PM, https://twitter.com/Rita_Katz/status/642174390361305088.
12 Scott and Starr, "Pentagon Confirms Death of Al Qaeda-Tied Bombmaker."
13 Adam Entous, "Senior al-Qaeda Leader in Syria Killed in U.S. Airstrike," *Wall Street Journal*, October 18, 2015, http://www.wsj.com/articles/senior-al-qaeda-leader-in-syria-killed-in-u-s-airstrike-1445186262.
14 Shane Harris, John Hudson, and Justine Drennan, "Is the Khorasan Group as Dangerous as the White House is Making it Out to Be?" *Foreign Policy*, September 23, 2014, http://www.foreignpolicy.com/articles/2014/09/23/is-the-khorasan-group-as-dangerous-as-the-white-house-claims.
15 Jeremy Bender and Brett Logiurato, "Meet the Khorasan, The Terrorist Group That's Suddenly a Bigger Threat Than ISIS," *Business Insider*, September 23, 2014, http://www.businessinsider.com/what-is-the-khorasan-group-airstrikes-isis-islamic-state-2014-9.
16 "Khorasan Terrorists Will Attack US 'Very, Very Soon,' FBI Director Warns," *Russia Today*, October 6, 2014, http://rt.com/usa/193532-khorasan-fbi-terrorism-syria/; Ken Dilanian and Eileen Sullivan, "AP Enterprise: Al-Qaida's Syrian Cell Alarms US," *Associated Press*, September 13, 2014, http://bigstory.ap.org/article/ap-enterprise-al-qaidas-syrian-cell-alarms-us.
17 For more about the Mahdi, see Stephane Lacroix, "Between Revolution and Apoliticism: Nasr al-Din al-Albani and his Impact on the Shaping of Contemporary Salafism," in *Global Salafism: Islam's New Religious Movement*, ed. Roel Meijer (London: C. Hurst, 2009), pp. 58-80.
18 For more on the topic, see Ali H. Sufyan, *The Black Banners: The Inside Story of 9/11 and the War Against al-Qaeda* (New York: W.W. Norton, 2011); Crowley, "Khorasan: Behind the Mysterious Name of the Newest Terrorist Threat."
19 Crowley, "Khorasan: Behind the Mysterious Name of the Newest Terrorist Threat."
20 Aaron Y. Zelin, Twitter Post, September 23, 2014, 1:31 AM, https://twitter.com/azelin/status/514331217198866434.
21 Adam Taylor, "The Strange Story Behind the 'Khorasan' Group's Name," *Washington Post*, September 25, 2014, http://www.washingtonpost.com/blogs/worldviews/wp/2014/09/25/the-strange-story-behind-the-khorasan-groups-name.
22 See, for example, Theodore Karasik, "Do Khorasan Militants Represent a Real Threat?" *Al-Arabiya*, September 28, 2014, http://english.alarabiya.net/en/views/news/middle-east/2014/09/28/Do-Khorasan-militants-represent-a-real-threat-.html.
23 Matthew Levitt, "The Khorasan Group Should Scare Us," *Washington Institute for Near East Policy*, September 25, 2014, http://www.

washingtoninstitute.org/policy-analysis/view/the-khorasan-group-should-scare-us; Matthew Levitt, "Khorasan group . . . Wolf Unit . . . What's in a Name?" *Washington Institute for Near East Policy*, October 2, 2014, http://www.washingtoninstitute.org/policy-analysis/view/khorasan-group...wolf-unit...whats-in-a-name. See also Levitt's response to Zelin, subsequent to a Twitter discussion about the Khorasan group and the threat it poses, Matthew Levitt, Twitter Post, September 23, 2014, 4:16 AM, https://twitter.com/Levitt_Matt/status/514372620046061568.

24 Siobhan Gorman and Maria Abi-Habib, "Syria Airstrikes Roil Rebel Alliances," *Wall Street Journal*, September 27, 2014, http://www.wsj.com/articles/airstrikes-in-syria-roil-rebel-alliances-1411773506.

25 Rosie Gray, "How 'Khorasan' Went from Nowhere to the Biggest Threat to the U.S.," *Buzz Feed News*, September 23, 2014, http://www.buzzfeed.com/rosiegray/how-khorasan-went-from-nowhere-to-the-biggest-threat-to-the#; Morand, "Jihadology Podcast."

26 Levitt, "The Khorasan group Should Scare Us"; Levitt, "Khorasan group . . . Wolf Unit . . . What's in a Name?"; Kristina Wong, "The Khorasan group: 5 things to Know," *Hill*, September 24, 2014, http://thehill.com/policy/defense/218848-the-khorasan-group-5-things-to-know.

27 A terrorist network based on the Haqqani tribe from Waziristan – a province on the Afghani-Pakistani border – where al-Qaeda commanders and operatives found refuge after the US invasion of Afghanistan following the 9/11 attacks. For more on the topic, see Vahid Brown and Don Rassler, *Fountainhead of Jihad: The Haqqani Nexus, 1973 - 2012* **(**New York: Oxford University Press, 2013).

28 Dina Temple-Raston, "Al-Qaida Reasserts Itself With Khorasan Group," *NPR*, October 3, 2014, http://www.npr.org/blogs/thetwo-way/2014/10/03/353498827/al-Qaida-reasserts-itself-with-khorasan-group; Mark Mazzetti, "A Terror Cell That Avoided the Spotlight," *New York Times*, September 24, 2014, http://www.nytimes.com/2014/09/25/world/middleeast/khorasan-a-terror-cell-that-avoided-the-spotlight.html; Mark Mazzetti, Michael S. Schmidt, and Ben Hubbard, "U.S. Suspects More Direct Threats Beyond ISIS," *New York Times*, September 20, 2014, http://www.nytimes.com/2014/09/21/world/middleeast/us-sees-other-more-direct-threats-beyond-isis-.html.

29 Morand, "Jihadology Podcast."

30 Al-Qaeda has branches in North Africa (al-Qaeda in the Islamic Maghreb), Yemen (al-Qaeda in the Arabian Peninsula), Somalia (al-Shabbab al-Mujahidin), Syria (Jabhat al-Nusra—al-Qaeda in the Levant), and in the Indian subcontinent.

31 Temple-Raston, "Al-Qaida Reasserts Itself with Khorasan Group"; Erin Banco, "Khorasan Group Disappears from US Political Rhetoric, Raising Questions about its Existence," *International Business Times*, November 5,

2014, http://www.ibtimes.com/khorasan-group-disappears-us-political-rhetoric-raising-questions-about-its-existence-1719393.

32 Kate Brannen, "Exclusive: U.S. Renews Air Campaign Against Khorasan Group," *Foreign Policy*, November 6, 2014, http://foreignpolicy.com/2014/11/06/exclusive-u-s-renews-air-campaign-against-khorasan-group/.

33 Ibid.

34 Victoria Nuland, "Terrorist Designations of the al-Nusrah Front as an Alias for al-Qa'ida in Iraq," US Department of State, December 11, 2012, http://www.state.gov/r/pa/prs/ps/2012/12/201759.html.

35 Another slogan used was "If terrorism means flying the flag of the One God [*tawhid*], we proudly say, 'we are all terrorists'"; see, for example, Yabrud Mabasher, "Yabrud 14-12-2012 Friday [slogan] we are all Jabhat al-Nusra 3c [third part] announcements to the world," YouTube, December 14, 2012, https://www.youtube.com/watch?v=FEtUeFwk5gY.

36 For more on the opposition against the Assad regime, see Jeffery White, Andrew J. Tabler, and Aaron Y. Zelin, "Syria's Military Opposition: How Effective, United or Extremist?" *Washington Institute for Near East Policy*, September 2013; Gorman and Abi-Habib, "Syria Airstrikes Roil Rebel Alliances."

37 See, for example, an announcement posted to the Twitter account of *Jihad News* – an online platform serving the propaganda needs of jihadist terrorist organizations from all over the world – that explains that operatives killed in the coalition airstrikes in Syria who were said to be members of the Khorasan group are actually Jabhat al-Nusra operatives, https://twitter.com/JihadNews2/status/514483571013468160. The account has since been suspended.

38 Glenn Greenwald and Murtaza Hussain, "The Fake Terror Threat Used to Justify Bombing Syria," *Intercept*, September 28, 2014, https://firstlook.org/theintercept/2014/09/28/u-s-officials-invented-terror-group-justify-bombing-syria.

39 Gabriel Weimann, "New Terrorism and New Media," Washington, DC: Commons Lab of the Woodrow Wilson International Center for Scholars, Research Series, 2 (2014), p. 8.

40 Temple-Raston, "Al-Qaida Reasserts Itself with Khorasan Group."

41 Erin Banco, "UN Documents Point To Deep Links Between Khorasan Leader Mohsin al Fadhli And Al Nusra Front In Syria," *International Business Times*, September 24, 2014, http://www.ibtimes.com/un-documents-point-deep-links-between-khorasan-leader-mohsin-al-fadhli-al-nusra-front-1694521; Phil Stewart, Mark Hosenball, "U.S. Says Still Assessing Fate of Khorasan Figure after Air Strike," *Reuters*, September 24, 2014, http://www.reuters.com/article/2014/09/24/us-syria-crisis-usa-khorasan-idUSKCN0HJ1HZ20140924.

42 Sami Moubayed, *Under the Black Flag: At the Frontier of the New Jihad* (London and New York: I. B. Tauris, 2015), pp. 67-68.

43 For announcement of the death of al-Baluchi, see Snafi al-Nasr, Twitter Post, August 24, 2015, 1:40 PM, https://twitter.com/snafialnasr0/status/635912047616753664.
44 Mazzetti, "A Terror Cell that Avoided the Spotlight."
45 Harris, Hudson and Drennan, "Is the Khorasan group as Dangerous as the White House is Making it Out to be?"; Gray, "How 'Khorasan' Went from Nowhere to the Biggest Threat to the U.S."; Temple-Raston, "Al-Qaida Reasserts Itself with Khorasan Group"; Dilanian and Sullivan, "Al-Qaida's Syrian Cell Alarms U.S. more than Islamic State Militants."
46 "Profile: Al-Qaeda 'Bomb Maker' Ibrahim al-Asiri," *BBC*, July 4, 2014, http://www.bbc.com/news/world-middle-east-11662143.
47 Karl Morand, "Jihadology Podcast: The Khurasan Group: Myth and Reality," Jihadology, October 7, 2015, http://jihadology.net/2015/10/07/jihadology-podcast-the-khurasan-group-myth-and-reality/.
48 Ibid.
49 Willis Robinson, "Hunt for French Intelligence Officer-Turned-Islamic-Terrorist Plotting Attack on US," *Mail Online*, October 6, 2014, http://www.dailymail.co.uk/news/article-2781803/French-intelligence-officer-defected-Al-Qaeda-target-US-air-strikes-Iraq.html; Mitchell Prothero, "Sources: U.S. Air Strikes in Syria Targeted French Agent who Defected to al Qaida," McClatchyDC, October 5, 2014, http://www.mcclatchydc.com/2014/10/05/242218/sources-us-air-strikes-in-syria.html.
50 "Father of 'Dead' French Jihadist Speaks Out," *Yahoo*, November 7, 2014, http://news.yahoo.com/father-dead-french-jihadist-speaks-162012833.html; "US Airstrikes 'Kill French Khorasan Bombmaker' in Syria," *Telegraph*, November 7, 2014, http://www.telegraph.co.uk/news/worldnews/islamic-state/11215196/US-airstrikes-kill-French-Khorasan-bombmaker-in-Syria.html.
51 "French Jihadist Drugeon Likely Killed in Syria: US Official," *France 24*, September 11, 2015, http://www.france24.com/en/20150911-french-jihadist-drugeon-likely-killed-syria-us-official; "Al-Qaeda Operative Muhsin al-Fadhli Killed in Air Strike – Pentagon," *Reuters*, July 22, 2015, http://uk.reuters.com/article/2015/07/22/uk-mideast-crisis-qaeda-idUKKCN0PV2AN20150722.
52 After the Soviet Union invaded Afghanistan in 1979, thousands of Muslim volunteers entered the country to fight against the Soviet occupation. These men were called *mujahidin* (holy warriors). Some joined Osama bin Laden and Abdullah Azzam's training camps. Later on they became known as the "graduates of Afghanistan."
53 Moubayed, *Under the Black Flag*, pp. 67-68.
54 Abu Thabat al-Qasimi, Twitter Post, September 23, 2014, 7:31 AM, https://twitter.com/mohager44/status/514421920557989888.
55 Levitt, "Khorasan group ...Wolf Unit ...What's in a Name?"

56 Johana Paraszczuk, "Wolf or Khorasan: Who Was Jabhat al-Nusra's Abu Yusuf al-Turki?" From Chechnya to Syria, October 2, 2014, http://www.chechensinsyria.com/?p=22623.

57 Gundem Manset, "Ebu Yusuf et Turki Kanas Birliği," YouTube, September 23, 2014, http://www.youtube.com/watch?v=4BivvIg1WxQ. The video has since then been removed.

58 Usama Korasani's Twitter account: https://twitter.com/KorasaN_1428. The account has since been suspended.

59 Mojahad Korasani's Twitter account: https://twitter.com/mojhdk. It has since been suspended. A new account at https://twitter.com/mojahdq.was opened on June 10, 2015, and updated on September 7, 2015. It also has been removed.

60 Paul Farrell and Michael Safi, "Former Australian Soldier Believed Dead May be Fighting for al-Qaida in Syria," *Guardian*, October 26, 2015, http://www.theguardian.com/australia-news/2015/oct/27/former-australian-soldier-believed-dead-may-be-fighting-for-al-qaida-in-syria.

61 "A Call from Usama: Hamza Australi, Jaish Nusra Trainer," *al-Risalah*, 2, pp. 11-18, https://archive.org/details/AlRisalah2_20151. This content has since been removed.

62 Bill Roggio, "Al Qaeda Opens Branch in the Indian Subcontinent," *Long War Journal*, September 3, 2014, http://www.longwarjournal.org/archives/2014/09/al_qaeda_opens_branc.php.

63 https://twitter.com/khorasan313. The account was closed in November 2014.

64 Bill Roggio, "Al Qaeda Brigade 313 Website Goes Online," *Long War Journal*, August 2, 2010, http://www.longwarjournal.org/archives/2010/08/al_qaeda_brigade_313_website_goes_online.php.

65 The Khorasan Author, "What's Happening in the Islamic Emirate – Battle for the Greater Subcontinent, Chapter 2," Justpaste.it, September 13, 2014, http://justpaste.it/IEACh2. This content has since been removed. The original tweet was posted on September 13, 2014 on https://twitter.com/khorasan313/status/510723600912236544. The account has since been suspended.

66 Hamza Ameer, "New Leader Plans Attacks on Pakistan," *Asia Times*, August 31, 2011, http://www.atimes.com/atimes/South_Asia/MH31Df01.html; Bill Roggio, "Jihadists Seek to Open New Front in Burma," *Long War Journal*, July 15, 2013, http://www.longwarjournal.org/archives/2013/07/jihadists_seek_to_op.php.

67 It should be noted that "al-Qaeda Airlines" is also the name of an online magazine in Arabic designed to instruct Muslims in carrying out attacks by means of smuggling and explosives onto passenger airlines. As of September 2015, only two issues had been published, both in April 2012. See, for example, Mytheos Holt, "'Al Qaeda Airlines Magazine': The Most Disturbingly Clinical Guide to Jihad You'll See," *Blaze*, May 16, 2012, http://

www.theblaze.com/stories/2012/05/16/al-qaeda-airlines-magazine-the-most-disturbingly-clinical-guide-to-jihad-youll-see/.

68 A photograph of "al-Qaeda Airlines" appeared on Khorasan al-Bala'gh's Twitter account, https://twitter.com/khorasan313/status/514508478761955328. This account has since been removed.

69 Roggio, "Al Qaeda Brigade 313 Website Goes Online"; Paul Cruickshank, "Inside al Qaeda Succession: Who is likely to Step Up," *CNN*, May 7, 2011, http://edition.cnn.com/2011/WORLD/asiapcf/05/06/al.qaeda.succession/.

70 One of the central groups in this umbrella organization is the Syrian Freedom Movement (*Harakat Ahrar al-Sham*), a Syrian Salafist group led by Abu Khaled al-Suri, Ayman al-Zawahiri's representative in Syria. Al-Suri was killed in an Islamic State suicide bombing in the struggle for control over territories liberated from Syrian army control. See Aaron Y. Zelin, "The War between ISIS and al-Qaeda," *Washington Institute for Near East Policy*, Research Notes Number 20, June 2014, p. 5.

71 The lore is that there were 313 emissaries of the prophet, the last of whom was Muhammad. Furthermore, the number refers also to the famous Battle of Badr in which Muhammad led an army of only 313 men, two horses, and seventy camels and defeated the infidels of Mecca who formed a large army of some 1,000 men. According to Islamic tradition, Muhammad was accompanied by angels. The Battle of Badr is still considered to be emblematic of heroism and bravery. For more on the meaning of the number 313, see the English-language Sufi website Deen Islam (The religion of Islam), which defines itself as a western guide to Sufism: "17th Ramadhan Urs of People of Badr – 'Ahl Badri and There [sic] Names are a Dua of Attained Sainthood – Wilaya and Tawassul," Deen Islam, http://www.deenislam.co.uk/17Ramadhan-Urs-of-People-of-Badr.htm.

72 Jund al-Fada'a's Twitter account: https://twitter.com/313jund. This account has since been suspended.

Combating Terrorism: Socioeconomic Issues, Boko Haram, and Insecurity in the North-East Region of Nigeria

Oluwaseun Bamidele

The discourse on the root causes of the Boko Haram domestic terrorism group rages on in Nigeria, as extremists continue to lure destitute militants to their cause. Counter-terrorism needs to focus its efforts on eradicating the breeding grounds for these impoverished sympathizers. A new strategy and a new method should be adopted to prevent the threat of domestic terrorism. Fighting domestic terrorism with human development, specifically social and economic development, should emerge as a new public narrative and long-term objective as part of strategic efforts to counter-terrorism. This paper is an attempt to explore the possible linkage between domestic terrorism and the socioeconomic situation in the North-East region of Nigeria. It examines the possible links between poverty, unemployment, illiteracy, health, and the growth of domestic terrorism.

Keywords: Boko Haram, counter-terrorism, domestic terrorism, North-East region, Nigeria

Introduction

Nigerian policymakers, analysts, and academics have been engaged in a national and international discourse on the underlying causes of the Boko Haram domestic terrorist group in the North-East region of Nigeria ever since the cataclysmic Boko Haram domestic terrorist attacks of 2009. Broadly speaking, two schools of thoughts have emerged. In one school of

Oluwaseun Bamidele is a graduate scholar at the Institute of Peace, Security and Governance, Ekiti State University, Nigeria. His research interests are in the field of corruption and anticorruption, transitional justice, security, gender justice, terrorism, and development in sub-Saharan Africa.

thought, the center-left maintains that the struggle against the root causes of domestic terrorism should prioritize social and economic development. Inspired by both contemporary theory and modernization theory, this school of thought sees social and economic development as the precursor of democratization. It also considers educational and economic empowerment as the best antidote against domestic terrorist recruitment. Since poverty often creates a breeding ground for domestic terrorism, socioeconomic development appears compelling as an effective panacea. This correlation between socioeconomic deprivation and domestic terrorism is strongly rejected by the second school of thought. Using simple logic, this school asserts that most domestic terrorists are neither poor nor uneducated. In fact, the majority seem to come from middle class, ordinary backgrounds. Domestic terrorism is therefore perceived almost exclusively as a "security threat" without any discernible socioeconomic roots or links to relative deprivation. Not surprisingly, this second schools of thought defines the fight against domestic terrorism with a single-minded focus on state actors, jihadist ideology, counter-intelligence, and coercive action.[1]

Both schools of thought make valid points; yet, they also share important shortcomings. The root causes of domestic terrorism are extremely complex, multifaceted, and often intertwined. They resist simplification and easy categorization. Therefore, it should be stated from the outset that there is no unique panacea or simple formula to eradicate domestic terrorism. In the absence of "one size fits all" measures, only a long-term, multipronged strategy aimed at strengthening the institutional underpinnings of development, democracy, and security will achieve effective results. Such a strategy should take into consideration the tension between the two schools outlined above. This article argues that the best way to bridge the important gap between the "development first" school and the "security first" school is to drop the notion of a "war against terror" in favor of a strategic campaign against Boko Haram's domestic terrorism. The tools with which to engage this long-term campaign will come to us by focusing on human development – not just economic growth – in a country where political, economic, and social conditions foment violence. In short, fighting domestic terrorism with human development should emerge as a new public narrative and long-term objective of strategically countering terrorism.

Prioritizing Socioeconomic Issues rather than Domestic Terrorism

Domestic terrorism has multiple causes. Attempts to create a single typology of domestic terrorism or generic profiles for Boko Haram terrorists are often misleading. An ideal breeding ground for recruitment emerges when various social, cultural, economic, political, and psychological factors come together; and even when such negative dynamics converge, different terrorist networks have varying political objectives. Despite such complexities and diversity, all domestic terrorist groups share one common objective: the willingness to kill or harm civilians for their cause. This is why domestic terrorism is ultimately a major security concern.

Therefore, there is no point in denying that counter-terrorism is primarily about securing the homeland and protecting unarmed civilians with utmost vigilance, applying safety measures, intelligence gathering, law enforcement, interagency coordination, and the use of force when necessary. The Boko Haram domestic terrorist group would not be deterred by anything less than the strongest security measures. The national debate about the root causes of Boko Haram's domestic terrorism, however, is not about foreign intervention or heavily armed military counter-terrorism. Advocates of this approach are interested in fighting the conditions that create Boko Haram's domestic terrorism, and not the Boko Haram terrorists themselves. This is why the case for social and economic development in the northern states of Nigeria, especially the North-East region, should not be made in the context of counter-terrorism.

The development agenda is not about the Boko Haram domestic terrorists themselves, but rather about those most susceptible to the goals and messages of domestic terrorism. It is precisely within this broader context that a political vocabulary, which goes beyond the narrow confines of domestic terrorism and counter-terrorism, is needed. Fighting socioeconomic issues rather than domestic terrorism provides a better paradigm and framework for a number of reasons. First, Islamist domestic terrorism more accurately reflects the political and ideological dimension of the threat. No matter how diverse the causes, motivations, and ideologies behind domestic terrorism, all attempts at premeditated violence against unarmed civilians share the traits of violent Islamist domestic terrorism. Second, while domestic terrorism is a deadly security challenge, Islamist domestic terrorism is primarily a political threat, and non-coercive measures should be given a chance to counter this terrorism. The possible transition from Islamist domestic terrorism to full-blown domestic terrorism is not pre-destined. In

fact, only a few domestic terrorists venture into full-blown terrorism. At the same time, it is clear that most Boko Haram terrorists start their individual journey towards extremist violence first by becoming Islamist terrorists.

Since socioeconomic issues are often a precursor to domestic terrorism, focusing on socioeconomic challenges amounts to preventing domestic terrorism at an earlier stage, before it is too late for non-coercive measures. In addition, domestic terrorism has social and economic dimensions. While there are Nigerian societies where acts of domestic terrorism find some sympathy and degree of support, there are no "domestic terrorist" societies. Moreover, it is impossible to talk about domestic terrorism as a social and economic phenomenon. The relative popularity of the Boko Haram terrorist group in the Northern region of Nigeria, specifically the North-East region, can only be explained within the framework of such indigent Nigerian societies where religious-based domestic terrorism finds a climate of legitimacy and implicit support. These impoverished Nigerian societies are permeated by a deep sense of collective frustration, humiliation, and deprivation relative to expectations. This social habitat is easily exploited by Boko Haram domestic terrorists. This is why focusing on the collective grievances behind Islamist domestic terrorism is probably the most effective way of addressing the root causes of domestic terrorism. This effort at prevention can be conceived of as a first line of defense against domestic terrorism. The goal is to reduce the social, economic, and political appeal of domestic terrorism by isolating Boko Haram terrorists and winning over potential recruits. Once the challenge is defined as such, the next and more difficult step is to identify an effective strategy to fight Islamist domestic terrorism.

Assessment of the Socioeconomic Problems in Nigeria

The socioeconomic and political context where domestic terrorism takes root, particularly in the context of the North-East region, presents an urgent situation for the remaining regions (North-Central, North-West, South-South, South-West, and South-East). This enabling environment can be altered most effectively by focusing on relative deprivation and human development. Domestic terrorism has deep roots in Nigerian society due to a number of reasons, including easy access to arms and ammunition, poor governance, marginalization of the rural areas, and absence of justice. Moreover, volatile geopolitical situations and porous borders make it vulnerable to all kinds of terrorist threats.[2] Research on domestic terrorism

has focused mainly on the roots of these problems; researchers, analysts, and policy makers alike have little understanding of what drives domestic terrorism. Issues such as poverty, unemployment, poor health, and illiteracy are important contributing factors.[3] In this highly competitive and polarized country, there is far greater awareness of economic and social injustices among the citizens. A survey of the current socioeconomic landscape of the North-East region of Nigeria reveals obvious deprivations. 36 percent of the population lives in poverty, and about 100,000 infants die annually because of diarrhea. Only 35 percent of the population is part of the labor force, and the gross enrolment in elementary education is less than 24 percent.[4] Social and economic inequities, limited access to education and other basic facilities, unemployment, and growing poverty have all produced an atmosphere of despair, which gives rise to frustrations, sense of deprivation and, ultimately, to outrage in the North-East region of Nigeria.

Since dealing with domestic terrorism requires a multidimensional approach, it is necessary for federal and state governments to re-examine the socioeconomic conditions in the North-East region, the main operational area of the domestic terrorists. The North-East region of Nigeria is the worst hit in terms of poverty, unemployment, underdevelopment, and lack of access to education. The people are the most essential pillar of any country's productivity and development. It is the fundamental duty and responsibility of the state to fulfill the basic needs of its people. Basic human needs comprise of shelter, food, and clothing; when these needs are not fulfilled, socioeconomic problems are bound to arise.

The real issue here is not the problems of the North-East region; rather, it is the extent to which the problems are being given attention and tackled. When grievances of the citizens are not rapidly addressed, they often turn out to be a menace for the country. Such citizens exert a negative impact on society; a people deprived of basic necessities of life is either ignorant of or may be spiteful of their duties and obligations toward the country. This results in deviant behavior such as violence, restiveness, drug abuse, smuggling, and corruption. It also breeds poverty, illiteracy, impunity, and many other social evils, including domestic terrorism. A country beset with socioeconomic crises also fails to attract investment. Negligible foreign direct investment (FDI) results in economic slowdown and absence or weakness of competitive local industries, leading to a decline in exports, tumbling stock markets, and inflation.

The North-East region has been facing a range of socioeconomic problems since Nigeria's independence in 1960. From the start, the region had problems of inadequate funds, the need to rehabilitate *almajaris*,[5] poor infrastructure, and widespread poverty. Sir Ahmadu Bello, the late premier of Northern Nigeria, tried his best to solve these socioeconomic problems and to get the state machinery working; due to his sudden death, he could not fulfil his mission. Unfortunately, subsequent military and civilian leaders did not devote enough attention to finding solutions to the various socioeconomic problems. Consequently, the problems exacerbated over time and have become social evils, transmuted into domestic terrorism.

As a developing region, the North-East faces a wide range of social problems, along with political instability which further aggravates the problems. The first problem is poverty. It is rightly said that poverty anywhere is a threat to prosperity everywhere. Some 70 percent of the population of the North-East region lives in rural villages. According to some sources, poverty has increased in the North-East, with the highest incidence of poverty ranging between 54.9 percent to 72.2 percent during the past few years.[6] By another account, 60 percent of the region's population lives below the poverty line.[7] In such conditions, large numbers of northeasterners are deprived of basic necessities of life. Quality education and healthcare are inaccessible. They are forced to think of their survival only.

Perhaps the greatest loss is in the field of education; lack of access to quality education renders the North-East region incapable of dealing with the growing challenges of the twenty-first century. Those affected by poverty are unable to afford quality education and provide a decent upbringing for their children. In addition, negligence on the part of the federal government and governments of the northeastern states aggravates the situation, especially in the area of providing mass education to the *almajiris*. Despite various steps taken by the different state governments to promote quality education, the illiteracy rate has hovered around 72 percent over the years.[8] The North-East spends a meager amount of its gross domestic product (GDP) on this vital sector. Owing to low investment, government-run schools in the region are deprived of basic facilities such as standard classrooms, well-equipped libraries and laboratories, water and sanitation facilities, and electricity. In contrast, the private sector is doing a commendable job in setting up privately-run schools. Owing to the profit objective of this sector, however, this education remains beyond the reach of the poor. The estimated completion rate of primary education

in the region is 30.7 percent among females and 50 percent among males, which shows that the majority of people in the six northeastern states (Adamawa, Bauchi, Borno, Gombe, Taraba, and Yobe) are unable to get a basic education.[9]

The North-East region is also facing the dragon of overpopulation. Its growth rate is very high – of the highest in all of the regions in Nigeria. This may also be a result of porous borders and poor border security and control, which has resulted in an illegal flow of migrants from northern Cameroon, Niger, Chad, and Libya. Since 1967, the population has more than tripled, and the region now has a population of almost 19 million people. Population growth has been a real issue of concern for the federal and northeastern state governments; with limited resources, it is very difficult to cater to the needs of this growing population. The problem is not merely that of population growth or dynamics, but rather negative demographics that are not well managed. The region presently has a youth bulge with over 30 percent of the population under the age of fifteen, and over 50 percent or so are under the age of thirty. Very few jobs are created annually to absorb the growing population and the millions of school leavers. In addition, there is overdependence on poor-yielding arid lands for agriculture and grazing without adequate irrigation and improved farm practices. The health facilities are poor and unable to cater to the rapidly growing population; as a result, life expectancy is about forty-five to fifty years. Great economic disparity also exists among the people of the North-East; the poor are committing crimes out of hunger while the rich are amassing more and more wealth.

The massively increasing population has almost outstripped resources and job opportunities. The region is faced with the problem of unemployment, underemployment, and unemployability; many youth, including graduates, do not even have employable skills for today's labor market nor do they make the best of opportunities around them, such as seeking employment during the dry season, so they remain underemployed or underutilized.[10] The existing unemployment rates are 46.1 percent in Adamawa, 41.4 percent in Bauchi, 52.3 percent in Borno, 46.7 percent in Gombe, 49.1 percent in Taraba, and 43.8 percent in Yobe.[11] The North-East confronts cyclical, technical, structural, and seasonal unemployment, which is economically and socially devastating. The worst is that the unemployment increases every year, which, in the long term, will be harmful to not only the regional

economy, but also the entire country. Unemployment creates frustration, a revengeful attitude among the deprived, and leads to an increase in crime.

The recently crowned Emir of Kano, Sanusi Lamido Sanusi, was quoted as saying in an interview with the *Financial Times* of London that,

> More useful is the suggestion that education (or lack of it) and religion (that has become less tolerant) constitute the bane of North-East underdevelopment. In the 1950s, the Western regional government inaugurated a free primary education program; South West governments in the Second Republic followed suit with free education at all levels, passing laws to make education compulsory till age 16. Imo, with the highest number of students in primary, secondary and tertiary institutions nationwide, has extended its free education program to all levels, while Ogun is spending N1.4 billion on free books for school pupils. The nineteen (19) Northern states, especially the North-East, will need to mobilize their people for mass and compulsory basic education. Illiteracy not only creates unemployment, it makes millions, who, without formal education and skills, become unemployable for life.[12]

Owing to poverty and lack of access to quality education, many parents in the North-East region become destitute and are unable to send their children to schools. Instead, their children become wage earners from a very early age and support their family. Human Rights Watch estimated in 2009 that there would be one to two million beggar children in the region by 2013. Reaffirming this situation, Sanusi also said,

> when the North East leaders organized a summit on the almajiri problem in 2009, they came out with a curious resolution to "reform" the system that has created a mass of two million beggar-children across the North with one million in Kano State alone, but child destitution needs total eradication and the children put to school to acquire knowledge and skills that are required in an increasingly globalized era.[13]

The previous comments underscore the gravity of the situation. The main reason for destitution is poverty, while a low literacy rate has also contributed to the problem to a large extent. Child destitution is a sort of deluge that drains away our precious talents from being utilized in the right places. Child destitution pushes children and young people into bad company and

immoral activities, such as the use of drugs and crime, and increases their vulnerability to extremist ideologies that offer emancipation.

Corruption is another huge socioeconomic problem. The Independent Corrupt Practices Commission (ICPC) has ranked the North-East as the most corrupt region in Nigeria.[14] The menace of corruption is linked to a multitude of social vices. Its roots are linked to injustice, inequity, mistrust, suspicion, favoritism, greed, inefficiency, and so forth. Corruption creates a sense of insecurity, exacerbates poverty, and adds to the misfortune of the vulnerable segments of the region. It also instills a sense of hopelessness and despondency and threatens the upright values that have been established over centuries of civilized struggle. Rising poverty in the North-East necessitates that 10 percent of the GDP is spent on the social sector, including education, health, safe drinking water, sanitation, and basic infrastructure to achieve the Millennium Development Goals (MDGs) by 2015. At present, northeastern state governments spend only 3 percent of GDP on both health and education whereas other regions allocate 9 percent of GDP to these sectors.[15] To make matters worse, the meager fraction allocated, which is already insufficient to cater to the needs of the population, is misappropriated.

Although phenomenal changes have occurred in other regions, the status and fate of women in the North-East region have not improved, and, indeed, have deteriorated. It comes as no surprise that the North-East region was recently rated as one of the worst regions in Nigeria for its treatment of women. More than fifty-two years after independence, 70 percent of North-East women are still subject to domestic violence. One in three is a victim of rape, honor killing, immolation, or acid attack.[16] Women in the North-East have suffered for years from systemic abuse of human rights, including in the state and sharia courts.[17] Whether women or children, Muslims or Christians, Shiites or atheists, the rights of minorities and vulnerable groups are usually threatened. Moreover, the people of the North-East still struggle between secular British and religious Islamic laws and traditions.

The violation of human rights can be attributed to the absence of timely justice for the masses; justice delayed is justice denied. Dispensation of timely justice is the essence of a welfare society. It is the duty of the state to promote justice and provide avenues for justice; however, this has been a dream for the poor masses in the northeastern region of Nigeria. Since independence, the judiciary has been held captive by the establishment. A

compromised and inefficient judiciary is unable to redress the grievances of the masses. Under such conditions, people resort to violent behavior and, as a means of filling in the gap, they resolve issues by applying extreme interpretations of the sharia legal methods.

Furthermore, religious differences add fuel to the fire. Religious extremism, which became entrenched in the North-East after the Maitatsine[18] religious riots in Kano and Borno states during 1980-1982, continues to manifest itself in different forms that are proving intractable in the region.[19] Religious extremism assumed the form of domestic terror against the state in 2009. Following the bombing of the United Nations' headquarters in Abuja, North-Central Nigeria, acts of domestic terror have only grown worse and more frequent. Targeted killings of unarmed civilians is another menace that claims too many innocent lives almost daily. Owing to poor governance, the government is losing control over law and order. Suicide bomb attacks, targeted and indiscriminate killings, robbery, and other crimes have become recurrent events. Sadly, the federal government and northeastern state governments seem to be at a loss as to how best to confront it.

Social problems are interlinked with economic problems. Economic prosperity serves as a backbone and insurance for the overall progress of a nation. One thing is common in all developed nations − they are economically sound and they are internally fairly stable. The state apparatus has a monopoly on the legitimate use of force and strictly enforces it, even if there are exceptional cases. When citizens of a country do not have to worry about their daily struggle to survive and earn a livelihood, they naturally divert their attention to more productive things. The focus usually shifts to improving the quality of education, providing accessible healthcare, developing technologies that make life more liveable, and much more. Poor economic conditions at the micro and macro levels are the root cause of so many problems that exist in the North-East. As if the power crises, lack of FDI for the development of industrial zones, and outdated technology were not enough, the region's free-fall into terrorist control has dealt a fatal blow to the region's already crumbling economic status.

Domestic terrorism has emerged as a monster for the world in general and for Nigeria's North-East region in particular. The involvement of the federal government and northeastern state governments in the declared War on Terror has proved a nightmare. In August 2014, Boko Haram ransacked the towns of Gwoza, Gamboa Biu, Bayo, Limankara, Ngala, Askira, Uba,

Kusar, Bara, Banki, Gulak, Madagali, Bama, and others in the North-East; dethroned their chiefs; occupied their territories; ransacked a riot-police training school; and successfully attacked military barracks.[20] The image of the North-East as a peace-loving region has since been tarnished. Thousands of people living in the region have lost their lives while millions have lost everything they owned and are either displaced to safer, but less welcoming locations in neighboring towns and states, or forced to migrate across the border into Cameroon and parts of Chad.

Boko Haram's domestic terrorism has affected the economy of the North-East region, and by extension, the economy of all of Nigeria. Domestic terrorism is very closely linked to the declining economic conditions. The region's economy has suffered on three accounts: first, large amounts of money are being expended on the war on terrorism, which could have gone to development; second, many foreign investors and markets have been lost due to the insecurity; third, local businesses, industries, and livelihoods have been lost. Energy crises have further crippled the already tumbling economy.[21] They have practically jammed the industrial wheel of the region; owing to frequent power outages, many industrial units have closed. Closure of industries has occasioned the loss of jobs and increased the competitive edge on a large scale. An energy-starved economy fails to attract foreign investment. The poor economic condition of the North-East does not only keep foreign investors away, but local ones as well. When the investment climate for businesses and the industrial sector are not healthy, the inflow of foreign exchange is checked, which may lead to a decline in foreign reserves, and will compel the country to seek loans from other countries and international financial institutions.

Another major problem is the North-East's huge debt incurred by incumbent and former governors as well as by the region's continued dependence on international donors. Moreover, the tax system in the North-East is inefficient and unsatisfactory. The ratio of direct taxes is more than indirect taxes. Tax evasion is common; the rich are reluctant to pay tax, while the poor pay tax even on the purchase of a matchbox. With unhealthy conditions, the region is likely to face low exports and high imports. This is also the case with the industrial sector. Due to an inconsistent supply of electricity to the industrial sector, industries fail to produce optimal output, let alone surplus production. The production of goods in lesser quantities has affected exports from the industrial sector. This causes federal and the northeastern state governments to import goods

and solicit billions of naira in order to meet the needs of the masses, leading to inflation. Inflation provides an important insight into the economy of the North-East states and the policies governing it. Stable inflation not only provides impetus for economic growth, but also helps uplift vulnerable strata of society. In recent years, the North-East region has been in the grip of high inflation, which among other things, has adversely affected its economic health. The overall Consumer Price Index, a key indicator of inflation, has swelled by 33 percent in the last four years, eroding the purchasing power of the people as the overall economy has not performed in line with ever-increasing prices.[22]

Moreover, people living in areas affected by domestic terrorism are migrating to other, safer areas in the region. The North-East has seen the largest internal displacement and migration since the beginning of Boko Haram's domestic terrorism in 2009. 650,000 people have abandoned their homes, businesses, possessions, and property.[23] This influx of people into new areas, in addition to their rehabilitation and provision, is an economic burden for federal and state governments. Unemployment is already prevalent, and now the need to provide employment and productive engagement to these migrants has also become a serious concern. This displaced portion of the population contributes little or nothing worthwhile to the national economy, yet the economy needs to provide for them.

Last, but not least, the loss of a vibrant tourism industry has also contributed to the economic decline. The North-East region has long been a great tourist attraction; the beautiful hills, game reserves, the lush green valleys, shimmering lakes, and flowing waterfalls brought many a tourist to the region. This tourism contributed to foreign exchange. Besides attracting foreign exchange, the tourism industry also provided employment to local people, and served as a source of friendly relations with other countries. Now, both local and foreign media have projected the region as a dangerous and unsafe place.

Relative Deprivation

Breeding grounds for Boko Haram's domestic terrorist recruitment emerge not necessarily under conditions of abject poverty and deprivation, but rather when negative social, economic, and political trends converge. In fact, when analyzed in a broader framework of socioeconomic and political deprivation, the societal support for domestic terrorism in the North-East region of Nigeria gains greater relevance. Dismissing the social and economic

causes of domestic terror on the grounds that some Boko Haram domestic terrorists have middle-class backgrounds is simplistic and misleading. The weak and failing Nigerian state, in addition to ungoverned border spaces that create safe havens for domestic terrorism, are all characteristic of the Northern and/or North-East regions of Nigeria. Boko Haram's domestic terrorism in the North-East region of Nigeria is not necessarily caused by socioeconomic problems, although certainly correlations exist between deprivation and domestic terrorism.

Absolute deprivation in the region is not the real challenge. The more challenging question, particularly in the North-East region of Nigeria, is relative deprivation: the absence of opportunities relative to expectations.[24] Such focus on relative deprivation is important because poverty is no longer an absolute concept in the context of civilization. Civilization creates an acute awareness about opportunities available elsewhere. This leads to frustration, victimization, and humiliation among growing cohorts of urbanized, undereducated, and unemployed Muslim youth who are aware of the opportunities across Nigeria. The scale of youth frustration in the North-East region is compounded by the demographic explosion, growing expectations, weak state capacity, and diminishing opportunities for upward mobility in most of the northern states.[25] Civilization further exacerbates this situation because restive Muslim masses of both genders are caught in the growing tension between religious tradition and civilization.

Socioeconomic decay in the North-East region of Nigeria has created considerably more frustration than in other parts of the Northern region, in part due to historical memory. Particularly in the states of Borno, Yobe, and Adamawa, a sense of nostalgia for the golden age of Islam – during which Arab civilizations far surpassed Europe – is deeply ingrained in the political culture. Muslim-dominated states in Nigeria have a historic, cultural, and civilizational sense of rivalry with the Christian populations in the other regions. Geographic proximity further complicates this picture. Other regions in the country (South-South, South-West, and South-East) are often a historic point of reference in terms of social, economic, and political success. Feelings of a historic sense of superiority combined with the more recent memories of colonial subjugation create a dangerous sense of victimization, resentment, and injustice in large parts of the Northern regions.

All these factors significantly compound the level of frustration of a great civilization nurturing tremendous expectations and aspirations. An

effective strategic campaign against domestic terrorism in the Northern region at large should take into consideration the socio-economic dimension of this collective frustration very seriously. Little can be done in the short term about deeply rooted cultural and psychological grievances, but quite a lot can be done in the social and economic sphere. Take the question of political Islam for example. Weak Muslim northern states in Nigeria are often unable to provide adequate social and economic services. The capacity gap within Muslim states such as Yobe, Adamawa, Borno, and Bauchi creates a vacuum frequently filled by grassroots Islamic organizations that provide goods and services in crucial areas such as health, education, and housing. The strength of these Islamic networks is magnified by the weaknesses of the state system. In that sense, the absence of effective public services opens the field for the rise of Islamist networks with their own political agendas.

Finally, in addition to socioeconomic decay, the absence of constitutional liberties (i.e., the use of sharia law) brings a "political" dimension to relative deprivation in the northern states, particularly in the North-East region. In other words, there is a growing gap between political aspirations and the realities on the ground. Improving educational standards without increasing prospects for employment, or providing jobs without creating outlets for political and social participation all create a combustible mix in the North-East region.

The growing number of educated but unemployed youth is particularly alarming. It is, after all, the educated youth who have the highest political aspirations and expectations, thus being the most frustrated when their expectations are unmet. The growth of unemployment among the educated often creates a class of "frustrated achievers" who may end up becoming domestic terrorists looking for a political cause to embrace.[26] Repressive political systems exacerbate these dynamics. In most Nigerian Muslim states, the mosque is the only institution that is not brutally suppressed; and when the mosque is the only outlet for mass politics, the outcome is predictable: the Islamization of dissent. As dissent turns Islamic, what naturally follows is the politicization of Islam. Political Islam thus slowly has evolved into a resistance movement against injustice, state oppression, and western support for repressive regimes.

As federal and state governments become more repressive, a vicious cycle of violence and counter-violence emerges. Once political Islam is pushed underground, it turns more aggressive and resentful. It is therefore

absolutely necessary to provide legitimate political outlets other than Islam and the mosque for opposition movements in the North-East states.[27] All these problems illustrate the need for alternative strategies to address domestic terrorism in the states of the North-East region. The new approach should find ways to promote democratization, security, and economic development in a comprehensive and harmonious framework. Given the multifaceted nature of factors fueling domestic terrorism, the social and economic agenda against relative deprivation and domestic terrorism needs to be defined very broadly. The goal of "human development in North-East region of Nigeria" offers such an alternative.

Human Development in the North-East Region of Nigeria

Human development involves a much broader public policy agenda than economic growth, mainly because it takes into consideration the social and political dimensions of the human condition as a whole. The basic idea behind human development, as I have conceptualized, is that Gross Domestic Product growth fails to capture the complexity and breadth of development as a social and political phenomenon. Human development considers the social and political progress towards freedom and democracy as an integral part of development. Having dedicated my career to drawing national attention to the crucial role of democracy, freedom, and human rights in promoting economic development,[28] this new way of looking at development is therefore motivated by the need to prioritize the quality of life as much as the quantity of growth. An integral part of my approach to economic development is the need for institutions that promote better governance. Improving state capacity, state legitimacy, and state security are equally important dimensions of better governance and human development. In that sense, human development expands the meaning of development in a similar way that relative deprivation broadens the meaning of poverty. Both concepts are particularly relevant to the debate on the root causes of domestic terrorism. With their emphasis on economic, social, and political aspirations rather than just income per capita, "relative deprivation" and "human development" offer analytical tools for a more strategic approach to domestic terrorism and counter-domestic terrorism. These two concepts also shift the debate from the realm of economic growth to the realm of governance and political economy. Such focus on the Nigerian state is particularly useful in the context of the North-East region, where political power and economic structures are strongly intertwined. One can argue

that the most important challenge facing the majority of the Muslim states in the North-East region is their inability to invest in human development. The underdevelopment of the North-East region needs to be addressed in its proper political, social, and economic context, and not in a vacuum detached from the reality of the power structure. Only such an approach can establish linkages, correlations, and even causalities between political and economic failure. For instance, linkages between failing educational systems and authoritarian state structures become particularly relevant when the problem is analyzed in light of the human development approach. This is also why human development sees democratization and development as a simultaneous process. In other words, it refutes the sequencing argument that places development first, democratization later – an approach strongly implied in modernization theory. As I have argued, democratization should not be detached from economic modernization. Prioritizing one over the other is often bound to produce neither. The systemic connections between political, economic, and social stagnation have been identified in four states in the North-East region, noted by human development reports focusing on democracy, knowledge, and gender deficits. Building on these findings, one can argue that an effective human development strategy can also go a long way in fighting domestic terrorism, especially if enough attention is paid to relative deprivation. This, in turn, requires prioritizing education and employment opportunities, better governance, and incremental democratization in the North-East region states.

The Case for Fighting Domestic Terrorism with Human Development

The economic and social context within which domestic terrorism takes root is profoundly important. Without societal support, most domestic terrorist groups are doomed to fail. That is why an impoverished and politically unstable country like Nigeria is where domestic terrorism tends to become a "systemic" problem. I have argued elsewhere that "Northern states with low, stagnant, and unequally distributed per capita income that have remained dependent on primary commodities for their exports face dangerously high risks of prolonged domestic terrorism. In the absence of economic development neither good political institutions, nor ethnic and religious homogeneity, nor high military spending provide significant defenses against large-scale violence."[29] These factors should help us realize that unfavorable socioeconomic dynamics can degenerate into

political violence and perpetuate a vicious cycle of domestic terrorism. At the very least, such problems create an environment where domestic terrorism finds social acceptance. While domestic terrorism results from many interrelated causes, it has recently become popular to argue that the root causes of domestic terrorism are unrelated to economic deprivation and lack of education.[30] The argument that poverty and a lack of education are not associated with domestic terrorism is based on a fallacy that can be summarized as follows: domestic terrorists do not tend to come from the poorest elements of the population; instead, they are often relatively well educated and above average in terms of income. Thus, poverty alone is not the primary factor that disposes people to domestic terrorism, and reducing poverty or improving education will not seriously diminish domestic terrorism.[31] The most common objection to this common argument comes in reference to the Boko Haram domestic terrorist attacks: the majority of their leaders came from good and well educated families, and their leader even had studied at the University of Medina, perceived as one of the most expensive universities. If poverty and a lack of education were to produce domestic terrorism as it is often argued, most Boko Haram terrorists would come from the poorest communities or states in Nigeria.[32] The argument that socioeconomic deprivation is unrelated to domestic terrorism is erroneous for a number of reasons. First, the argument is based on a very narrow and exclusive focus on "elite" domestic terrorist leaders. As a domestic terrorism expert points out, "Effective domestic terrorist groups rely on a division of labor between young and uneducated 'foot soldiers' and ideologically trained and well-funded elite operatives. In Nigeria, the former are often plucked from *madaris*."[33] It is therefore important to acknowledge that while domestic terrorist leaders tend to come from professional classes, the foot soldiers are often poor and uneducated. One should also not be confused by the fact that at the highest level, the implementation of domestic terrorist activity requires proficient group skills and sophistication. The poorest and least educated masses can be recruited by domestic terrorist masterminds; yet they would make ineffective domestic terrorists in a complex operation. Indeed, the more complex an operation is, the greater security risks it entails, and the more likely the participants are to be from the elite – the result of a careful screening process. All these factors only reinforce the importance of addressing the question of relative deprivation and frustrated achievers as a social milieu. The second point with regard to the link between socioeconomic deprivation and domestic terrorism

is the fact that domestic terrorist groups usually seek a failing and poor state like Nigeria, in which to set up shop. This is why Nigeria has easily turned into a haven for domestic terrorism and is often engulfed in a vicious cycle of domestic terrorism or violence. As an expert points out, "Nigeria provides convenient operational bases and safe havens for domestic terrorists. Boko Haram domestic terrorist group take advantage of failing states' porous borders, of its weak and non-existent law enforcement and security services, and of its ineffective judicial institutions to move men, weapons, and money around North-East region of Nigeria."[34]

The number of those impoverished, malnourished, and deprived of fundamental needs, such as security, health care, and education, totals in the hundreds of millions. Is the fact that Nigeria is feared as a breeding ground of instability and mass-murder, as well as reservoirs and exporters of terror, not evidence enough of social and economic problems that are leading to increased transnational terrorism? From Nigeria to Chad, from Chad to Cameroon, from Cameroon to Mali, ungoverned border spaces often attract domestic terrorist networks that use these territories for two major purposes: first, as a staging ground for national attacks; and second, to recruit uneducated and impoverished young men without any prospects.[35]

In that sense, what we should really be focusing on is not the decision of this or that individual (particularly not leaders such as Abubakar Shekau, who are highly atypical even in their own movements) to become a domestic terrorist; rather, we should be looking at the social conditions that make dissident movements more likely to turn to terror and, more importantly, the circumstances under which such dissident movements receive popular support. Such an approach may also provide us with invaluable keys to distinguish between the limited success of a domestic terrorist who does not have any popular support versus the broad backing that Abubakar Shekau and Boko Haram enjoy. When thinking about domestic terrorism, we have to remind ourselves that it is primarily within a troubled and desperate social, economic, and cultural environment that the engineers of domestic terrorism freely recruit and operate, thus causing greater dangers to Nigerian society.

Finally, the assumption that Boko Haram domestic terrorism is unrelated to education and development is based on the failure to distinguish between education and indoctrination in Nigeria. It has been argued that Nigerian Boko Haram domestic terrorism is unrelated to economic deprivation and a lack of education.[36] I have suggested elsewhere that associating a secondary

school education or a higher education with participation in Boko Haram mistakenly imposes a generalized image of educated terrorists.[37] Before reaching sweeping generalizations about economic deprivation and a lack of education with Boko Haram domestic terrorism, it is important to remember that the context within which domestic terrorism occurs has crucial implications. Instead of looking at the connection between Boko Haram domestic terrorism and education in a broader global context, it should be solely confined to Nigerian domestic terrorism.[38] In the case of Nigeria's extremist Boko Haram, what is considered education is actually ideological indoctrination.[39]

Conclusion: The Need for Human Development Support in the North-East Region of Nigeria

Change in Nigeria towards better governance and human development will essentially come from within; yet outside actors such as the United States can also help by increasing and coordinating their financial assistance for human development in the North-East region states. The coordination of federal and state governments' assistance programs will assure the pooling of funds into one budget. If managed effectively, such budget coordination can significantly improve the effectiveness of assistance by avoiding duplication and putting more resources in critical areas such as rural literacy, labor productivity, and microcredit programs linked to technical training. Such increased assistance, however, should be granted with stricter conditionality for institutional reforms. In other words, increased economic assistance to Muslim states like Borno, Yobe, Bauchi, and Adamawa should be presented as an incentive for domestic political reforms. The ownership of reform should be located in the states in the North-East region. While no attempts should be made to impose reforms, federal government assistance should be conditional on institutional reforms. A common mistake of the past has been to accept cosmetic changes as signs of modernization or democratization. This time the effort needs to go beyond the creation of civil society organizations that can easily be co-opted by repressive federal and state governments. The criteria should be institutional changes promoting better governance, political participation, and human development. The reason civil society promotion or income per capita growth has not led to genuine political change in Nigeria is because state institutions never had to change. The organizations, arrangements, laws, decrees, and regulations that constitute the political rules remain

stagnant in Nigeria. Rather than providing transparency, accountability, and political rights – giving citizens a voice and a stake in the system – Nigerian political institutions tended to limit political participation and individual freedom. As previously mentioned, these repressive measures drove political opposition to the mosques and fueled political Islam and domestic terrorism. This is why conditionality in federal government assistance should focus on institutions that will promote not only socioeconomic growth, but also political rights and liberties. In short, this is the essence of a new strategy that will fight domestic terrorism with human development. Such conditionality, in practice, will have to consider progress in areas such as constitutional reform, freedom of the press, the formation of political parties, and a domestically determined calendar for free and fair elections in the medium to long run. There is obviously no simple blueprint for good political liberalization and democratization. Yet, good governance seldom takes root in the absence of social and economic development. Across a wide range of studies and a great variety of sampling, time periods, and statistical methods, the level of socioeconomic development continues to be the single most powerful predictor of the likelihood of democratization.[40] Particularly when it comes to the crucial question of the sustainability of democracy, the level of socioeconomic development is an even stronger determinant. Nigeria's foreign policy urgently needs alternative strategies to address domestic terrorism in its Muslim states. The new approach should seek to promote democratization, security, and economic development in a comprehensive and harmonious framework. Ultimately, Nigeria's success against domestic terrorism will not depend on winning wars in the North-East region, but rather on promoting non-military policies that will strengthen the institutional underpinning of human development in its Muslim North-East region and Northern region generally.

Notes

1 Oluwaseun Bamidele, "Under Threat of Domestic Terrorism: Addressing and Overcoming the Boko Haram 'Jama'atu Ahlus-Sunnah Lidda'Awati Wal Jihad' in the North-Eastern Region of Nigeria," *Africa Insight* 44, no. 3 (2014): 97-110.

2 ICG (International Crisis Group), "Curbing violence in Nigeria (11): The Boko Haram insurgency," *Africa Report* no. 216 (2014): 1-54.

3 Ben E. Aigbokhan, "Growth, Inequality and Poverty in Nigeria," Economic Commission for Africa, *ACGS/ MPAMS Discussion Paper* no. 3 (February 2008).

4 Ibid.

5 The Hausa term "*almajiri*" refers to a person who migrates in the quest for Islamic knowledge, either to study in a specific place or with a popular teacher. The term is derived from the Arabic *al-muhaajir* (*al-muhaajirun*, plural) which means emigrant, and, by inference, is a learned scholar who propagates the peaceful course of Islam. The Islamic concept of migration is widely practiced, especially when acquisition of knowledge at home is either inconvenient or insufficient. *Al-muhaajirun* refers to the companions of the noble Prophet Muhammad who migrated with him from Mecca to Medina in the year 622 CE due to the persecution by the Meccan idol worshippers. The *muhaajirun* or "emigrants" saw the historic migration as an opportunity to leave an environment where learning, preaching, and practicing Islam were criminalized for a clime where learning and righteousness flourished. In contrast, the *almajiri* concept has since outlived its purpose and has contributed to child begging and creating potential terrorist camps in Nigeria.

6 Temidayo Akinsuyi and Seyi Taiwo- Oguntuase, "Ignorance, Poverty Root Cause of Boko Haram - Aregbesola," *Daily Independent Nigeri*a, March 5, 2014, http://independentnig.com/2014/03/05/ignorance-poverty-root-cause-of-boko-haram-aregbesola/.

7 O. Awoyemi, "Poverty in North," *Nigerian Nation Newspaper,* February 21, 2011.

8 Victoria Ojeme, "North has Highest Rate of Poverty – Report," *Vanguard*, September 14, 2011, http://www.vanguardngr.com/2011/09/north-has-highest-rate-of-poverty-report/.

9 Ibid.

10 Bola Tinubu, "Poverty and Terrorism Threaten the Foundations of our Democracy," *Premium Times*, July 1, 2014, https://www.premiumtimesng.com/opinion/164204-boko-haram-poverty-and-threats-to-nigerias-democracyby-bola-tinubu.html#sthash.wBy4XJEm.dpuf.

11 William Wallis, "Nigerian Central Banker Calls for End to Imbalances," *Financial Times* (London), January 26, 2012, https://next.ft.com/content/02ce9e7e-4837-11e1-b1b4-00144feabdc0.

12 Ibid.

13 Ibid.

14 Peter Ikita, "Corruption in Nigeria, not just Boko Haram, is at the Root of Violence: Secrecy surrounding Security Matters and Deeply Entrenched Corruption Are Failing Communities across the Country," *Guardian*, July 11, 2014, http://www.theguardian.com/global-development/povertymatters/2014/jul/11/boko-haram-nigeria-violence-corruption-security.

15 Nigerian National Bureau of Statistics, "Poverty Report on North-East Region (Adamawa, Bauchi, Borno, Gombe, Taraba, and Yobe) of Nigeria 1985–2013," Unpublished Report no. 16, (2013), pp. 28–30.

16 Amnesty International, "The State of the World's Human Rights: Amnesty International Report 2014/15,", http://www.amnestyusa.org/pdfs/AIR15_English.PDF.

17 Freedom House, "Freedom in the World, Nigeria," https://freedomhouse.org/report/freedom-world/2014/nigeria#.VeTqX601j4g.

18 Mohammed Marwa (died 1980), best known by his nickname Maitatsine, was a controversial Islamic preacher in Nigeria. Maitatsine is a Hausa word meaning "the one who damns," and referred to his vitriolic speeches against the state. Originally from Marwa in northern Cameroon. Mohammed Marwa moved to Kano, Nigeria around 1945 upon completing his studies. There he became known for his controversial preaching on the Qur'an. Maitatsine claimed to be a prophet, and saw himself as a *mujaddid* (one who revives Islam) in the image of Sheikh Usman dan Fodio.

19 A.O. Adesoji, "Between Maitatsane and Boko Haram: Islamic Fundamentalism and the Response of the Nigerian State," *Africa Today* 57, no. 4 (2010): 98–119.

20 "Islamic Caliphate: Five Nigerian Towns Taken by Boko Haram in One Week, Hundreds Killed," *Information Nigeria*, September 7, 2014, http://www.informationng.com/2014/09/islamic-caliphate-five-nigerian-towns-taken-by-boko-haram-in-one-week-hundreds-killed.html.

21 Paul Wiseman, "Tumbling Oil Prices, Boko Haram Insurgency, Political Tension Threaten Nigeria's Credit Rating," *Canadian Business*, February 10, 2015, http://www.canadianbusiness.com/business-news/tumbling-oil-prices-boko-haram-insurgency-political-tension-threaten-nigerias-credit-rating/.

22 "Nigeria Consumer Price Index (CPI), 1995-2016," Trading Economics, http://www.tradingeconomics.com/nigeria/consumer-price-index-cpi.

23 436,600 people alone have been displaced in the three states of Adamawa, Borno, and Yobe. In addition to the massive migration, a report from the United Nations Humanitarian Office (OCHA) in August, 2013 indicated that attacks by Boko Haram Islamists in Nigeria's crisis-hit North-East have killed more than 10,000 people since 2009.

24 Audu Jacob, "Poverty and the Security Challenges in the Northern Nigeria: Beyond the Fairy Tales," in *The National Security, Integration & Sustainable Development in Nigeria*, ed. R. Ayo Dunmoye, Ejembi A. Unobe, and Aliyu Rafindadi Sanusi (Zaria: Amadu Bello University 2012), p. 65.

25 Simeon H.O. Alozieuwa, "Contending Theories on Nigeria's Security Challenge in the Era of Boko Haram Insurgency," *Peace and Conflict Review* 7, no. 1 (Fall 2012): 40-63.

26 Oluwaseun Bamidele, "Under Threat of Domestic Terrorism: Addressing and Overcoming the Boko Haram 'Jama'atu Ahlus-Sunnah Lidda'Awati Wal Jihad' in the North-Eastern Region of Nigeria," *Africa Insight* 44, no. 3 (2014): 97-110.

27 Ibid.

28 Ibid.
29 Oluwaseun Bamidele, "Boko Haram Catastrophic Terrorism: An Albatross to National Peace, Security and Sustainable Development in Nigeria," *Journal of Sustainable Development in Africa* 14, no. 1 (2012): 32-42.
30 Patrick L. Akpan, Ebele Mary Onwuka, and Chinedu Onyeizugbe, "Terrorist Activities and Economic Development in Nigeria: An Early Warning Signal," *International Journal of Sustainable Development* 5, no. 4 (2012): 69-78.
31 David Olademeji Alao, Atere Clement Olusegun, and Oluwafisayo Alao, "Boko Haram Insurgence in Nigeria: The Challenges and Lessons," *Singaporean Journal of Business Economics, and Management Studies* 1, no. 4 (2012): 1-15.
32 K. Beetseh and R. Echikwonye, "The Impact of Terrorism and Global Security on the Development of Nigerian Foreign Policy: A Challenge," *Journal of Arts and Contemporary Society* 3, no. 1 (2011).
33 Oluwatoyin Badejogbin, "Boko Haram: An Enquiry into the Socio-Political Context of Nigeria's Counter-Terrorism Response," *Law Democracy & Development* 17 (2013): 226-252.
34 Nkechi O. Anyadike, "Boko Haram and National Security Challenges in Nigeria; Causes and Solutions," *Journal of Economics and Sustainable Development* 4, no. 5 (2013): 12-23.
35 Badejogbin, "Boko Haram."
36 Oluwaseun Bamidele, "Terrorism in Mali and Nigeria: Assessment and Projection," *Counter Terrorist Trends and Analysis: A Journal of the International Centre for Political Violence and Terrorism Research* 7, no. 8 (September 2015): 10-15.
37 Oluwaseun Bamidele, "Boko Haram Catastrophic Terrorism − An Albatross to National Peace, Security and Sustainable Development in Nigeria," *Journal of Sustainable Development in Africa* 14, no. 1 (2012).
38 Don John O. Omale, "Terrorism and Counter Terrorism in Nigeria: Theoretical Paradigms and Lessons for Public Policy," *Canadian Social Science* 9, no. 3 (2013).
39 Oluwaseun Bamidele, "Terrorism in Mali and Nigeria: Assessment and Projection", *Counter Terrorist Trends and Analysis: A Journal of the International Centre for Political Violence and Terrorism Research* 7, no. 8 (September 2015): 10-15.
40 Faith Osasumwen Oviasogie, "State Failure, Terrorism and Global Security: An Appraisal of the Boko Haram Insurgency in Northern Nigeria," *Journal of Sustainable Society* 2, no. 1 (2013): 20-30.

Cyber: Intelligence and Security
Call for Papers

The Institute for National Security Studies (INSS) at Tel Aviv University invites submission of articles for publication in ***Cyber: Intelligence and Security***, a peer-reviewed journal that is published three times a year in English and Hebrew. The journal is edited by Gabi Siboni, Head of the Cyber Security Program and Military and Strategic Affairs Program at INSS.

Articles may relate to the following issues:

- Global policy and strategy in cyberspace
- Cyberspace regulation
- National cybersecurity resilience
- Cyber defense of critical infrastructure
- Cyberspace force buildup
- Ethical and legal aspects of cyberspace
- Cyberspace technologies
- Military cyber operations and warfare
- Military and cyber strategic thinking
- Intelligence, information sharing, and public-private partnership (PPP)
- Cyberspace deterrence
- Cybersecurity threats and risk-analysis methodologies
- Analysis of cyber incidents and lessons learned
- Tactics, techniques, and procedures (TTPs)

Submitted articles should not exceed 6,000 words (including citations and footnotes), and should include an abstract of up to 120 words, and up to ten keywords. Previous issues of the journal may be accessed on the INSS website at http://www.inss.org.il.

Hadas Klein
Coordinator
Cyber: Intelligence and Security
Tel: +972-3-6400400/Ext 488
Cell: +972-54-4510411
hadask@inss.org.il